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

Practice Exam and Answers..... 1
Certified Ethical Hacker..... 1
Practice Exam Questions..... 2
Answers to Practice Exam Questions..... 27

Practice Exam and Answers. Certified Ethical Hacker Exam Prep, ISBN: 0789735318

Practice Exam and Answers

Certified Ethical Hacker

This exam consists of 110 questions that reflect the material covered in this book. The questions represent the types of questions you should expect to see on the Certified Ethical Hacker exam; however, they are not intended to match exactly what is on the exam.

Some of the questions require that you deduce the best possible answer. In other cases, you are asked to identify the best course of action to take in a given situation. You must read the questions carefully and thoroughly before you attempt to answer them. It is strongly recommended that you treat this exam as if it were the actual exam. When you take it, time yourself, read carefully, and answer all the questions to the best of your ability.

The answers to all the questions appear in the section following the exam. Check your letter answers against those in the answers section, and then read the explanations provided. If you answer incorrectly, you should return to the appropriate chapter in the book to review the material.

Practice Exam and Answers. Certified Ethical Hacker Exam Prep, ISBN: 0789735318

Practice Exam Questions

1. You just noticed a member of your pen test team sending an email to an address that you know does not exist within the company for which you are contracted to perform the penetration test. Why is he doing this?

   - ❍ **A.** To determine who is the holder of the root account
   - ❍ **B.** To determine if the email server is vulnerable to a relay attack
   - ❍ **C.** To test the network's IDS systems
   - ❍ **D.** To generate a response back that will reveal information about email servers

2. What is the range for dynamic random ports?

   - ❍ **A.** 1024–49151
   - ❍ **B.** 1–1024
   - ❍ **C.** 49152–65535
   - ❍ **D.** 0–1023

3. What does the following command achieve?

```
Telnet <IP Address> <Port 80>
HEAD /HTTP/1.0
<Return>
<Return>
```

   - ❍ **A.** This command returns the home page for the IP address specified.
   - ❍ **B.** This command opens a backdoor Telnet session to the IP address specified.
   - ❍ **C.** This command returns the banner of the website specified by the IP address.
   - ❍ **D.** This command allows a hacker to determine if the server has a SQL database.

4. You would like to perform a port scan that would allow you to determine if a stateless firewall is being used. Which of the following would be the best option?

   - ❍ **A.** XMAS scan
   - ❍ **B.** Idle scan
   - ❍ **C.** Stealth scan
   - ❍ **D.** ACK scan

5. You have become concerned that someone could attempt to poison your DNS server. What determines how long cache poisoning would last?

- ❍ **A.** A record
- ❍ **B.** CNAME
- ❍ **C.** SOA
- ❍ **D.** MX

6. Which of the following Trojans uses port 6666?

- ❍ **A.** Subseven
- ❍ **B.** NetBus
- ❍ **C.** Amitis
- ❍ **D.** Beast

7. Which of the following best describes a wrapper?

- ❍ **A.** Wrappers are used as tunneling programs.
- ❍ **B.** Wrappers are used to cause a Trojan to self execute when previewed within email.
- ❍ **C.** Wrappers are used as backdoors to allow unauthenticated access.
- ❍ **D.** Wrappers are used to package covert programs with overt programs.

8. Loki uses which of the following by default?

- ❍ **A.** ICMP
- ❍ **B.** UDP 69
- ❍ **C.** TCP 80
- ❍ **D.** IGRP

9. You have become concerned that one of your workstations might be infected with a malicious program. Which of the following netstat switches would be the best to use?

- ❍ **A.** `netstat -an`
- ❍ **B.** `netstat -r`
- ❍ **C.** `netstat -p`
- ❍ **D.** `netstat -s`

10. You have just completed a scan of your servers, and you found port 12345 open. Which of the following programs uses that port by default?

- ❍ **A.** Donald Dick
- ❍ **B.** Back Orifice
- ❍ **C.** Subseven
- ❍ **D.** NetBus

11. Which of the following federal laws makes it a crime to knowingly and intentionally use cellular telephones that are altered or have been cloned?

- ❍ **A.** 18 USC 2701
- ❍ **B.** 18 USC 2511
- ❍ **C.** 18 USC 2319
- ❍ **D.** 18 USC 1029

12. You have been reading about SSIDs and how they are transmitted in clear text. Which of the following is correct about SSIDs?

- ❍ **A.** SSIDs are up to 32 bits and are not case sensitive.
- ❍ **B.** SSIDs are up to 24 bits and are case sensitive.
- ❍ **C.** SSIDs are up to 32 bits and are case sensitive.
- ❍ **D.** SSIDs are up to 24 bits and are not case sensitive.

13. You have been asked to install and turn on WEP on an access point that is used in the shipping area. Which of the following statements is true?

- ❍ **A.** The MAC addresses can still be sniffed.
- ❍ **B.** The IP header can still be sniffed.
- ❍ **C.** FTP passwords will still be seen in clear text if a hacker sniffs the wireless network.
- ❍ **D.** WEP will make the network secure from DoS attacks.

14. Which of the following does not provide server authentication?

- ❍ **A.** EAP-TLS
- ❍ **B.** PEAP
- ❍ **C.** LEAP
- ❍ **D.** EAP-MD5

15. You would like to scan for Bluetooth devices that are used in the office. Which of the following tools would work best?

- ❍ **A.** Airsnort
- ❍ **B.** Aeropeek
- ❍ **C.** RedFang
- ❍ **D.** NetStumbler

16. Rosa would like to make sure that the digital photos and art she produces are recognizable in case her work is stolen and placed on another website. What should she do?

- ❍ **A.** Copyright it
- ❍ **B.** Use steganography
- ❍ **C.** Digital watermark
- ❍ **D.** Use a digital certificate

17. What do programs, such as Tripwire, MD5sum, and Windows System File Protection, all rely on?

- ❍ **A.** Digital certificates
- ❍ **B.** Hashing
- ❍ **C.** Digital signatures
- ❍ **D.** Steganography

18. How many characters is the output of an MD5sum?

- ❍ **A.** 128 characters
- ❍ **B.** 64 characters
- ❍ **C.** 32 characters
- ❍ **D.** 16 characters

19. What binary coding is most commonly used for email purposes?

- ❍ **A.** UUencode
- ❍ **B.** SMTP
- ❍ **C.** XOR
- ❍ **D.** Base64

20. What hashing algorithm produces a 128-bit hash value?

- ❍ **A.** MD5
- ❍ **B.** 3DES
- ❍ **C.** SHA-1
- ❍ **D.** AES

21. During a penetration text, you found several systems connected to the Internet that have a low security level, which allows for the free recording of cookies. This creates a risk because cookies locally store which of the following?

- ❍ **A.** Information about the web server
- ❍ **B.** Information about the user
- ❍ **C.** Information for the Internet connection
- ❍ **D.** Specific Internet pages

22. You have been asked to analyze the following portion of a web page:

```
<!-- Begin
function Login(){
var done=0;
var username=document.login.username.value;
username=username.toLowerCase();
var password=document.login.password.value;
password=password.toLowerCase();
if (username=="customer" && password=="solutions")
➥ { window.location="customer.html"; done=1; }
if (done==0) { alert("Invalid login!"); }
}
// End -->
```

What do you surmise?

- ❍ **A.** This is part of a web script that is used for PKI authentication.
- ❍ **B.** This is part of a web script for a customer solutions page.
- ❍ **C.** This is part of a web script that uses an insecure authentication mechanism.
- ❍ **D.** You see no problems with the script as written.

23. While performing a penetration test for an ISP that provides Internet connection services to airports for their wireless customers, you have been presented with the following issues: The ISP uses Wireless Transport Layer Security (WTLS) and Secure Socket Layers (SSL) technology to protect the airports end users' authentication and payment transactions. Which of the following are you most concerned about?

- ❍ **A.** If a hacker were to compromise the Wireless Application Protocol (WAP) gateway
- ❍ **B.** If a hacker installed a sniffing program in front of the server
- ❍ **C.** If a hacker stole a user's laptop at the security checkpoint
- ❍ **D.** If a hacker sniffed the wireless transmission

24. Peter has successfully stolen the SAM from a system he has been examining for several days. Here is the output:

```
Administrator:1008:6145CBC5A0A3E8C6AAD3B435B51404EE
Donald:1000:16AC416C2658E00DAAD3B435B51404EE
Tony:1004:AA79E536EDFC475E813EFCA2725F52B0
Chris:0:A00B9194BEDB81FEAAD3B435B51404EE
George:1003:6ABB219687320CFFAAD3B435B51404EE
Billy:500:648948730C2D6B9CAAD3B435B51404EE:
```

From the preceding list, identify the user with Administrator privileges?

