1. While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

   A. Clickjacking

   B. Cross-Site Scripting

   C. Cross-Site Request Forgery

   D. Web form input validation

2. Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

   A. LDAP Injection attack

   B. Cross-Site Scripting (XSS)

   C. SQL injection attack

   D. Cross-Site Request Forgery (CSRF)

3. User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

   A. Application

   B. Transport

   C. Session

   D. Presentation

4. If you want to only scan fewer ports than the default scan using Nmap tool, which option would you use?

A. -r

B. -F

C. -P

D. –sP

5. Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

   A. SOA

   B. biometrics

   C. single sign on

   D. PKI

6. If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

   A. Traceroute

   B. Hping

   C. TCP ping

   D. Broadcast ping

7. Which is the first step followed by Vulnerability Scanners for scanning a network?

   A. OS Detection

   B. Firewall detection

   C. TCP/UDP Port scanning

   D. Checking if the remote host is alive

8. Which of the following programs is usually targeted at Microsoft Office products?

   A. Polymorphic virus

   B. Multipart virus

   C. Macro virus

   D. Stealth virus

9. Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

   A. 113

   B. 69

   C. 123

   D. 161

10. Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

    A. Nikto

    B. John the Ripper

    C. Dsniff

    D. Snort

11. DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed. What command is used to determine if the entry is present in DNS cache?

    A. nslookup -fullrecursive update.antivirus.com

    B. dnsnooping -rt update.antivirus.com

    C. nslookup -norecursive update.antivirus.com

D. dns --snoop update.antivirus.com

12. Which of the following is an extremely common IDS evasion technique in the web world?

    A. Spyware

    B. Subnetting

    C. Unicode Characters

    D. Port Knocking

13. John the Ripper is a technical assessment tool used to test the weakness of which of the following?

    A. Passwords

    B. File permissions

    C. Firewall rulesets

    D. Usernames

14. During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?

    A. Circuit

    B. Stateful

    C. Application

    D. Packet Filtering

15. By using a smart card and pin, you are using a two-factor authentication that satisfies

    A. Something you are and something you remember

    B. Something you have and something you know

C. Something you know and something you are

D. Something you have and something you are

16. Which of the following is the best countermeasure to encrypting ransomwares?

    A. Use multiple antivirus softwares

    B. Pay a ransom

    C. Keep some generation of off-line backup

    D. Analyze the ransomware to get decryption key of encrypted data

17. Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?

    A. tcpsplice

    B. Burp

    C. Hydra

    D. Whisker

18. You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly. What is the best Nmap command you will use?

    A. nmap -T4 -q 10.10.0.0/24

    B. nmap -T4 -F 10.10.0.0/24

    C. nmap -T4 -r 10.10.1.0/24

    D. nmap -T4 -O 10.10.0.0/24

19. Which of the following is the BEST way to defend against network sniffing?

    A. Using encryption protocols to secure network communications

    B. Register all machines MAC Address in a Centralized Database

    C. Use Static IP Address

    D. Restrict Physical Access to Server Rooms hosting Critical Servers

20. Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

    A. Iris patterns

    B. Voice

    C. Height and Weight

    D. Fingerprints

21. Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?

    A. SFTP

    B. Ipsec

    C. SSL

    D. FTPS

22. To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

    A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit

    B. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit

C. if (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit

D. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

23. You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL. What may be the problem?

    A. Traffic is Blocked on UDP Port 53

    B. Traffic is Blocked on TCP Port 80

    C. Traffic is Blocked on TCP Port 54

    D. Traffic is Blocked on UDP Port 80

24. Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a Linux platform?

    A. Kismet

    B. Abel

    C. Netstumbler

    D. Nessus

25. You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8. While monitoring the data, you find a high number of outbound connections. You see that IPs owned by XYZ (Internal) and private IPs are communicating to a Single Public IP. Therefore, the Internal IPs are sending data to the Public IP. After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised. What kind of attack does the above scenario depict?

    A. Botnet Attack

    B. Spear Phishing Attack

    C. Advanced Persistent Threats

D. Rootkit Attack

26. A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named inc. The FTP servers access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP servers software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port. What kind of vulnerability must be present to make this remote attack possible?

    A. File system permissions

    B. Privilege escalation

    C. Directory traversal

    D. Brute force login

27. Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?

