EXAM PREP

Your Complete Certification Solution!

Exam 312-50

Certified Ethical Hacker

More Than 500,000 Exam Prep Books Sold!

Michael Gregg

Table of Contents

Fast Facts. Certified Ethical Hacker Exam Prep, ISBN: 0789735318

Fast Facts

Certified Ethical Hacker

The Fast Facts listed in this chapter are designed as a refresher for some of the key knowledge areas required to pass the Certified Ethical Hacker (CEH) certification exam. If you can spend an hour prior to your exam reading through this information, you will have a solid understanding of the key information required to succeed in each major area of the exam. You should be able to review the information presented here in less than an hour.

This summary cannot serve as a substitute for all the material supplied in this book. However, its key points should refresh your memory on critical topics. In addition to the information in this chapter, remember to review the glossary terms because they are intentionally not covered here.

Ethics and Legality

- Never exceed the limits of your authorization—Every assignment will have rules of engagement. These not only include what you are authorized to target, but also the extent to which you are authorized to control such a system.
- Written approval is the most critical step of the testing process.
- Ethical hackers perform penetration tests. They perform the same activities a hacker would but without malicious intent.
- Insider attack—This ethical hack simulates the types of attacks and activities that could be carried out by an authorized individual with a legitimate connection to the organization's network.
- Outsider attack—This ethical hack seeks to simulate the types of attacks that could be launched across the Internet. It could target HTTP, SMTP, SQL, or any other available service.
- Stolen equipment attack—This simulation is closely related to a physical attack, as it targets the organizations equipment. It could seek to target

the CEO laptop or the organization's backup tapes. No matter what the target, the goal is the same—extract critical information, usernames, and passwords.

- Physical entry—This simulation seeks to test the organization's physical controls. Systems such as doors, gates, locks, guards, CCTV, and alarms are tested to see if they can be bypassed.
- Bypassed authentication attack—This simulation is tasked with looking for wireless access points and modems. The goal is to see if these systems are secure and offer sufficient authentication controls. If the controls can be bypassed, the ethical hacker may probe to see what level of system control can be obtained.
- Social engineering attack—This simulation does not target technical systems or physical access. Social engineering attacks target the organization's employees and seek to manipulate them to gain privileged information. Proper controls, policies, and procedures can go a long way in defeating this form of attack.

Hackers

- Whitehat hackers—These individuals perform ethical hacking to help secure companies and organizations. Their belief is that you must examine your network in the same manner as a criminal hacker to better understand its vulnerabilities.
- Reformed Blackhat hackers—These individuals often claim to have changed their ways and that they can bring special insight into the ethical hacking methodology.
- Grayhat hackers—These individuals typically follow the law but sometimes venture over to the darker side of black hat hacking. It would be unethical to employ these individuals to perform security duties for your organization as you are never quite clear where they stand.
- Section 1029—Fraud and related activity with access devices. This law gives the U.S. federal government the power to prosecute hackers who knowingly and with intent to defraud produce, use, or traffic in one or more counterfeit access devices. Access devices can be an application or hardware that is created specifically to generate any type of access credentials, including passwords, credit card numbers, long distance telephone service access codes, PINs, and so on for the purpose of unauthorized access.
- Section 1030—Fraud and related activity in connection with computers. The law covers just about any computer or device connected to a network or Internet. It mandates penalties for anyone who accesses a computer in an unauthorized manner or exceeds one's access rights. This makes this a powerful law because companies can use it to prosecute employees when they carry out fraudulent activities by using the rights the companies have given to them.

Footprinting

- The information-gathering steps of footprinting and scanning are of utmost importance. Good information gathering can make the difference between a successful pen test and one that has failed to provide maximum benefit to the client.
- The wayback machine located at www.archive.org can be used to browse archived web pages dating back to 1996. It's a useful tool for looking for information no longer on a site.
- One method to reduce the information leakage from job postings is to reduce the system specific information in the job post or to use a company confidential job posting.