- ❍ **A.** Administrator
- ❍ **B.** Donald
- ❍ **C.** Chris
- ❍ **D.** Billy

25. You have been asked to set up an access point and override the signal of a real access point. This way, you can capture the user's authentication as he attempts to log in. What kind of attack is this?

- ❍ **A.** Wardriving
- ❍ **B.** Rogue access point
- ❍ **C.** Denial of service
- ❍ **D.** Bluejacking

26. Which of the following can help you detect changes made by a hacker to the system log of a server?

- ❍ **A.** Mirroring the system log onto a second server
- ❍ **B.** Writing the system log to not only the server, but also on a write-once disk
- ❍ **C.** Setting permissions to write protect the directory containing the system log
- ❍ **D.** Storing the backup of the system log offsite

27. Which of the following is not one of the three items that security is based on?

- ❍ **A.** Confidentiality
- ❍ **B.** Availability
- ❍ **C.** Authentication
- ❍ **D.** Integrity

28. Which of the following best describes a phreaker?

- ❍ **A.** A hacker who is skilled in manipulating the phone system
- ❍ **B.** A hacker who is skilled in social engineering
- ❍ **C.** A hacker who is skilled in manipulating the Voice over IP (VoIP)
- ❍ **D.** A hacker who is skilled in manipulating cryptographic algorithms

29. Which of the following terms best describes malware?

- ❍ **A.** Risks
- ❍ **B.** Threats
- ❍ **C.** Vulnerabilities
- ❍ **D.** Exploit

30. Which of the following best describes the principle of defense in-depth?

- ❍ **A.** Two firewalls in parallel to check different types of incoming traffic
- ❍ **B.** Making sure that the outside of a computer center building has no signs or marking so that it is not easily found
- ❍ **C.** Using a firewall as well as encryption to control and secure incoming network traffic
- ❍ **D.** Using two firewalls made by different vendors to consecutively check the incoming network traffic

31. Which of the following are the two primary U.S. laws that address cybercrime?

- ❍ **A.** 1030 and 2701
- ❍ **B.** 2510 and 1029
- ❍ **C.** 2510 and 2701
- ❍ **D.** 1029 and 1030

32. Which of the following is the most serious risk associated with vulnerability assessment tools?

- ❍ **A.** False positives
- ❍ **B.** False negatives
- ❍ **C.** Non-specific reporting features
- ❍ **D.** Platform dependent

33. You have successfully extracted the SAM from a Windows 2000 server. Is it possible to determine if an LM hash that you're looking at contains a password fewer than eight characters long?

- ❍ **A.** A hash cannot be reversed; therefore, you are unable to tell.
- ❍ **B.** The rightmost portion of the hash will always have the same value.
- ❍ **C.** The hash always starts with 1404EE.
- ❍ **D.** The leftmost portion of the hash will always have the same value.

34. You have been tasked with examining the web pages of a target site. You have grown tired of looking at each online. Which of the following offers a more efficient way of performing this task?

- ❍ **A.** Using wget to download all pages for further inspection
- ❍ **B.** Using pwdump to download all pages for further inspection
- ❍ **C.** Using dumpsec to download all pages for further inspection
- ❍ **D.** Using Achilles to download all pages for further inspection

35. You would like to find out more information about a website from a company based in France. Which of the following is a good starting point?

- ❍ **A.** AfriNIC
- ❍ **B.** ARIN
- ❍ **C.** APNIC
- ❍ **D.** RIPE

36. Which of the following best describes passive information gathering?

- ❍ **A.** Scanning
- ❍ **B.** Maintaining access
- ❍ **C.** Cover tracks and placing backdoors
- ❍ **D.** Reconnaissance

37. While scanning the target network, you discovered that all the web servers in the DMS respond to ACK packets on port 80. What does this tell you?

- ❍ **A.** All the servers are Windows based.
- ❍ **B.** The target organization is not using an IDS.
- ❍ **C.** All the servers are UNIX based.
- ❍ **D.** The target organization is using a packet filter.

38. After gaining access to a span of network that connects local systems to a remote site, you discover that you can easily intercept traffic and data. Which of the follow should you recommend in your report as a countermeasure?

- ❍ **A.** Installing high-end switches
- ❍ **B.** Encryption
- ❍ **C.** Callback modems
- ❍ **D.** Message authentication

39. As you prepare to set up a covert channel using Netcat, you are worried about your traffic being sniffed on the network. Which of the following is your best option?

- ❍ **A.** Use netcat with the –v option
- ❍ **B.** Use netcat with the –p option
- ❍ **C.** Use cryptcat instead
- ❍ **D.** Use netcat with the –e option

40. You were successful in your dumpster diving raids against the target organization, and you uncovered sensitive information. In your final report, what is the best solution you can recommend to prevent this kind of hacking attack?

- ❍ **A.** Signs warning against trespassing
- ❍ **B.** CCTV cameras in the dumpster area
- ❍ **C.** Shredders
- ❍ **D.** Locks on dumpsters

41. The ability to capture a stream of data packets and then insert them back into the network as a valid message is known as which of the following?

- ❍ **A.** Eavesdropping
- ❍ **B.** Message modification
- ❍ **C.** Brute-force attack
- ❍ **D.** Packet replay

42. A SYN flood can be detected by which of the following?

- ❍ **A.** A large number of SYN packets appearing on the network without corresponding ACK responses
- ❍ **B.** Packets that have both the same source and destination IP addresses
- ❍ **C.** A large number of SYN packets appearing on the network with random segment sizes
- ❍ **D.** Packets that have both the same source and destination port addresses

43. While preparing to hack a targeted network, you would like to check the configuration of the DNS server. What port should you look for to attempt a zone transfer?

- ❍ **A.** 53 UDP
- ❍ **B.** 79 TCP
- ❍ **C.** 53 TCP
- ❍ **D.** 79 UDP

44. Refer to the following figure. What is the destination MAC address?

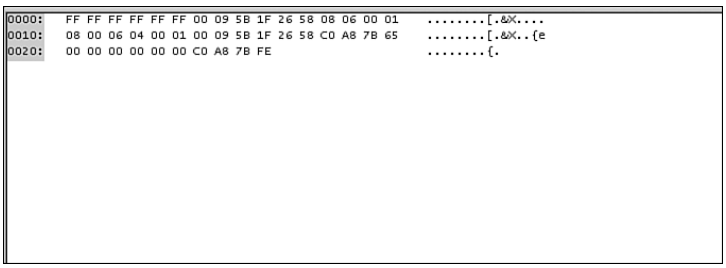

FIGURE PE.1 Packet capture.

- ❍ **A.** A multicast
- ❍ **B.** A broadcast
- ❍ **C.** The default gateway
- ❍ **D.** C0 A8 7B 65

45. Which of the following is used to verify the proof of identity?

- ❍ **A.** Asymmetric encryption
- ❍ **B.** Symmetric encryption
- ❍ **C.** Non-repudiation
- ❍ **D.** Hashing

46. Which type of lock would be considered the easiest to pick?

- ❍ **A.** Cipher
- ❍ **B.** Warded
- ❍ **C.** Device
- ❍ **D.** Tumbler

47. You have successfully run an exploit against an IIS4 server. Which of the following is the default privilege you will have within the command shell that you have spawned?

- ❍ **A.** Local system
- ❍ **B.** Administrator
- ❍ **C.** IIS default account
- ❍ **D.** IUSR_Computername

48. An idle scan makes use of which of the following parameters?

- ❍ **A.** The datagram size
- ❍ **B.** The segment size
- ❍ **C.** The IPID
- ❍ **D.** The ACK number

49. Which of the following can be used to ensure a sender's authenticity and an email's confidentiality?

- ❍ **A.** By first encrypting the hash of the message with the sender's private key and then encrypting the hash of the message with the receiver's public key
- ❍ **B.** Having the sender digitally signing the message and then encrypting the hash of the message with the sender's private key
- ❍ **C.** By first encrypting the hash of the message with the sender's private key and then encrypting the message with the receiver's public key
- ❍ **D.** By first encrypting the message with the sender's private key and then encrypting the message hash with the receiver's public key

50. Which of the following is used for integrity?

- ❍ **A.** DES
- ❍ **B.** Diffie-Hellman
- ❍ **C.** MD5
- ❍ **D.** AES

51. Which kind of lock includes a keypad that can be used to control access into areas?

- ❍ **A.** Cipher
- ❍ **B.** Warded
- ❍ **C.** Device
- ❍ **D.** Tumbler

52. You have been given the data capture in the following figure to analyze. What type of packet is this?

FIGURE PE.2
Data dump.

- ❍ **A.** It was generated by Loki.
- ❍ **B.** It is a Linux ping packet.
- ❍ **C.** There is not enough information to tell.
- ❍ **D.** It is a Windows ping packet.

53. When working with Windows systems, what is the RID of the first user account?

- ❍ **A.** 100
- ❍ **B.** 500
- ❍ **C.** 1000
- ❍ **D.** 1001

54. Which of the following GUI scanners is designed to run on a Windows platform and is used for port 80 vulnerability scans?