    Code:

    #include <string.h> int main(){ char buffer[8];

    strcpy(buffer, 1111111111111111111111111111);} Output: Segmentation fault

    A. C#

    B. Python

    C. Java

    D. C++

28. Internet Protocol Security IPsec is actually a suite pf protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.

    A. Protect the payload and the headers

    B. Encrypt

    C. Work at the Data Link Layer

D. Authenticate

29. An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

    A. Make sure that legitimate network routers are configured to run routing protocols with authentication.

    B. Disable all routing protocols and only use static routes

    C. Only using OSPFv3 will mitigate this risk.

    D. Redirection of the traffic cannot happen unless the admin allows it explicitly.

30. Which method of password cracking takes the most time and effort?

    A. Dictionary attack

    B. Shoulder surfing

    C. Rainbow tables

    D. Brute force

31. An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gain access to the DNS server and redirect the direction www.google.com to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

    A. MAC Flooding

    B. Smurf Attack

    C. DNS spoofing

    D. ARP Poisoning

32. An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

    A. Reverse Social Engineering

    B. Tailgating

    C. Piggybacking

    D. Announced

33. Which of the following is the best countermeasure to encrypting ransomwares?

    A. Use multiple antivirus softwares

    B. Keep some generation of off-line backup

    C. Analyze the ransomware to get decryption key of encrypted data

    D. Pay a ransom

34. An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", that the user is directed to a phishing site. Which file does the attacker need to modify?

    A. Boot.ini

    B. Sudoers

    C. Networks

    D. Hosts

35. Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

    A. Produces less false positives

    B. Can identify unknown attacks

    C. Requires vendor updates for a new threat

    D. Cannot deal with encrypted network traffic

36. You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line. Which command would you use?

    A. c:\gpedit

    B. c:\compmgmt.msc

    C. c:\ncpa.cp

    D. c:\services.msc

37. In Wireshark, the packet bytes panes show the data of the current packet in which format?

    A. Decimal

    B. ASCII only

    C. Binary

    D. Hexadecimal

38. PGP, SSL, and IKE are all examples of which type of cryptography?

    A. Hash Algorithm

    B. Digest

    C. Secret Key

    D. Public Key

39. Which of the following is considered as one of the most reliable forms of TCP scanning?

    A. TCP Connect/Full Open Scan

    B. Half-open Scan

    C. NULL Scan

    D. Xmas Scan

40. Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

    A. ICMP Echo scanning

    B. SYN/FIN scanning using IP fragments

    C. ACK flag probe scanning

    D. IPID scanning

41. Which of the following is the BEST way to defend against network sniffing?

    A. Restrict Physical Access to Server Rooms hosting Critical Servers

    B. Use Static IP Address

    C. Using encryption protocols to secure network communications

    D. Register all machines MAC Address in a Centralized Database

42. You have successfully gained access to a Linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by Network-Based Intrusion Detection Systems (NIDS). What is the best way to evade the NIDS?

    A. Out of band signaling

    B. Protocol Isolation

    C. Encryption

    D. Alternate Data Streams

43. What is the purpose of a demilitarized zone on a network?

    A. To scan all traffic coming through the DMZ to the internal network

    B. To only provide direct access to the nodes within the DMZ and protect the network behind it

    C. To provide a place to put the honeypot

D. To contain the network devices you wish to protect

44. You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

    A. All three servers need to be placed internally

    B. A web server facing the Internet, an application server on the internal network, a database server on the internal network

    C. A web server and the database server facing the Internet, an application server on the internal network

    D. All three servers need to face the Internet so that they can communicate between themselves

45. When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

    A. Identifying operating systems, services, protocols and devices

    B. Modifying and replaying captured network traffic

    C. Collecting unencrypted information about usernames and passwords

    D. Capturing a network traffic for further analysis

46. A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application. What kind of Web application vulnerability likely exists in their software?

    A. Cross-site scripting vulnerability

    B. Web site defacement vulnerability

    C. SQL injection vulnerability

    D. Cross-site Request Forgery vulnerability

47. Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned. Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

    A. "GET/restricted/goldtransfer?to=Rob&from=1 or 1=1”HTTP/1.1Host: westbank.com"

    B. "GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com"

    C. "GET/restricted/bank.getaccount(“Ned”) HTTP/1.1 Host: westbank.com"

    D. "GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"

48. A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer’s software and hardware without the owner’s permission. Their intention can either be to simply gain knowledge or to illegally make changes. Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

    A. White Hat

    B. Suicide Hacker

    C. Gray Hat

    D. Black Hat

49. You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user’s password or activate disabled Windows accounts?

    A. John the Ripper

    B. SET

    C. CHNTPW

    D. Cain & Abel

50. What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

    A. Cross-site request forgery

    B. Cross-site scripting

    C. Session hijacking

    D. Server side request forgery

51. You are doing an internal security audit and intend to find out what ports are open on all the servers. What is the best way to find out?

    A. Scan servers with Nmap

    B. Scan servers with MBSA

    C. Telnet to every port on each server

    D. Physically go to each server

52. Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?