TABLE FF.1 DNS Records and Types

Record Name	Record Type	Purpose
Host	A	Maps a domain name to an IP address
Pointer	PTR	Maps an IP address to a domain name
Name Server	NS	Configures settings for zone transfers and record caching
Start of Authority	SOA	Configures settings for zone transfers and record caching
Service Locator	SRV	Used to locate services in the network
Mail	MX	Used to identify SMTP servers

- A zone transfer is unlike a normal lookup in that the user is attempting to retrieve a copy of the entire zone file for a domain from a DNS server.
- Traceroute is a utility that is used to determine the path to a target computer.

Scanning

- One of the most basic methods of identifying active machines is to perform a ping sweep. Ping is found on just every system running TCP/IP. Although many networks have restricted ping, it is an effective tool if available. Ping uses ICMP and works by sending an *echo request* to a system and waiting for the target to send an *echo reply* back.
- Port scanning is the process of connecting to TCP and UDP ports for the purpose of finding what target device services and applications are open.

TABLE FF.2 Common Port Numbers

Port	Service	Protocol
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
161/162	SNMP	UDP
1433/1434	MSSQL	TCP

TABLE FF.3 TCP Flags

Flag	Purpose
SYN	Synchronize sequence number
ACK	Acknowledgement of sequence number
FIN	Final data flag used during the 4-step shutdown
RST	Reset bit used to close and abnormal connection
PSH	Push data bit used to signal that data in this packet should be pushed to the beginning of the queue
URG	Urgent data bit used to signify that urgent control characters are in this packet that should have priority

- TCP Connect scan—This type of scan is the most reliable but also the most detectable. It is easily logged and detected since a full connection is established. Open ports reply with a SYN/ACK, whereas closed ports respond with a RST/ACK.
- TCP SYN scan—This type of scan is known as half open because a full TCP connection is not established. This type of scan was originally developed to be stealthy and evade IDS systems, although most now detect it. Open ports reply with a SYN/ACK, whereas closed ports respond with a RST/ACK.
- TCP FIN scan—Forget trying to set up a connection; this technique jumps straight to the shutdown. This type of scan sends a FIN packet to the target port. Closed ports should send back a RST.
- TCP NULL scan—Sure, there should be some type of flag in the packet, but a NULL scan sends a packet with no flags set. If the OS has implemented TCP per RFC 793, closed ports will return a RST.

- TCP ACK scan—This scan attempts to determine access control list (ACL) rule sets or identify if stateless inspection is being used. If an ICMP destination is unreachable, a communication administrative prohibited message is returned, the port is considered to be filtered.
- TCP XMAS scan—A port scan that has toggled on the FIN, URG, and PSH flags. Closed ports should return a RST.

Enumeration

- The administrator account has a RID of 500 by default, the guest 501, and the first user account has a RID of 1000.
- Windows stores user information and passwords in the Security Accounts Manager (SAM) database.
- The `net use` command is one powerful tool for enumerating Windows. With a `net use \\target\ipc$ "" /u:""` command, you can perform many enumeration activities.
- Simple Network Management Protocol (SNMP) is a popular TCP/IP standard for remote monitoring and management of hosts, routers, and other nodes and devices on a network. Version 1 is a clear text protocol and provides only limited security through the use of community strings. The default community strings are *public* and *private* and are transmitted in clear text. If the community strings have not been changed or if someone can sniff the community strings, they have more than enough to launch an attack.

System Hacking

- The NetBIOS Auditing Tool (NAT) is a command-line automated password guessing tool.
- Windows authentication protocols include
  - LM authentication—Used by 95/98/ME and based on DES.
  - NTLM authentication—Used by NT until service pack 3 and based on DES and MD4.
  - NTLM v2 authentication—Used post NT service pack 2 and based on MD4 and MD5.
  - Kerberos—Implemented in Windows 2000 and created by MIT in 1988.

- LM passwords are considered weak. The maximum 14 character password is divided into two seven character parts; the two hashed results are concatenated and stored as the LM hash, which is stored in the SAM. Each piece can be cracked separately.
- NTFS alternate data streams (ADS) was developed to provide for compatibility outside the Windows world with structures such as the Macintosh Hierarchical File System (HFS). It is a prime tool that can be used by hackers to hide tools. It only works with NTFS drives.