- ❍ **A.** Nessus
- ❍ **B.** Ethereal
- ❍ **C.** N-Stealth
- ❍ **D.** Whisker

55. Which of the following represents the weakest form of encryption?

- ❍ **A.** DES ECB
- ❍ **B.** RC5
- ❍ **C.** Base64
- ❍ **D.** AES

56. During a physical assessment of an organization, you noticed that there is only an old dilapidated wood fence around the organization's R&D facility. As this building is a key asset, what height chain-link fence should you recommend be installed to deter a determined intruder?

- ❍ **A.** Four foot
- ❍ **B.** Five foot
- ❍ **C.** Six foot
- ❍ **D.** Eight foot

57. You have been asked if there are any tools that can be used to run a covert channel over ICMP. What should you suggest?

- ❍ **A.** Netbus
- ❍ **B.** Loki
- ❍ **C.** Fpipe
- ❍ **D.** Sid2User

58. This DoS tool is characterized by the fact that it sends packets with the same source and destination address. What is it called?

- ❍ **A.** Ping of death
- ❍ **B.** Smurf
- ❍ **C.** Land
- ❍ **D.** Targa

59. Your sniffing attempts have been less than successful, as the targeted LAN is using a switched network. Luckily, a co-worker introduced you to Cain. What type of attack can Cain perform against switches to make your sniffing attempt more successful?

- ❍ **A.** MAC flooding
- ❍ **B.** ICMP redirect
- ❍ **C.** ARP poisoning
- ❍ **D.** IP forwarding

60. Which of the following uses the same key to encode and decode data?

- ❍ **A.** RSA
- ❍ **B.** El Gamel
- ❍ **C.** ECC
- ❍ **D.** RC5

61. This type of active sniffing attack attempts to overflow the switch's content addressable memory (CAM).

- ❍ **A.** MAC flooding
- ❍ **B.** ICMP redirect
- ❍ **C.** ARP poisoning
- ❍ **D.** IP forwarding

62. You have been asked to prepare a quote for a potential client who is requesting a penetration test. Which of the following listed items is the most important to ensure the success of the penetration test?

- ❍ **A.** A well-documented planned testing procedure
- ❍ **B.** A proper schedule that specifies the timed length of the test
- ❍ **C.** The involvement of the management of the client organization
- ❍ **D.** The experience and qualifications of the staff involved in the pen test

63. You were able to log on to a user's computer and plant a keystroke logger after you saw the user get up and walk away without logging out or turning off his computer. When preparing your final report, what should you recommend to the client as the best defense to prevent this from happening?

- ❍ **A.** The use of encryption
- ❍ **B.** Instruct users to switch off the computers when leaving or stepping away from the system
- ❍ **C.** Enforcing strict passwords
- ❍ **D.** Implementing screensaver passwords

64. Which of the following can be used to lure attackers away from real servers and allow for their detection?

- ❍ **A.** Honeypots
- ❍ **B.** Jails
- ❍ **C.** IDS systems
- ❍ **D.** Firewalls

65. Which of the following best describes what happens when two message digests produce the same hash?

- ❍ **A.** Fragments
- ❍ **B.** Collisions
- ❍ **C.** Agreements
- ❍ **D.** Hash completion

66. Which of the following is one of the primary ways that people can get past controlled doors?

- ❍ **A.** Shoulder surfing
- ❍ **B.** Piggybacking
- ❍ **C.** Spoofing
- ❍ **D.** Lock picking

67. You are preparing to perform a subnet scan. Which of the following Nmap switches would be useful for performing a UDP scan of the lower 1024 UDP ports?

- ❍ **A.** `Nmap -hU <host(s)>`
- ❍ **B.** `Nmap -sU -p 1-1024 <host(s)>`
- ❍ **C.** `Nmap -u -v -w2 <host> 1-1024`
- ❍ **D.** `Nmap -sS -O target/1024`

68. You are concerned that the target network is running PortSentry to block Nmap scanning. Which of the following should you attempt to bypass their defense?

- ❍ **A.** `Nmap -O <hosts>`
- ❍ **B.** `Nmap -sT -p 1-1024 <hosts>`
- ❍ **C.** `Nmap -s0 -PT -O -T1  <hosts>`
- ❍ **D.** `Nmap -sA  -T1  <hosts>`

69. What is the real reason that WEP is vulnerable?

- ❍ **A.** RC4 is not a real encryption standard.
- ❍ **B.** The 24-bit IV field is too small.
- ❍ **C.** 40-bit encryption was shown to be weak when cracked in the 1980s.
- ❍ **D.** Tools, such as WEPCrack, can brute force WEP by trying all potential keys in just a few minutes.

70. What encryption standard was chosen as the replacement for 3DES?

- ❍ **A.** RC5
- ❍ **B.** ECC
- ❍ **C.** Knapsack
- ❍ **D.** Rijndael

71. You recently used social engineering to talk your way into a secure facility. Which of the following should you recommend in your ethical hacking report as the best defense to prevent this from happening in the future?

- ❍ **A.** Guests are escorted.
- ❍ **B.** Guests are required to wear badges.
- ❍ **C.** Guests must sign in.
- ❍ **D.** Guests are searched before they can enter.

72. This method of transmission operates by taking a broad slice of the bandwidth spectrum and dividing it into smaller subchannels of about 1MHz. The transmitter then hops between subchannels and sends out short bursts of data on each subchannel for a short period of time. What method was just described?

- ❍ **A.** Frequency-hopping spread spectrum (FHSS)
- ❍ **B.** Wired equivalent protection (WEP)
- ❍ **C.** Direct-sequence spread spectrum (DSSS)
- ❍ **D.** Wi-Fi Protected Access (WPA)

73. Which of the following software products is not used to defend against buffer overflows?

- ❍ **A.** Return Address Defender (RAD)
- ❍ **B.** C+
- ❍ **C.** StackGuard
- ❍ **D.** Immunix

74. This type of virus scanning examines computer files for irregular or unusual instructions. Which of the following matches that description?

- ❍ **A.** Integrity checking
- ❍ **B.** Heuristic scanning
- ❍ **C.** Activity blocker
- ❍ **D.** Signature scanning

75. Which of the following is considered the weakest form of DES?

- ❍ **A.** DES ECB
- ❍ **B.** DES CBC
- ❍ **C.** DES CFM
- ❍ **D.** DES OFB

76. Which of the following is the best example of a strong two factor authentication?

- ❍ **A.** A passcard and a token
- ❍ **B.** A token and a pin number
- ❍ **C.** A username and a password
- ❍ **D.** A hand scan and fingerprint scan

77. While looking over data gathered by one of your co-workers, you come across the following data:

```
system.sysDescr.0 = OCTET STRING: "Sun SNMP Agent, "
system.sysObjectID.0 = OBJECT IDENTIFIER: enterprises.42.2.1.1
system.sysUpTime.0 = Timeticks: (5660402) 15:43:24
system.sysContact.0 = OCTET STRING: "System administrator"
system.sysName.0 = OCTET STRING: "unixserver"
system.sysLocation.0 = OCTET STRING: "System admins office"
system.sysServices.0 = INTEGER: 72
interfaces.ifNumber.0 = INTEGER: 2
interfaces.ifTable.ifEntry.ifIndex.1 = INTEGER: 1
interfaces.ifTable.ifEntry.ifIndex.2 = INTEGER: 2
```

What was used to obtain this output?

- ❍ **A.** An Nmap scan
- ❍ **B.** A Nessus scan
- ❍ **C.** An SNMP walk
- ❍ **D.** SolarWinds

78. You found the following information that had been captured by a keystroke log:

```
Type nc.exe > sol.exe:nc.exe
```

What is the purpose of the command?

- ❍ **A.** An attacker is using a wrapper.
- ❍ **B.** An attacker is streaming a file.
- ❍ **C.** An attacker is using a dropper.
- ❍ **D.** An attacker has used a steganographic tool.

79. You're planning on planting a sniffing program on a Linux system but are worried that it will be discovered when someone runs an `ifconfig -a`. Which of the following is your best option for hiding the tool?

- ❍ **A.** Run the tool in stealth mode.
- ❍ **B.** Replace the original version of `ifconfig` with a rootkit version.
- ❍ **C.** Redirect screen output should someone type the `ifconfig` command.
- ❍ **D.** Store the tool in a hidden directory with an ADS.

80. Which of the following is a program used to wardial?

- ❍ **A.** Toneloc
- ❍ **B.** Kismet
- ❍ **C.** SuperScan
- ❍ **D.** NetStumbler

81. Which of the following best describes Tripwire?

- ❍ **A.** It is used as a firewall to prevent attacks.
- ❍ **B.** It is used as an IPS to defend against intruders.
- ❍ **C.** It is used encrypt sensitive files.
- ❍ **D.** It is used to verify integrity.