    A. Honeypots

    B. Firewalls

    C. Network-based intrusion detection system (NIDS)

    D. Host-based intrusion detection system (HIDS)

53. Which protocol is used for setting up secure channels between two devices, typically in VPNs?

    A. PPP

    B. IPSEC

    C. PEM

    D. SET

54. Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

    A. SHA-2

    B. SHA-3

    C. SHA-1

    D. SHA-0

55. If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

    A. Traceroute

    B. Hping

    C. TCP ping

    D. Broadcast ping

56. Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?

    A. Bootrom Exploit

    B. iBoot Exploit

    C. Sandbox Exploit

    D. Userland Exploit

57. The "white box testing" methodology enforces what kind of restriction?

    A. Only the internal operation of a system is known to the tester.

    B. The internal operation of a system is completely known to the tester.

C. The internal operation of a system is only partly accessible to the tester.

D. Only the external operation of a system is accessible to the tester.

58. Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

    A. SQL injection attack

    B. Cross-Site Scripting (XSS)

    C. LDAP Injection attack

    D. Cross-Site Request Forgery (CSRF)

59. The following is part of a log file taken from the machine on the network with the IP address of 192.168.0.110: What type of activity has been logged?

    A. Teardrop attack targeting 192.168.0.110

    B. Denial of service attack targeting 192.168.0.105

    C. Port scan targeting 192.168.0.110

    D. Port scan targeting 192.168.0.105

60. Bob, your senior colleague, has sent you a mail regarding aa deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bob denies that he had ever sent a mail. What do you want to "know" to prove yourself that it was Bob who had send a mail?

    A. Confidentiality

    B. Integrity

    C. Non-Repudiation

    D. Authentication

61. What is attempting an injection attack on a web server based on responses to True/False questions called?

    A. DMS-specific SQLi

    B. Compound SQLi

    C. Blind SQLi

    D. Classic SQLi

62. The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?

    A. ACK

    B. SYN

    C. RST

    D. SYN-ACK

63. You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity. What tool would you most likely select?

    A. Snort

    B. Nmap

    C. Cain & Abel

    D. Nessus

64. Which of the following will perform an Xmas scan using NMAP?

    A. nmap -sA 192.168.1.254

    B. nmap -sP 192.168.1.254

    C. nmap -sX 192.168.1.254

    D. nmap -sV 192.168.1.254

65. Code injection is a form of attack in which a malicious user:

    A. Inserts text into a data field that gets interpreted as code

    B. Gets the server to execute arbitrary code using a buffer overflow

    C. Inserts additional code into the JavaScript running in the browser

    D. Gains access to the codebase on the server and inserts new code

66. Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?

    A. [cache:]

    B. [site:]

    C. [inurl:]

    D. [link:]

67. This asymmetry cipher is based on factoring the product of two large prime numbers. What cipher is described above?

    A. SHA

    B. RSA

    C. MD5

    D. RC5

68. Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules. Which of the following types of firewalls can protect against SQL injection attacks?

    A. Data-driven firewall

    B. Stateful firewall

    C. Packet firewall

D. Web application firewall

69. Which of the following attacks exploits web age vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend?

    A. Command Injection Attacks

    B. File Injection Attack

    C. Cross-Site Request Forgery (CSRF)

    D. Hidden Field Manipulation Attack

70. Which is the first step followed by Vulnerability Scanners for scanning a network?

    A. TCP/UDP Port scanning

    B. Firewall detection

    C. OS Detection

    D. Checking if the remote host is alive

71. Alice encrypts her data using her public key PK and stores the encrypted data in the cloud. Which of the following attack scenarios will compromise the privacy of her data?

    A. None of these scenarios compromise the privacy of Alice's data

    B. Agent Andrew subpoenas Alice, forcing her to reveal her private key. However, the cloud server successfully resists Andrew's attempt to access the stored data

    C. Hacker Harry breaks into the cloud server and steals the encrypted data

    D. Alice also stores her private key in the cloud, and Harry breaks into the cloud server as before

72. You perform a scan of your company's network and discover that TCP port 123 is open. What services by default run on TCP port 123?

    A. Telnet

B. POP3

C. Network Time Protocol

D. DNS

73. Based on the below log, which of the following sentences are true? Mar 1, 2016, 7:33:28 AM 10.240.250.23 "" 54373 10.249.253.15 "" 22 tcp_ip

A. SSH communications are encrypted it’s impossible to know who is the client or the server

B. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server

C. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server

D. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the server

74. Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool

B. Create a disk imageof a clean Windows installation

C. Check MITRE.org for the latest list of CVE findings

D. Used a scan tool like Nessus

75. Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGI's?