Trojans and Backdoors

- Trojans are programs that pretend to do one thing but when loaded actually perform another more malicious act.

TABLE FF.4 Remote Control Programs and Their Default Ports

Name	Default Protocol	Default Port
Back Orifice	UDP	31337
Back Orifice 2000	TCP/UDP	54320/54321
Beast	TCP	6666
Citrix ICA	TCP/UDP	1494
Donald Dick	TCP	23476/23477
Loki	ICMP	NA
Masters Paradise	TCP	40421/40422/40426
Netmeeting Remote Desktop Control	TCP/UDP	49608/49609
NetBus	TCP	12345
Netcat	TCP/UDP	Any
pcAnywhere	TCP	5631/5632/65301
Reachout	TCP	43188
Remotely Anywhere	TCP	2000/2001
Remote	TCP/UDP	135–139
Timbuktu	TCP/UDP	407
VNC	TCP/UDP	5800/5801

- Email attachments are the number one means of malware propagation.
- A wrapper is a program used to combine two or more executables into a single packaged program.

- A covert channel is a means of moving information in a manner in which it was not intended.
- Port redirection works by listening on certain ports and then forwarding the packets to a secondary target. Some of the tools used for port redirection include datapipe, fpipe, and Netcat.

TABLE FF.5 Common Netcat Switches

Netcat Switch	Purpose
`nc -d`	Used to detach Netcat from the console
`nc -l -p [port]`	Used to create a simple listening TCP port, adding –u will place it into UDP mode
`nc -e [program]`	Used to redirect stdin/stdout from a program
`nc -w [timeout]`	Used to set a timeout before Netcat automatically quits
`Program ¦ nc`	Used to pipe output of program to Netcat
`nc ¦ program`	Used to pipe output of Netcat to program
`nc -h`	Used to display help options
`nc -v`	Used to put Netcat into verbose mode
`nc -g` or `nc -G`	Used to specify source routing flags
`nc -t`	Used for Telnet negotiation
`nc -o [file]`	Used to hex dump traffic to file
`nc -z`	Used for port scanning, no I/O i

Sniffers

- Passive sniffing is performed when the user is on a hub. Because the user is on a hub, all traffic is sent to all ports.
- Server versions of Windows cannot be upgraded to Windows XP Professional.
- MAC flooding and ARP poisoning are the two ways that the attacker can attempt to overcome the switch.
- MAC flooding is the act of attempting to overload the switches content addressable memory (CAM) table.
- ARP poisoning is the second method that can be used to overcome switches.
- ARP is how network devices associate a specific MAC addresses with IP addresses so that devices on the local network can find each other.
- The ARP cache stores the IP address, the MAC address, and a timer for each entry.

TABLE FF.6 IP Forwarding Syntax

Operating System	Command	Syntax
Linux	Enter the following command: `to edit /proc: 1=Enabled, 0=Disabled`	`echo 1 > /proc/sys/net/ipv4/ip_forward`
Windows 2000, XP, and 2003	Edit the following value in the registry: 1=Enabled, 0=Disabled	IPEnableRouter Location: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\` Parameters Data type: REG_DWORD Valid range: 0–1 Default value: 0 Present by default: Yes

Denial of Service

- DoS attacks represent one of the biggest threats on the Internet. DoS attacks might target a user or an entire organization and can affect the availability of target systems or the entire network.
- DoS attacks can be categorized into three broad categories: bandwidth consumption, resource starvation, and programming flaws.
- Smurf—Exploits Internet Control Message Protocol (ICMP) by sending a spoofed ping packet addressed to the broadcast address with the source address listed as the victim.
- SYN flood—A SYN flood disrupts Transmission Control Protocol (TCP) by sending a large number of fake packets with the SYN flag set. This large number of half open TCP connections fills the buffer on a victim's system and prevents it from accepting legitimate connections.
- One of the distinct differences between DoS and DDoS is that a DDoS attack consists of two distinct phases. First, during the pre-attack, the hacker must compromise computers scattered across the Internet and load software on these clients to aid in the attack. The second phase is the attack.
- Tracking the source of a DDoS attack is difficult because of the distance between the attacker and victim.