82. You are preparing to attack several critical servers and perform the following command:

```
net use \\windows_server\ipc$ "" /u:""
```

What is its purpose?

- ❍ **A.** Grabbing the etc/passwd file
- ❍ **B.** Stealing the SAM
- ❍ **C.** Probing a Linux-based Samba server
- ❍ **D.** Establishing a null session

83. Several of your co-workers are having a discussion about the etc/passwd file. They are at odds over what types of encryption are used to secure Linux passwords. Which of the following is the least likely to be used?

- ❍ **A.** Linux passwords can be encrypted with MD5.
- ❍ **B.** Linux passwords can be encrypted with DES.
- ❍ **C.** Linux passwords can be encrypted with Blowfish.
- ❍ **D.** Linux passwords are encrypted with asymmetric algorithms.

84. You noticed the following entry:

```
http://server/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

What is the attacker attempting to do?

- ❍ **A.** DoS the targeted web server
- ❍ **B.** Exploit a vulnerability in a CGI script
- ❍ **C.** Exploit a vulnerability in an Internet Information Server
- ❍ **D.** Gain access on a SQL server

85. You discovered the following in the logs:

```
192.186.13.100/myserver.aspx..%255C..%255C..%255C..%255C..%255C.
.%255C..%255C..%255C..%255C..%255
..c:\winnt\system32\cmd.exe%/c:dir
```

What is the hacker attempting to do?

- ❍ **A.** Directory traversal attack
- ❍ **B.** Buffer overflow
- ❍ **C.** .+htr attack
- ❍ **D.** Execute MS Blaster

86. DES has an effective key length of which of the following?

- ❍ **A.** 48 bit
- ❍ **B.** 56 bit
- ❍ **C.** 64 bit
- ❍ **D.** 128 bit

87. Because of findings discovered during a penetration test, you have been asked to investigate biometric authentication devices. Which of the following would represent the best system to install?

- ❍ **A.** A system with a high CER
- ❍ **B.** A system with a high FAR
- ❍ **C.** A system with a low CER
- ❍ **D.** A system with a high FRR

88. One of your team members has asked you to analyze the following SOA record:

```
ExamCram2.com.SOA NS1.ExamCram2.com pearson.com (200509024 3600
3600 604800 2400)
```

Based on this information, which of the following is the correct TTL?

- ❍ **A.** 200509024
- ❍ **B.** 3600
- ❍ **C.** 604800
- ❍ **D.** 2400

89. Which of the following statements about SSIDs is correct?

- ❍ **A.** The SSID is the same value on all systems.
- ❍ **B.** The SSID is only 32 bits in length.
- ❍ **C.** The SSID is broadcast in clear text.
- ❍ **D.** The SSID and the wireless AP's MAC address will always be the same.

90. While examining a file from a suspected hacker's laptop, you come across the following snippet of code:

```
char linuxcode[]= /* Lam3rZ chroot() code */
 "\x31\xc0\x31\xdb\x31\xc9\xb0\x46\xcd\x80\x31\xc0\x31\xdb"
 "\x43\x89\xd9\x41\xb0\x3f\xcd\x80\xeb\x6b\x5e\x31\xc0\x31"
 "\xc9\x8d\x5e\x01\x88\x46\x04\x66\xb9\xff\xff\x01\xb0\x27"
 "\xcd\x80\x31\xc0\x8d\x5e\x01\xb0\x3d\xcd\x80\x31\xc0\x31"
 "\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9\x31\xc0\x8d"
 "\x5e\x08\xb0\x0c\xcd\x80\xfe\xc9\x75\xf3\x31\xc0\x88\x46"
 "\x09\x8d\x5e\x08\xb0\x3d\xcd\x80\xfe\x0e\xb0\x30\xfe\xc8"
 "\x88\x46\x04\x31\xc0\x88\x46\x07\x89\x76\x08\x89\x46\x0c"
 "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xb0\x0b\xcd\x80\x31\xc0"
 "\x31\xdb\xb0\x01\xcd\x80\xe8\x90\xff\xff\xff\xff\xff\xff"
 "\x30\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31";
#define MAX_FAILED 4
#define MAX_MAGIC 100
static int magic[MAX_MAGIC],magic_d[MAX_MAGIC];
static char *magic_str=NULL;
int before_len=0;
char *target=NULL,*username="ftp",*password=NULL;
```

What is its purpose?

- ❍ **A.** The hex dump of a bitmap picture
- ❍ **B.** A buffer overflow
- ❍ **C.** An encrypted file
- ❍ **D.** A password cracking program

91. Which of the following is considered a vulnerability of SNMP?

- ❍ **A.** Clear text community strings
- ❍ **B.** Its use of TCP
- ❍ **C.** The fact that it is on by default in Windows 2000 server
- ❍ **D.** The fact that it is on by default in Windows XP Professional

92. Disabling which of the following would make your wireless network more secure against unauthorized access?

- ❍ **A.** Wired Equivalent Privacy (WEP)
- ❍ **B.** Media access control (MAC) address filtering
- ❍ **C.** Extensible Authentication Protocol (EAP)
- ❍ **D.** Service Set ID (SSID) broadcasting

93. You are hoping to exploit a DNS server and access the zone records. As such, when does a secondary name server request a zone transfer from a primary name server?

- ❍ **A.** When a secondary SOA serial number is higher than a primary SOA
- ❍ **B.** When a primary name server has had its service restarted
- ❍ **C.** When the TTL reaches 0
- ❍ **D.** When a primary SOA serial number is higher that a secondary SOA

94. Which of the following indicates an ICMP destination unreachable type?

- ❍ **A.** 0
- ❍ **B.** 3
- ❍ **C.** 5
- ❍ **D.** 13

95. This form of antivirus scan looks at the beginning and end of executable files for known virus signatures. Which of the following matches that description?

- ❍ **A.** Integrity checking
- ❍ **B.** Heuristic scanning
- ❍ **C.** Activity blocker
- ❍ **D.** Signature scanning

96. You have successfully run an exploit against an IIS6 server. Which of the following default privileges will you have within the command shell that you have spawned?

- ❍ **A.** Local system
- ❍ **B.** Administrator
- ❍ **C.** IIS default account
- ❍ **D.** IUSR_Computername

97. Which of the following protocols was developed to be used for key exchange?

- ❍ **A.** Diffie-Hellman
- ❍ **B.** MD5
- ❍ **C.** Rijndael
- ❍ **D.** Base64

98. This type of access control system uses subjects, objects, and labels.

- ❍ **A.** DAC
- ❍ **B.** MAC
- ❍ **C.** Kerberos
- ❍ **D.** TACACS

99. Jack is conducting an assessment of a target network. He knows that there are services, such as web and mail, although he cannot get a ping reply from these devices. Which of the following is the most likely reason that he is having difficulty with this task?

- ❍ **A.** A packet filter is blocking ping.
- ❍ **B.** UDP is blocked by the gateway.
- ❍ **C.** The hosts are down.
- ❍ **D.** The TTL value is incorrect.

100. Locks are considered what type of control?

- ❍ **A.** Detective
- ❍ **B.** Preventive
- ❍ **C.** Expanded
- ❍ **D.** Weak

101. Which of the following best describes firewalking?

- ❍ **A.** It's a tool used to discover promiscuous settings on NIC cards, and, as such, it can enumerate firewalls.
- ❍ **B.** It is a technique used to discover what rules are configured on the gateway.
- ❍ **C.** It is a tool used to cause a buffer overflow on a firewall.
- ❍ **D.** It is a technique used to map wireless networks.

102. The art of hiding information in graphics or music files is known as which of the following?

- ❍ **A.** Non-repudiation
- ❍ **B.** Steganography
- ❍ **C.** Hashing
- ❍ **D.** Encryption

103. What is the following Snort rule used for?

```
#alert tcp any any -> $HOME_NET 22 (msg:
➥ "Policy Violation Detected"; dsize: 52; flags: AP;
➥  threshold: type both, track by_src, count 3, seconds 60;
➥  classtype: successful-user; sid:2001637; rev:3; )
```

- ❍ **A.** This rule detects if someone attempts to use FTP.
- ❍ **B.** This rule detects if someone attempts to use Telnet.
- ❍ **C.** This rule detects if someone attempts to use SSH.
- ❍ **D.** This rule detects if someone attempts to use TFTP.

104. What is the purpose of the following Snort rule?