A. Snort

B. Dsniff

C. Nikto

D. John the Ripper

76. You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

    A. Host-based IDS

    B. Firewall

    C. Network-Based IDS

    D. Proxy

77. Which of the following protocols is used for exchanging routing information between two gateways in a network of autonomous systems?

    A. IGMP

    B. ICMP

    C. EGP

    D. OSPF

78. Which of the following is an attack on a website that changes the visual appearance of the site and seriously damages the trust and reputation of the website?

    A. Website defacement

    B. Zero-day attack

    C. Spoofing

    D. Buffer overflow

79. What does the term “Ethical Hacking” mean?

    A. Someone who is hacking for ethical reasons.

    B. Someone who is using his/her skills for ethical reasons.

    C. Someone who is using his/her skills for defensive purposes.

    D. Someone who is using his/her skills for offensive purposes.

80. What is the essential difference between an ‘Ethical Hacker’ and a ‘Cracker’?

    A. The ethical hacker does not use the same techniques or skills as a cracker.

    B. The ethical hacker does it strictly for financial motives unlike a cracker.

    C. The ethical hacker has authorization from the owner of the target.

    D. The ethical hacker is just a cracker who is getting paid.

81. A very useful resource for passively gathering information about a target company is:

    A. Host scanning

    B. Whois search

    C. Traceroute

    D. Ping sweep

82. Which Type of scan sends a packets with no flags set ?

    A. Open Scan

    B. Null Scan

    C. Xmas Scan

    D. Half-Open Scan

83. Which of the following commands runs snort in packet logger mode?

    A. ./snort -dev -h ./log

    B. ./snort -dev -l ./log

    C. ./snort -dev -o ./log

    D. ./snort -dev -p ./log

84. Samantha has been actively scanning the client network for which she is doing a vulnerability assessment test. While doing a port scan she notices ports open in the 135 to 139 range. What protocol is most likely to be listening on those ports?

    A. SMB

    B. FTP

    C. SAMBA

    D. FINGER

85. Which of the following tools is used to perform a credential brute force attack?

    A. Hydra

    B. John the Ripper

    C. Hashcat

    D. Peach

86. Which of the following attacks specifically impact data availability?

    A. DDoS

    B. Trojan

    C. MITM

    D. Rootkit

87. A penetration tester is crawling a target website that is available to the public. Which of the following represents the actions the penetration tester is performing?

    A. URL hijacking

    B. Reconnaissance

    C. White box testing

    D. Escalation of privilege

88. How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

    A. 128

    B. 64

    C. 32

    D. 16

89. In the context of file deletion process, which of the following statement holds true?

    A. When files are deleted, the data is overwritten and the cluster marked as available

    B. The longer a disk is in use, the less likely it is that deleted files will be overwritten

    C. While booting, the machine may create temporary files that can delete evidence

    D. Secure delete programs work by completely overwriting the file in one go

90. Which part of the Windows Registry contains the user's password file?

    A. HKEY_LOCAL_MACHINE

    B. HKEY_CURRENT_CONFIGURATION

    C. HKEY_USER

    D. HKEY_CURRENT_USER

91. When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

    A. Universal Time Set

B. Network Time Protocol

C. SyncTime Service

D. Time-Sync Protocol

92. What happens when a file is deleted by a Microsoft operating system using the FAT file system?

A. only the reference to the file is removed from the FAT

B. the file is erased and cannot be recovered

C. a copy of the file is stored and the original file is erased

D. the file is erased but can be recovered

93. What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?

A. rootkit

B. key escrow

C. steganography

D. Offset

94. If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

A. The system files have been copied by a remote attacker

B. The system administrator has created an incremental backup

C. The system has been compromised using a t0rnrootkit

D. Nothing in particular as these can be operational files

95. The efforts to obtain information before a trial by demanding documents, depositions, questions and answers written under oath, written requests for admissions of fact, and examination of the scene is a description of what legal term?

    A. Detection

    B. Hearsay

    C. Spoliation

    D. Discovery

96. What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?

    A. Every byte of the file(s) is given an MD5 hash to match against a master file

    B. Every byte of the file(s) is verified using 32-bit CRC

    C. Every byte of the file(s) is copied to three different hard drives

    D. Every byte of the file(s) is encrypted using three different methods

97. What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

    A. Cracks every password in 10 minutes

    B. Distribute processing over 16 or fewer computers

    C. Support for Encrypted File System

    D. Support for MD5 hash verification

98. An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

    A. Smurf

    B. Ping of death

    C. Fraggle

D. Nmap scan

99. When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

A. FF D8 FF E0 00 10

B. FF FF FF FF FF FF

C. FF 00 FF 00 FF 00

D. EF 00 EF 00 EF 00

100. Where does Encase search to recover NTFS files and folders?

A. MBR

B. MFT

C. Slack space

D. HAL