TABLE FF.7 DDoS Types and Protocols

DDoS Tool	Attack Method
Trinoo	UDP
TFN	UDP, ICMP, TCP
Stacheldrach	UDP, ICMP, TCP
TFN2K	UDP, ICMP, TCP
Shaft	UDP, ICMP, TCP
Mstream	TCP
Trinity	UDP, TCP

- Egress filtering can be performed by the organization's border routers to reduce the threat of DDoS.

Social Engineering

- Six types of behaviors for a positive response to social engineering are as follows:
  - Scarcity—Works on the belief that something is in short supply. It's a common technique of marketers, "buy now; quantities are limited."
  - Authority—Works on the premise of power. As an example, "hi, is this the help desk? I work for the senior VP, and he needs his password reset in a hurry!"
  - Liking—Works because we tend to do more for people we like than people we don't.
  - Consistency—People like to be consistent. As an example," why should I badge in? Everyone else just walks in once someone opens the door."
  - Social validation—Based on the idea that if one person does it, others will too.
  - Reciprocation—If someone gives you a token or small gift, you feel pressured to give something in return.
- Human-based social engineering works on a personal level. It works by impersonation—posing as an important user, using a third-party approach, masquerading—and can be attempted in person.
- Computer-based social engineering uses software to retrieve information. It works by means of pop-up windows, email attachments, and fake websites.

- Reverse social engineering involves sabotaging someone else's equipment and then offering to fix the problem. It requires the social engineer to first sabotage the equipment, and then market the fact that he can fix the damaged device, or pretend to be a support person assigned to make the repair.
- There are a few good ways to deter and prevent social engineering, and user awareness, policies, and procedures rate among the best.

Session Hijacking

- Spoofing is the act of pretending to be someone else, whereas hijacking involves taking over an active connection.
- For hijacking to be successful, several things must be accomplished. Identify and find an active session, predict the sequence number, take one of the parties offline, and take control of the session.
- A fundamental design of TCP is that every byte of data transmitted must have a sequence number. The sequence number is used to keep track of the data and to provide reliability.
- Using encrypted protocols such as SSH can make session hijacking more difficult for the attacker.

Hacking Web Servers

- Attacks can be categorized as either a buffer overflow attack, source disclosure attack, or a file system traversal attack.
- Unicode input validation attack. Unicode was developed as a replacement to ASCII. Unlike ASCII, however, Unicode uses a 16-bit dataspace, so it can support a wide variety of alphabets, including Cyrillic, Chinese, Japanese, Arabic, and others. The source of the vulnerability is not the Unicode itself but how it is processed.
- An un-patched server can suffer a multitude of attacks that target well-known exploits and vulnerabilities. Security patches and updates are critical to ensure that the operating system and web server are running with the latest files and fixes.

Fast Facts. Certified Ethical Hacker Exam Prep, ISBN: 0789735318

Web Application Vulnerabilities

- Windows has a variety of services that can run in the background to provide continuous functionality or features to the operating system. By disabling unwanted services, you can reduce the attack surface of the IIs server.
- Perform logging to keep track of activity on your IIs server. Auditing allows you to understand and detect any unusual activity. Although auditing is not a preventative measure, it will provide valuable information about the access activity on your IIs server.

Web-Based Password Cracking Techniques

- Basic authentication is achieved through the process of exclusive ORing (XOR) and is considered weak.
- Message digest authentication is a big improvement over basic. Message digest uses the MD5 hashing algorithm. Message digest is based on a challenge response protocol. It uses the username, the password, and a nonce (random) value to create an encrypted value that is passed to the server.
- Forms-based authentication is widely used on the Internet. It functions through the use of a cookie that is issued to a client. Once authenticated, the application generates a cookie or session variable.
- Certificate-based authentication is considered strong. When users attempt to authenticate, they present the web server with their certificate. The certificate contains a public key and the signature of the Certificate authority.
- Dictionary attacks—A text file full of dictionary words is loaded into a password program and then run against user accounts located by the application. If simple passwords have been used, this might be enough to do the trick.
- Hybrid attacks—Similar to a dictionary attack, except that it adds numbers or symbols to the dictionary words. Many people change their passwords by simply adding a number to the end of their current password. The pattern usually takes this form: first month's password is "Mike"; second month's password is "Mike2"; third month's password is "Mike3"; and so on.
- Brute force attacks—The most comprehensive form of attack and the most potentially time-consuming. Brute force attacks can take weeks, depending on the length and complexity of the password.