```
alert tcp any any -> 192.168.160.0/24 12345
➥ (msg:"Possible Trojan access";)
```

- ❍ **A.** This rule detects a Subseven scan.
- ❍ **B.** This rule detects a Netbus scan.
- ❍ **C.** This rule detects a Back Orfice scan.
- ❍ **D.** This rule detects a Donald Dick scan.

105. Because of a recent penetration test, you have been asked to recommend a new firewall for a rapidly expanding company You have been asked what type of firewall would be best for the organization if used in conjunction with other products and only needs the capability to statelessly filter traffic by port or IP address.

- ❍ **A.** An access control list implemented on a router
- ❍ **B.** Operating system–based firewall
- ❍ **C.** Host-based firewall
- ❍ **D.** Demilitarized design

106. Which of the following describes programs that can run independently, travel from system to system, and disrupt computer communications?

- ❍ **A.** Trojans
- ❍ **B.** Viruses
- ❍ **C.** Worms
- ❍ **D.** Droppers

107. How many bits does SYSKEY use for encryption?

- ❍ **A.** 48 bits
- ❍ **B.** 56 bits
- ❍ **C.** 128 bits
- ❍ **D.** 256 bits

108. While examining the company's website for vulnerabilities, you received the following error: `Microsoft OLE DB Provider for ODBC Drivers error '80040e14'`. What does it mean?

- ❍ **A.** The site has a scripting error.
- ❍ **B.** The site is vulnerable to SQL injection.
- ❍ **C.** The site is vulnerable to a buffer overflow.
- ❍ **D.** The site has a CGI error.

109. While searching a website, you have been unable to find information that was on the site several months ago. What might you do to attempt to locate that information?

- ❍ **A.** Visit Google's cached page to view the older copy.
- ❍ **B.** Forget about it, as there is no way to find this information.
- ❍ **C.** Visit a partner site of the organization to see if it is there.
- ❍ **D.** Use the wayback machine.

110. What program is used to conceal messages in ASCII text by appending whitespace to the end of lines?

- ❍ **A.** Snow
- ❍ **B.** wget
- ❍ **C.** Blindside
- ❍ **D.** Wrapper

Answers to Practice Exam Questions

1. **D**. Sending a bogus email is one way to find out more about internal servers, gather additional IP addresses, and learn how they treat mail. Answer A is incorrect, as this will not allow you to determine the holder of the root account. Answer B is incorrect, as this will not tell you if the mail server is vulnerable to a relay attack. Answer C is incorrect, as bounced email will not normally trigger an IDS. For more information, see Chapter 3.
2. **C**. Dynamic random ports range from 49152–65535. Most established well-known applications range from 0–1023. Answers A, B, and D are incorrect because well-known ports range from 0–1023, registered ports range from 1024–49151, and dynamic ports range from 49152–65535. For more information, see Chapter 3.
3. **C**. This command is used for banner grabbing. Banner grabbing helps identify the service and version of the web server running. Answer A is incorrect, as this command will not return the web server's home page. Answer B is incorrect because it will not open a backdoor on the IP address specified. Answer D is incorrect, as this command will not allow an attacker to determine if there is a SQL server at the target IP address. For more information, see Chapter 3.
4. **D**. An ACK scan would be the best choice to determine if stateless inspection is being used. If there is an ACL in place, the ACK would be allowed to pass. Answer A is incorrect because an XMAS scan is not used to bypass stateless inspection. It uses an abnormal flag setting. Answer B is incorrect, as an idle scan requires a third idle device and is used because it is considered stealthy. Answer C is incorrect, as a stealth scan simply performs the first two steps of the three-step handshake. For more information, see Chapter 3.

5. **C**. The TTL is the value that would determine how long cache poisoning would last. It is typically found in the SOA record. Answer A is incorrect, as the A record maps a hostname to its IP address. Answer B is incorrect because the CNAME is an alias. Answer D is incorrect because the MX record maps to mail exchange servers. For more information, see Chapter 3.

6. **D**. Beast uses port 6666 and is considered unique because it uses injection technology. Answer A is incorrect, as Subseven uses port 6711. Answer B is incorrect because NetBus uses port 12345, and answer C is incorrect because Amitis uses port 27551. For more information, see Chapter 6.

7. **D**. Wrappers are used to package covert programs with overt programs. They act as a type of file joiner program or installation packager program. Answer A is incorrect because wrappers do not tunnel programs. An example of a tunneling program would be Loki. Answer B is incorrect, as wrappers are not used to cause a Trojan to execute when previewed in email; the user must be tricked into running the program. Answer C is incorrect because wrappers are not used as backdoors. A backdoor program allows unauthorized users to access and control a computer or a network without normal authentication. For more information, see Chapter 6.

8. **A**. Loki is a Trojan that opens and can be used as a backdoor to a victim's computer by using ICMP. Answer B is incorrect because Loki does not use UDP port 69 by default. Answer C is incorrect because Loki does not use TCP port 80 by default. Answer D is incorrect because Loki does not use IGRP. For more information, see Chapter 6.

9. **A**. `Netstat -an` would be the proper syntax. The -a displays all connections and listening ports. The `-n` displays addresses and port numbers in numerical form. Answer B is incorrect, as `-r` displays the routing table. Answer C is incorrect because `-p` shows connections for a specific protocol, although none was specified in the answer. Answer D is incorrect, as `-s` displays per-protocol statistics. By default, statistics are shown for TCP, UDP, and IP. For more information, see Chapter 6.

10. **D**. NetBus uses port 12345 by default. Answers A, B, and C are incorrect because Donald Dick uses 23476, BOK uses port 31337, and Subseven uses port 6711. For more information, see Chapter 6.

11. **D**. 18 USC 1029 makes it a crime to knowingly and intentionally use cellular telephones that are altered or have been cloned. Answer A is incorrect because 18 USC 2701 addresses access to electronic information, answer B is incorrect because 18 USC 2511 addresses interception of data, and answer C is incorrect because 18 USC 2319 addresses copyright issues. For more information, see Chapter 9.

12. **C**. The SSID is a 32-bit character identifier attached to the header of wireless packets that are sent over a wireless LAN. Because the SSID can be sniffed in clear text from the packet, it does not provide any real security. The SSID is used to differentiate one network from another and is used to identify the network. Answer A is incorrect because SSIDs are case sensitive, answer B is incorrect because SSIDs are 32 bits, not 24, and answer D is incorrect because, as mentioned, they are case sensitive and are not 24 bits. For more information, see Chapter 9.

13. **A**. WEP encrypts the wireless packet but not the header; therefore, the MAC addresses will still be visible. Answer B is incorrect, as the IP header will be encrypted. Answer C is incorrect, as the FTP data will be encrypted. Answer D is incorrect, as WEP will not make the network secure from DoS

attacks. A hacker can still jam the network or even launch a deauthentication attack against one of the clients. For more information, see Chapter 9.

14. **D**. EAP-MD5 does not provide server authentication. Answers A, B, and C are incorrect because they do provide this capability. LEAP does so by password hash, and PEAP and EAP-TLS provide authentication with public key technology. For more information, see Chapter 9.

15. **C**. RedFang is used to scan for Bluetooth devices. Answer A is incorrect because Airsnort is an 802.11 wireless tool. Answer B is incorrect, as Aeropeek is a Windows 802.11 wireless sniffer. Answer D is incorrect because Netstumbler is used to find 802.11 wireless devices, not Bluetooth devices. For more information, see Chapter 9.

16. **C**. The commercial application of steganography lies mainly in the use of digital watermark. A digital watermark acts as a type of digital fingerprint and can verify proof of source. Answer A is incorrect because copyrighting the picture would allow her protection, but it might not be enough to prove that the stolen digital photos are hers. Answer B is incorrect, as steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of their existence. Answer D is incorrect because a digital certificate would not prove ownership of the files. For more information, see Chapter 12.

17. **B**. Programs, such as Tripwire, MD5sum, and Windows System File, all rely on hashing. Hashing is performed to verify integrity. Answer A is incorrect because digital certificates are not used by Tripwire, MD5sum, and Windows System File Protection. Digital certificates provide authentication. Answer C is incorrect, as digital signatures provide non-repudiation and are not used in the hashing process. Answer D is incorrect, as steganography is used for file hiding. For more information, see Chapter 12.

18. **C**. The output of an MD5sum is 32 characters long. An example is shown here: `4145bc316b0bf78c2194b4d635f3bd27`. All other answers are incorrect because they do not correctly specify the character length of an MD5sum. For more information, see Chapter 12.

19. **A**. UUencode was developed to aid in the transport of binary images via email. Answer B is incorrect, as Simple Mail Transport Protocol (SMTP) is not an encoding method; it used to send standard email. Answer C is incorrect because XOR is not commonly used to encode email, although it is used for weak password management. Answer D is incorrect because Base64 is not used for email; it is primarily used for weak password management. For more information, see Chapter 12.

20. **A**. MD5 produces a 128-bit hash value. Answer B is incorrect, as 3DES is a symmetric algorithm. Answer C is incorrect because SHA-1 is a hashing algorithm, although it produces a 160-bit hash value. Answer D is incorrect because AES is the advanced encryption standard, which is a symmetric algorithm chosen to replace DES. For more information, see Chapter 12.

21. **B**. A cookie file resides on a client system and can contain data passed from websites so that websites can communicate with this file when the same client returns. Cookie files have caused some issues with respect to privacy because they can be used with form authentication and they can contain passwords. Answers A, C, and D are incorrect. Even though they all relate to a cookie, they do not specifically address the security risks to the user. For more information, see Chapter 8.

22. **C**. This script is insecure because it allows anyone with a username of *customer* and a password of *solutions* to access the customer.html web page. Anyone reading the source code could determine this information. Answer A is incorrect because no PKI is used here, only security by obscurity. Answer B is incorrect because it is part of a page for authentication users. Answer D is incorrect because there are problems, as anyone viewing the source code can see the username and password in clear text. For more information, see Chapter 8.

23. **A**. The WAP gateway is a critical junction because encrypted messages from end customers must be decrypted for transmission to the Internet. If the hacker could hack the gateway, all the data traffic would be exposed. WTLS provides authentication, privacy, and integrity. SSL protects users from sniffing attacks on the Internet, which limits disclosure of the customer's information. Answer B is incorrect, as sniffing in front of the server would only provide encrypted traffic. Answer C is incorrect, as the laptop would not be useful without a username and password. Answer D is incorrect, as the wireless transmission is encrypted. For more information, see Chapter 9.

24. **D**. The true administrator account has a RID of 500. Therefore, answers A, B, and C are incorrect. For more information, see Chapter 4.

25. **B**. The most common definition of a rogue access point is an access point that was set up without permission by the network owners to allow individuals to capture users' wireless MAC addresses. Answer A is incorrect because wardriving is the act of searching for wireless points. Answer C is incorrect, as the purpose of a DoS is specifically to deny service, not to capture information. Answer D is incorrect because Bluejacking involves Bluetooth connections. For more information, see Chapter 9.

26. **B**. By using a write-once CD that cannot be overwritten, the logs are much safer. Answers A, C, and D are incorrect, as write protecting the system log does little to prevent a hacker from deleting or modifying logs because the superuser or administrator can override the write protection. Backup and mirroring could overwrite earlier files and might not be current. Storing the backup does not prevent tampering. For more information, see Chapter 5.

27. **D**. Authentication is not one of the items that is part of the three building blocks of security. Answers A, B, and C are incorrect because they are part of the three basic security items. There are many ways in which security can be achieved, although it's universally agreed that confidentiality, integrity, and availability (CIA) form the basic building blocks of any good security initiative. For more information, see Chapter 1.

28. **A**. A phreaker is a hacker who is skilled in manipulating the phone system. Answers B, C, and D are incorrect, as phreakers don't specialize in social engineering, VoIP, or cryptography. For more information, see Chapter 1.

29. **B**. A threat is any agent, condition, or circumstance that could potentially cause harm, loss, or damage. Answers A, C, and D are incorrect because risk is the probability or likelihood of the occurrence or realization of a threat. A vulnerability is a weakness in the system design, implementation, software, code, or other mechanism. An exploit refers to a piece of software, tool, or technique that takes advantage of a vulnerability, which leads to privilege escalation, loss of integrity, or denial of service on a computer system. For more information, see Chapter 1.

30. **C**. Using a firewall as well as encrypted data is the best example of defense in-depth. Answer A is incorrect because firewalls alone are not an example of defense in-depth. Answer B is incorrect because even though it is a good idea to ensure that a computer center is not marked, it is not an example of defense in-depth. Answer D is incorrect because using firewalls by different vendors is a good example of layered firewall security, and defense in-depth would best be assured if you had both firewall and logical controls. For more information, see Chapter 1.

31. **B**. Sections 1029 and 1030 are the main federal statutes that address computer hacking under U.S. Federal Law. Answers A, C, and D are incorrect, as Sections 2510 and 2701 are part of the Electronic Communication Privacy Act and address information in storage and in transit. For more information, see Chapter 1.

32. **B**. False-negative reporting of uncovered weaknesses means that potential vulnerabilities in the network are not identified and might not be addressed. This would leave the network vulnerable to attack from malicious hackers. Answer A is incorrect because false positives would indicate that defenses are in place but are weak and should be checked. Answer C is incorrect, as non-specific reporting features would not be as serious a discovery as false negatives. Answer D is incorrect, as many vulnerability scanners run only from a specific platform and are not as important as false negatives. For more information, see Chapter 5.

33. **B**. After the SAM has been extracted, you can examine the rightmost portion of the hash. Padding on a password is used when passwords are fewer than eight characters long. Therefore, answers A, C, and D are incorrect. For more information, see Chapter 4.

34. **A**. Wget is used to retrieve HTTP, HTTPS, and FTP files and data. Answers B, C, and D are incorrect because pwdump is used to extract the SAM, dumpsec is used for examining user account details on a Windows system, and Achilles is used to proxy web pages. For more information, see Chapter 8.

35. **D**. Regional registries maintain records from the areas from which they govern. RIPE is responsible for domains served within Europe and therefore would be a good starting point for a .fr domain. Answers A, B, and C are incorrect because AfriNIC is a proposed registry for Africa, ARIN is for North and South America, and APNIC is for Asian and Pacific countries. For more information, see Chapter 8.

36. **D**. Reconnaissance is considered a passive information gathering method. Answers A, B, and C are incorrect because maintaining access is not a passive step; it is active. Maintaining access can be achieved if you use rootkits and sniffers. Covering tracks is also an active attack, as the hacker seeks to hide his activities. For more information, see Chapter 2.

37. **D**. Packet filters cannot keep up with transaction state; therefore, the ACK packets would easily pass. Answer A is incorrect, as not enough information is given to determine if the systems are all Windows based. Answer B is incorrect because not enough information is given to determine if the organization is using an IDS. Answer C is incorrect, as not enough information is given to determine if the systems are all UNIX based. For more information, see Chapter 3.

38. **B**. Encryption is the most secure method to ensure the security of information in transit. Answers A, C, and D are incorrect because they are all less secure methods and still leave open the possibility of interception of traffic. For more information, see Chapter 12.

39. **C**. Cryptcat is an encrypted version of netcat. Answers A, B, and D are incorrect because –v is verbose, -p is for port number, and –e is for execute. None of the options will make the traffic more secure to sniffing. For more information, see Chapter 12.

40. **B**. Paper shredders are an easy option to implement to prevent dumpster divers from retrieving sensitive information. Although answers A, C, and D are all important, shredding is the easiest and most effective fix from the choices given. For more information, see Chapter 13.

41. **D**. Packet replay is a combination of passive and active attacks that can be used to inject packets into the network. Answers A, B, and C are incorrect because eavesdropping is the act of sniffing, message modification is the act of altering a message, and a brute force attack attempts to use all possible combinations. For more information, see Chapter 7.

42. **A**. A IDS system can detect a SYN flood, as there will be a large number of SYN packets appearing on the network without corresponding ACK responses. Answers B, C, and D are incorrect because the source and target IP and port will not be the same, and segment size is not the determining factor in a SYN attack. For more information, see Chapter 7.

43. **C**. TCP port 53 is used for zone transfers. Therefore, answers A, B, and D are incorrect. Port 79 is used by finger, and UDP 53 is usually used for lookups. For more information, see Chapter 3.

44. **B**. In Figure PE.1, the packet shown is targeted to the broadcast address of ff ff ff ff ff ff. Answers A, C, and D are incorrect, as it is not a multicast that would begin with an 01; it is not the default gateway, as that is now a broadcast address, and it is not c0 A8 7B 65. That is the IP address of the originator, 192.168.123.101. For more information, see Chapter 7.

45. **C**. Non-repudiation is the ability to verify proof of identity. It is used to ensure that a sender of data is provided with proof of delivery and the recipient is assured of the sender's identity. Neither party should be able to deny having sent or received the data at a later date. Answers A, B, and D are incorrect, as asymmetric encryption is used primarily for confidentiality, as is symmetric encryption. Hashing is used for integrity. For more information, see Chapter 12.

46. **B**. Your basic padlock that uses a key is a warded lock. These can be picked by inserting a stiff piece of wire or thin strip of metal. They do not provide a high level of security. Answers A, C, and D are incorrect, as cipher, device, and tumbler locks are considered more robust than warded locks. For more information, see Chapter 13.

47. **A**. By default, IIS 4.0 (inetinfo.exe) is configured to run in the local System account context. Answers B, C, and D are incorrect, as they do not properly specify the user privilege. For more information, see Chapter 8.