SQL Injection

- SQL servers are vulnerable because of poor coding practices, lack of input validation, and the failure to update and patch the service.
- There are a lot of tools to hack SQL databases. Some are listed here: SQLDict, SQLExec, SQLbf, SQLSmack, and SQL2.

Hacking Wireless Networks

- Bluetooth operates at a frequency of 2.45GHz and divides the bandwidth into narrow channels to avoid interference with other devices that use the same frequency.
- Bluetooth has been shown to be vulnerable to attack. One early exploit is *Bluejacking*. It allows an individual to send unsolicited messages over Bluetooth to other Bluetooth devices.
- Bluesnarfing is the theft of data, calendar information, or phone book entries. This means that no one within range can make a connection to your Bluetooth device and download any information they want without your knowledge or permission.

TABLE FF.8 Wireless Standards and Frequencies

IEEE WLAN Standard	Over-the-Air Estimates	Frequencies
802.11b	11Mbps	2.4000–2.2835GHz
802.11a	54Mbps	5.725–5.825GHz
802.11g	54Mbps	2.4000–2.2835GHz
802.11n	540Mbps	2.4000–2.2835GHz

- The 802.11b 802.11g and 802.11n systems divide the usable spectrum into 14 overlapping staggered channels whose frequencies are 5MHz apart.
- Direct-sequence spread spectrum (DSSS)—This method of transmission divides the stream of information to be transmitted into small bits. These bits of data are mapped to a pattern of ratios called a *spreading code*.
- Frequency-hopping spread spectrum (FHSS)—This method of transmission operates by taking a broad slice of the bandwidth spectrum and dividing it into smaller subchannels of about 1MHz.
- WPA uses Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and adds an integrity-checking feature which verifies that the keys haven't been tampered with. WPA improves on WEP by increasing the IV from 24 bits to 48. Rollover has also been eliminated, which means that key reuse is less likely to occur.

TABLE FF.9 WPA Versus WPA2

Mode	WPA	WPA2
Enterprise mode	Authentication: IEEE 802.1x EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1x EAP Encryption: AES-CCMP
Personal mode	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

TABLE FF.10 EAP Types

Service	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Server Authentication	No	Uses password hash	Public key certificate	Public key certificate	Public key certificate
Supplicant Authentication	Uses password hash	Uses password hash	Smart card or public key certificate	PAP, CHAP, or MS-CHAP	Any EAP type such as public key certificate
Dynamic Key Delivery	No	Yes	Yes	Yes	Yes
Security Concerns	Vulnerable to man-in-the-middle attack, session hijack, or identity exposure	Vulnerable to dictionary attack or identity exposure	Vulnerable to identity exposure	Vulnerable to man-in-the-middle attack	Vulnerable to man-in-the-middle attack

Virus and Worms

- Master boot record infection—This is the original method of attack. It works by attacking the master boot record of floppy disks or the hard drive. This was effective in the days when everyone passed around floppy disks.
- File infection—A slightly newer form of virus that relies on the user to execute the file. Extensions such as .com and .exe are typically used. Some form of social engineering is normally used to get the user to execute the program. Techniques include renaming the program or trying to run an .exe extension and make it appear as a graphic or .bmp.
- Macro infection—The most modern type of virus began appearing in the 1990s. Macro viruses exploit scripting services installed on your computer. The I Love You virus is a prime example of a macro infector.
- Signatures scanning antivirus programs work in a similar fashion as IDS pattern matching systems. Signature scanning antivirus software looks at the beginning and end of executable files for known virus signatures.
- Heuristic scanning is another method that antivirus programs use. Software designed for this function examines computer files for irregular or unusual instructions.