48. **C**. An idle scan uses the IP ID number to allow for a truly blind scan of a target. It simply reads the current value of the IP ID to determine if the port was open or closed when the zombie made the probe. Answer A is incorrect, as an idle scan does not tweak the datagram size. Answer B is incorrect, as the TCP segment size is not altered. Answer D is incorrect, as the TCP ACK number is not manipulated during an idle scan. For more information, see Chapter 3.

49. **C**. To ensure a sender's authenticity and an email's confidentiality, first encrypt the hash of the message with the sender's private key and then encrypt the message with the receiver's public key. This is the only correct combination; therefore, answers A, B, and D are incorrect. For more information, see Chapter 12.

50. **C**. MD5 is a hashing algorithm and, as such, is used for integrity; it produces a 128-bit output. Answer A is incorrect, as DES is a symmetric encryption standard. Answer B is incorrect, as Diffie-Hellman is used for key distribution. Answer D is incorrect, as AES is the symmetric standard used to replace DES. For more information, see Chapter 12.

51. **B**. Cipher locks can use keypads or smart locks to control access into restricted areas. Answers A, C, and D are incorrect because warded locks are the weakest form of padlock, device locks are used to secure equipment, and tumbler locks are more complex than warded locks and offer greater security. For more information, see Chapter 13.

52. **D**. The packet shown in Figure PE.2 is a Windows ping packet. That can be determined by examining the ASCII portion of the packer that displays `"a, b, c, d, e, f, g ..."`. Answers, A, B, and C are incorrect because the ICMP packet was not generated by Loki, it is not a Linux packer, and there is enough information to tell, as the entire packet is shown. For more information, see Chapter 3.

53. **C**. The first user account has a RID of 1000. Answer A is incorrect because it is not a valid RID. Answer B is incorrect because it is the RID of the administrator. Answer D is incorrect because it is the RID of the second user account. For more information, see Chapter 4.

54. **C**. N-Stealth is a Windows-based scanner used to scan on port 80 for web server vulnerabilities. Answer A is incorrect because Nessus runs on Linux; answer B is incorrect because Etheral is a sniffer, not a vulnerability scanner; and answer D is incorrect because Whisker can be run on Linux or Windows clients. For more information, see Chapter 5.

55. **C**. Basic64 provides very weak security as it performs encoding, not encryption. Answers A, B, and D are incorrect because DES, RC5, and AES are all much stronger. For more information, see Chapter 12.

56. **D**. Eight feet should deter a determined intruder. Three strands of topping of barbed wire can be added and pointed out at a 45° angle. Answers A, B, and C are incorrect. Four and five feet are only causal deterrent, whereas 6 foot is hard to climb. Eight feet is needed for effective security. For more information, see Chapter 12.

57. **B**. Loki is a covert channel tool that can be used to set up a covert server and client that will transmit information in ICMP ping packets. Answers A, C, and D are incorrect because Netbus is a Trojan, Fpipe is a port redirection tool, and Sid2User is used for enumeration. For more information, see Chapter 6.

58. **C**. A Land DoS sends packets with the same source and destination address. Answers A, B, and D are incorrect, as a ping of death uses large ICMP ping packets, Smurf is targeted to a broadcast address, and Targa is a DDOS attack. For more information, see Chapter 7.

59. **C**. There are two basic methods to overcome the functionality of a switch. One of these is ARP poisoning. Answers A, B, and D are incorrect because MAC flooding, ICMP redirection, and IP forwarding are not supported by Cain. For more information, see Chapter 7.

60. **D**. RC5 is a block-based symmetric cipher in which the number of rounds can range from 0–255, and the key can range from 0 to 2040 bits in size. Answers A, B, and C are incorrect because they are examples of asymmetric algorithms. For more information, see Chapter 12.

61. **A**. MAC flooding and ARP poisoning are the two ways that switches are attacked for active sniffing. Answers, B, C, and D are incorrect because MAC flooding seeks to overflow the switch's CAM. For more information, see Chapter 12.

62. **C**. The most critical item is the involvement of the client organization. It must be involved to determine what kind of test should occur and what the organization's most critical assets are. Answers A, B, and D are incorrect. Even though they are important, management's involvement is the most important. Penetration testing without management approval could reasonably be considered criminal in many jurisdictions. For more information, see Chapter 1.

63. **D**. Screensaver passwords are an easy way to ensure end user security. These can be used as a effective security control. Answer A is incorrect because it would be of no help in this situation. Answer B is incorrect because it would not ensure that users actually logged off systems. Answer C is incorrect because it would not prevent the occurrence in the question from happening. For more information, see Chapter 13.

64. **A**. A honeypot can be used to lure attackers away from real servers and allow for their detection. Answers B, C, and D are incorrect. Jails are not an adequate description of what is actually a honeypot. An IDS would not help in luring an attacker. A firewall can be used to prevent attacks or to limit access, but will not hold or lure an attacker. For more information, see Chapter 10.

65. **B**. Collisions occur when two message digests produce the same hash value. Attackers can use this vulnerability to make an illegitimate item appear genuine. This is not something that should easily occur. Answers A, C, and D are incorrect, as fragments, agreements, and hash completion are not the proper terms for when two message digests produce the same hash value. For more information, see Chapter 12.

66. **B**. Piggybacking is the primary way that someone would try to bypass a mantrap. To prevent and detect this, guards and CCTV can be used. Answer A is incorrect because shoulder surfing is done to steal passwords. Answer C is incorrect because spoofing is pretending to be someone else, and answer D is incorrect because lock picking is not the most common way to bypass access. For more information, see Chapter 13.

67. **B**. `Nmap -sU -p 1-1024 <host(s)>` is the proper syntax for performing a Nmap UDP scan. Learning Nmap and its uses are critical for successful completion of the CEH exam. Answers A, C, and D are incorrect because they are not the correct switches. `-hU` and `-u` are invalid, and `-sS` is used for stealth scanning. For more information, see Chapter 3.

68. **D**. PortSentry may not be able to pick up an ACK scan as the program is looking for a startup connection sequence. Answer A is incorrect as a fingerprint "-O" scan relies on one open and one closed port. When PostSentry detects such a scan it will block access from the requesting IP address. Answer B is incorrect as PortSentry will detect and log a notice saying this IP has been blocked and will subsequently ignor this activity. Answer C is incorrect as a –sO is an IP protocol scan and looks for IP header values.

69. **B**. The 24-bit IV field is too small because of this, and key reusage, WEP is vulnerable. Answer A is incorrect because RC4 is not too small. Answer C is incorrect because while 40 bits is not overly strong, it was not cracked in the 1980s. Answer D is incorrect because tools such as WEPCrack must capture millions of packets before it can crack the WEP key. For more information, see Chapter 9.

70. **D**. In 2002, NIST decided on the replacement for DES. Rijndael was the chosen replacement. Rijndael is an iterated block cipher that supports variable key and block lengths of 128, 192, or 256 bits. Answer A is incorrect because it is a symmetric encryption standard but is not the replacement for DES. Answer B is incorrect because it is an asymmetric encryption standard. Answer incorrect because it is also a asymmetric encryption standard and, as such, is not the replacement for DES. For more information, see Chapter 12.

71. **A**. The best defense to having individuals illegally physically enter a facility is by requiring them to be escorted. Answers B, C, and D are incorrect because they are not the best defense, but badges and sign-in sheets are recommended. Searching guests might not be socially or legally acceptable. For more information, see Chapter 13.

72. **A**. FHSS is a method of transmission that operates by taking a broad slice of the bandwidth spectrum and dividing it into smaller subchannels of about 1MHz. The transmitter then hops between subchannels, sending out short bursts of data on each subchannel for a short period of time. Answer B is incorrect because WEP is not a transmission method. It is a means of protection. Answer C is incorrect because DSSS is a method of transmission that 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. Answer D is incorrect, as it is an improved method of protecting wireless transmissions that replaced WEP. For more information, see Chapter 9.

73. **B**. C language is one of the languages that is more vulnerable to buffer overflows, and their use may actually increase the chance of buffer overflow. Answers A, C, and D are incorrect because Return Address Defender (RAD), StackGuard, and Immunix are all software products that can be used to defend against buffer overflows. For more information, see Chapter 11.

74. **B**. Heuristic scanning examines computer files for irregular or unusual instructions. Therefore, answers A, C, and D are incorrect because integrity checking, activity blocking, and signature scanning do not work in that way. For more information, see Chapter 11.

75. **A**. DES electronic code book (ECB) produces the highest throughput but is the easiest form of DES to break. The same plaintext encrypted with the same key will always produce the same ciphertext. CBC, CFM, and OFB are all more secure; therefore, answers B, C, and D are incorrect. For more information, see Chapter 12.

76. **B**. Two factor authentication requires that you use two of the three authentication types such as a token, something you have, and a pin, something you know. Answers A, C, and D are incorrect, as each only represents one form of authentication. For more information, see Chapter 12.

77. **C**. The output is from an SNMP walk. SNMP is used to remotely manage a network and hosts/devices on the network. It contains a lot of information about each host that probably shouldn't be shared. Answers A, B, and D are incorrect because Nmap scan would not include this type of information, nor would Nessus. Solar Winds is used for SNMP discovery but is a GUI tool. For more information, see Chapter 3.

78. **B**. When using NTFS, a file consists of different data streams. Streams can hold security information, real data, or even a link to information instead of the real data stream. This link allows attackers to hide data that cannot easily be found on an NTFS drive. Answer A is incorrect because a

wrapper is used to hide a Trojan; answer C is incorrect because a dropper is used to hide a virus; and answer D is incorrect because the example shown is not a steganographic tool. For more information, see Chapter 4.

79. **B**. Your best option would be to replace the original version of ifconfig with a rootkit version. Answer A is incorrect, as a stealth setting will not keep the program from being discovered. Answer C is incorrect, as screen redirection will not help. Answer D is not possible, as ADS is only on Windows NTFS drives. For more information, see Chapter 5.

80. **A**. Toneloc is a wardialing program, whereas Kismet and Netstumbler are used for wardriving. Superscan is a port scanning program. For more information, see Chapter 9.

81. **D**. Tripwire is a file integrity program and, as such, makes answers A, B, and C incorrect. For more information, see Chapter 10.

82. **D**. The net use statement shown in this question is used to establish a null session. This will enable more information to be extracted from the server. Answer A is incorrect because it is not used to attack the passwd file. Answer B is incorrect because it is not used to steal the SAM. Answer C is incorrect because it is not used to probe a Linux server. For more information, see Chapter 4.

83. **D**. Linux passwords are encrypted with symmetric passwords; therefore, answer D is correct. Answers A, B, and C are incorrect. DES, MD5, or Blowfish are valid password encryption types. For more information, see Chapter 5.

84. **B**. PHF is a cgi program that came with many web servers such as Apache. It had a parsing problem such that you could execute arbitrary commands on the web server host as the web server user. Answers A, C, and D are incorrect because a PHF attack does not DoS the server, is not a vulnerability in IIs, and does not target SQL. For more information, see Chapter 8.

85. **A**. This is an example of a directory traversal attack. It is not a buffer overflow, .+htr, or MS Blaster; therefore answers B, C, and D are incorrect. For more information, see Chapter 8.

86. **B**. DES has an effective key length of 56 bits; eight bits are used for parity. As it is symmetric encryption, it uses the same key to encrypt and decrypt. Answers A, C, and D are incorrect because DES does not use a 48-, 64-, or 128-bit key. For more information, see Chapter 12.

87. **C**. The accuracy of a biometric device is going to be determined by several items. The false rejection rate (FRR), which is the number of times a legitimate user is denied access. Its false acceptance rate (FAR) is the number of times unauthorized individuals can gain access. The point on a graph at which these two measurements meet is known as the crossover error rate (CER). The lower the CER, the better. Therefore, answers A, B, and D are incorrect. For more information, see Chapter 13.

88. **D**. The SOA includes a timeout value. Among other things, this informs a hacker how long DNS poisoning would last. 2400 seconds is 40 minutes. Answers A, B, and C are incorrect because those fields do not display the timeout value. For more information, see Chapter 2.

89. **C**. The SSID is set on the wireless AP and broadcast to all wireless devices in range. Answers A, B, and D are incorrect. The SSID is not 32 bits; it is 32 characters: it is not the same on all devices and does not match the MAC. For more information, see Chapter 9.

90. **B**. The code shown in this question was taken from a WUFTP buffer overflow program. The code is not a hex dump, which should be visible, as it is C code; it is not an encrypted file and is not used for password cracking; therefore, A, C, and D are incorrect. For more information, see Chapter 11.

91. **A**. The use of cleartext community strings, such as public and private, is a huge vulnerability of SNMP. Answers B, C, and D are incorrect. SNMP does not use TCP, and is not on in Windows 2003 by default. Being turned off in Windows 2000 would be considered a good thing. For more information, see Chapter 3.

92. **D**. Disabling SSID broadcasting adds security by making it more difficult for hackers to find the name of the access point. Answers A, B, and C are incorrect, as disabling WEP, MAC filtering, or LEAP would make the wireless network more vulnerable. For more information, see Chapter 9.

93. **D**. When the serial number within the SOA record of the primary server is higher than the serial number in the SOA record of the secondary DNS server, a zone transfer will take place; therefore, answers A, B, and C are incorrect. For more information, see Chapter 2.

94. **B**. A type 3 is an ICMP destination unreachable. Answers A, C, and D are incorrect because type 0 is aping, type 5 is a redirect, and type 13 is a timestamp request. For more information, see Chapter 11.

95. **D**. Signature scanning antivirus software looks at the beginning and end of executable files for known virus signatures. Answers A, B, and C do not describe that type of scanning. Heuristics looks at usual activity, integrity looks at changes to hash values, and activity blocks known virus activity. For more information, see Chapter 11.

96. **D**. Windows 2003 IIS 6.0 is more secure than earlier versions and is configured to run as in the lower access IUSR_Computername account. Answers A, B, and C are incorrect because they do not properly specify the user privilege. For more information, see Chapter 8.

97. **A**. Diffie-Hellman was developed for key exchange protocol. It is used for key exchange in Secure Sockets Layer (SSL) and IPSec. It is extremely valuable in that it allows two individuals to exchange keys who have not communicated with each other before. Answers B, C, and D are incorrect because they are not examples of key exchange protocols. For more information, see Chapter 12.

98. **B**. When a subject attempts to access an object, the label is examined for a match to the subject's level of clearance. If a match is found, access is allowed. Answers A, C, and D are incorrect because they do not use subjects, objects, and labels. For more information, see Chapter 13.

99. **A**. The most likely reason is that the packet filter is blocking ping. This is a common practice with many organizations. Answers B, C, and D are incorrect because UDP is probably not the cause of the problem, the web server would most likely be up, and it is unlikely that this is caused by the TTL. For more information, see Chapter 12.

100. **B**. Locks are a preventative control, and although they might not keep someone from breaking in, they do act as a deterrent and slow the potential loss. Answers A, C, and D are incorrect because they are not primarily a detective control. Weak and expanded controls are just distracters. For more information, see Chapter 13.

101. **B**. Firewalk is a network security tool that attempts to determine what the ruleset is on a firewall. It works by sending out TCP and UDP packets with a TTL configured one greater than the targeted firewall. Answers A, C, and D are incorrect because Firewalk is not used to determine NIC settings, used for buffer overflows, or used for mapping wireless networks. For more information, see Chapter 10.

102. **B**. With steganography, messages can be hidden in image files, sound files, or even the whitespace of a document before being sent. Answers A, C, and D are incorrect because they do not describe steganography. For more information, see Chapter 12.

103. **C**. Snort is a popular open source IDS service. The rule shown in the question is used to detect if SSH is being used. Locating the target port of 22 should have helped in this summation. Therefore, answers A, B, and D are incorrect because FTP is port 21, Telnet is port 22, and TFTP is port 69. For more information, see Chapter 10.

104. **B**. Snort can be a powerful IDS. The rule shown in the question triggers on detection of a Netbus scan. Netbus defaults to port 12345. Answers A, C, and D are incorrect. Subseven, BackOrfice, and DonaldDick do not use that port by default. For more information, see Chapter 10.

105. **A**. An access control list implemented on a router is the best choice for a stateless firewall. Most organizations already have the routers in place to perform such services, so this type of protection can be added for little additional cost. Answers B, C, and D are incorrect because they represent more expensive options and offer more than stateless inspection. For more information, see Chapter 10.

106. **C**. Worms are replicating programs that can run independently and travel from system to system. Answer A is incorrect because a Trojan typically gives someone else control of the system. Answer B is incorrect because viruses do not run independently. Answer D is incorrect because a dropper is used with a virus. For more information, see Chapter 11.

107. **C**. SYSKEY was added in Windows NT (SP3) to add a second layer id 128-bit encryption. As such, answers A, B, and D are incorrect. For more information, see Chapter 4.

108. **B**. SQL Injection is a subset of an unverified/unsanitized user input vulnerability. The idea is to convince the application to run SQL code that was not intended. Therefore, answers A, C, and D are incorrect because they do not describe SQL injection. For more information, see Chapter 8.

109. **D**. Archive.org maintains the wayback machine that preserves copies of many websites from months or years ago. Answers A, B, and C are incorrect because none of these methods offer much hope in uncovering the needed information. For more information, see Chapter 8.

110. **A**. Snow is used to conceal messages in ASCII text by appending whitespace to the end of lines. Spaces and tabs are not usually visible in document viewer programs; therefore, the message is effectively hidden from casual observers. Answer B is incorrect because wget is used to copy web pages. Answer C is incorrect because Blindside is used to hide text in graphics files, and answer D is incorrect because a wrapper is used with Trojans to make their installation easy. For more information, see Chapter 12.