- Integrity checking can also be used to scan for viruses. Integrity checking works by building a database of checksums or hashed values. These values are saved in a file. Periodically new scans occur, and the results are compared to the stored results.
- Activity blockers can also be used by antivirus programs. An activity blocker intercepts a virus when it starts to execute and blocks it from infecting other programs or data. Activity blockers are usually designed to start upon bootup and continue until the computer is shut down.

Physical Security

TABLE FF.11 Power Faults

Fault	Description
Blackout	Prolonged loss of power
Brownout	Power degradation that is low and less than normal
Sag	Momentary low voltage
Fault	Momentary loss of power
Spike	Momentary high voltage
Surge	Prolonged high voltage
Noise	Interference superimposed onto the power line
Transient	Noise disturbances of a short duration
Inrush	Initial surge of power at startup

- A turnstile is a form of gate that prevents more than one person at a time from gaining access to a controlled area. Turnstiles usually only turn in one direction to restrict movement to only that direction.
- Piggybacking is the primary way that someone would try to bypass a mantrap. To prevent and detect this, guards and CCTV can be used.
- Fire prevention should be performed to make sure that employees are trained and know how to prevent fires from occurring and how to respond when they do.
- Fire detection systems are used to signal employees that there might be a problem.
- Fire suppression addresses the means of extinguishing a fire. Not all fires are composed of the same combustible components.
- Passwords and pin numbers—These authentication systems are based on something you know: as an example, a name and an alphanumeric password or pin number.

- Tokens, smart cards, and magnetic strip cards—These authentication systems are based on something you have. As an example, your employer might have issued you a smart card with your ID embedded in it that is read by readers throughout the organization and will allow you to access controlled areas.
- Biometrics—These authentication systems are based on what you are, such as a fingerprint, retina scan, or voice print. As an example, the company you work for might have placed a fingerprint reader outside the server room to keep unauthorized individuals out.
- The discretionary access control model is one most users are familiar with. Access control is left to the owner's discretion.
- Mandatory access control features a static model and is based on a predetermined list of access privileges.
- Defense in depth is about building multiple layers of security that will protect the organization better than one single layer.

Linux Hacking

- Root is always assigned the UID 0 and the GID 0.
- The shadow file is used to protect passwords as it is only readable by root.
- Most versions of Linux, such as Red Hat, use *MD5* for password encryption.
- Salts are needed to add a layer of randomness to the passwords.
- Because the passwd file is world readable, passwords should be stored in the shadow file.
- Password cracking programs such as John the Ripper work against the Linux OS; all they require is access to the encrypted passwords.
- Linux passwords are usually salted. This means that they have had a second layer or randomness added so that no two users have the same encrypted password.
- Rootkits can be divided into two basic types. Traditionally, rootkits replaced binaries such as ls, ifconfig, inetd, killall, login, netstat, passwd, pidof, or ps with trojaned versions. The second type of rootkit is the loadable kernel module (LKM). A kernel rootkit is loaded as a driver or kernel extension.
- Tripwire is the most commonly used file integrity program. It performs integrity checking by using cryptographic checksums.

Evading Firewalls, IDS, and Honeypots

- Pattern matching and anomaly detection are the two distinct types of IDS systems used.
- Snort is a freeware IDS.

TABLE FF.12 Snort Keywords and Meaning

Keyword	Detail
content	Used to match a defined payload value.
ack	Used to match TCP ack settings.
flags	Used to match TCP flags.
id	Matches IP header fragment.
ttl	Used to match the IP header TTL.
msg	Prints a message.

TABLE FF.13 Snort Rulesets

Rule	Description
Alert tcp any any -> 192,168.13.0/24 (msg: "O/S Fingerprint detected"; flags: S12;)	OS fingerprint
Alert tcp any any -> 192,168.13.0/24 (msg: "NULL scan detected"; flags: 0;)	Null scan
Alert tcp any any -> 192,168.13.0/24 (msg: "SYN-FIN scan detected"; flags: SF;)	SYN/FIN scan
Alert udp any any -> any 69 (msg "TFTP Connection Attempt)";)	TFTP attempt
Alert tcp any any -> 192,168.13.0/24 (content: "Password"; msg: "Password Transfer Possible!";)	Password transfer

- Attackers can use a range of techniques to attempt to prevent IDS detection, including flooding, evasion, and session splicing.

Buffer Overflows

- C programs are especially susceptible to buffer overflow attacks.
- Buffer overflows occur when a program puts more data into a buffer than it can hold.
- A heap is a memory space that is dynamically allocated. Heap-based buffer overflows are different from stack-based buffer overflows in that the stack-based buffer overflow depends on overflowing a fixed length buffer.

- A range of software products can be used to defend against buffer overflows, including Return Address Defender (RAD), StackGuard, and Immunix.

Cryptography

- Plaintext—Clear text that is readable.
- Ciphertext—Data that is scrambled and unreadable.
- Cryptographic key—A key is a piece of information that controls how the cryptographic algorithm functions. It can be used to control the transformation of plaintext to ciphertext or ciphertext to plaintext. As an example, the Caesar cipher uses a key that moves forward three characters to encrypt and back by three characters to decrypt.
- Substitution cipher—A simple method of encryption in which units of plaintext are substituted with ciphertext according to a regular system. This could be by advancing one or more letters in the alphabet. The receiver deciphers the text by performing an inverse substitution.

TABLE FF.14 Encryption Advantages and Disadvantages

Type of Encryption	Advantage	Disadvantage
Symmetric	Faster than asymmetric	Key Distribution
		Only provides confidentiality
Asymmetric	Easy key exchange	Slower than symmetric
	Can provide confidentiality and authentication	

- Digital certificates are used to prove your identity when performing electronic transactions.

Penetration Testing

- An asset is any item of economic value owned by an individual or corporation. Assets can be real, such as routers, servers, hard drives, and laptops, or assets can be virtual, such as formulas, databases, spreadsheets, trade secrets, and processing time.
- A threat is any agent, condition, or circumstance that could potentially cause harm, loss, damage, or compromise to an IT asset or data asset. From a security professional's perspective, threats can be categorized as events that can affect the confidentiality, integrity, or availability of the organization's assets. These threats can result in destruction, disclosure, modification, corruption of data, or denial of service.

- A vulnerability is a weakness in the system design, implementation, software or code, or other mechanism. A specific vulnerability might manifest as anything from a weakness in system design to the implementation of an operational procedure.
- Security testing is the primary job of ethical hackers. These tests might be configured in such way that the ethical hackers have full knowledge, partial knowledge, or no knowledge of the *target of evaluation* (TOE).
- No knowledge testing is also known as *blackbox testing*. Simply stated, the security team has no knowledge of the target network or its systems. Blackbox testing simulates an outsider attack, as outsiders usually don't know anything about the network or systems they are probing.
- Whitebox testing takes the opposite approach of blackbox testing. This form of security test takes the premise that the security tester has full knowledge of the network, systems, and infrastructure.
- In the world of software testing, graybox testing is described as a partial knowledge test. EC-Council literature describes graybox testing as a form of internal test. Therefore, the goal is to determine what insiders can access.
- Pen testing follows a fixed methodology. To beat a hacker, you have to think like one, so it's important to understand the methodology.
- Reconnaissance is considered the first pre-attack phase. The hacker seeks to find out as much information as possible about the victim.
- Scanning and enumeration is considered the second pre-attack phase. At this step in the methodology, the hacker is moving from passive information gathering to active information gathering.
- Gaining access is when the hacker moves from simply probing the network to actually attacking it. Once the hacker has gained access, he can begin to move from system to system, spreading his damage as he progresses.
- Privilege escalation can best be described as the act of leveraging a bug or vulnerability in an application or operating system to gain access to resources that normally would have been protected from an average user.
- Covering tracks is when an attempt is made to make sure to remove all evidence of an attacker's activities. This might include using rootkits to cover their tracks. Other hackers might hunt down log files and attempt to alter or erase them.