Exam Code: 1D0-470

Exam Name: CIW SECURITY PROFESSIONAL

Vendor: CIW

Version: DEMO

Part: A

1: What is the final step in assessing the risk of network intrusion from an internal or external source?
A.Using the existing management and control architecture
B.Evaluating the existing perimeter and internal security
C.Analyzing, categorizing and prioritizing resources
D.Considering the business concerns
Correct Answers: A

2: While assessing the risk to a network, which step are you conducting when you determine whether the network can differentiate itself from other networks?
A.Considering the business concerns
B.Analyzing, categorizing and prioritizing resources
C.Evaluating the existing perimeter and internal security
D.Using the existing management and control architecture
Correct Answers: C

3: Which service, tool or command allows a remote or local user to learn the directories or files that are accessible on the network?
A.Traceroute
B.Share scanner
C.Port scanner
D.Ping scanner
Correct Answers: B

4: Which type of attack uses a database or databases to guess a password in order to gain access to a computer system?
A.Hijacking attack
B.Virus attack
C.Dictionary attack
D.Man-in-the-middle attack
Correct Answers: C

5: Your IDS application paged you at 3:00 a.m. and informed you that an attack occurred against your DNS server. You drive to the server site to investigate. You find no evidence of an attack, although the IDS application claims that a remote DNS server waged an attack on port 53 of your intranet DNS server. You check the logs and discover that a zone transfer has occurred. You check your zones and name resolution, and discover that all entries exist, and no unusual entries have been added to the database. What has most likely occurred?
A.A DNS poisoning attack against your internal DNS server
B.A denial-of-service attack against your internal DNS server
C.A false positive generated by the IDS
D.A malfunction of the internal name server

Correct Answers: C

6: Your company allows end-user employees to work from home. Aside from antivirus protection and login through a secure VPN, which tool can help your work-at-home employees to protect their systems at home?
A.A tunneling application
B.A personal firewall
C.Tripwire scripts
D.Updated connection services
Correct Answers: B

7: What host-level information would you want to obtain so you can exploit defaults and patches?
A.Servers
B.Routers and switches
C.Databases
D.Firewall types
Correct Answers: A

8: Which type of attack occurs when a hacker obtains passwords and other information from legitimate transactions?
A.Man-in-the-middle attack
B.Denial-of-service attack
C.Dictionary attack
D.Illicit server attack
Correct Answers: A

9: In a typical corporate environment, which of the following resources demands the highest level of security on the network?
A.Purchasing
B.Engineering
C.Sales
D.Accounting
Correct Answers: D

10: When assessing the risk to a machine or network, what step should you take first?
A.Analyzing, categorizing and prioritizing resources
B.Evaluating the existing perimeter and internal security
C.Checking for a written security policy
D.Analyzing the use of existing management and control architecture
Correct Answers: C

11: Andreas visited an e-commerce site and bought a new mouse pad with his credit card for $5.00 plus shipping and handling. He never received the mouse pad so he called his credit card company to cancel the transaction. He was not charged for the mouse pad, but he was charged for several

other items he did not purchase. He tried to revisit the same e-commerce site but could not find it. Which type of hacking attack occurred?
A.Denial-of-service attack
B.Hijacking attack
C.Illicit server attack
D.Targa attack
Correct Answers: B

12: A hacker has just changed information during a zone transfer. This attack caused false information to be passed on to network hosts as if it were legitimate. Which type of server is the target in such an attack?
A.An e-mail server
B.A DNS server
C.A router
D.An FTP server
Correct Answers: B

13: Which service, tool or command provides information about administrators, domain name servers, additional domains and physical locations?
A.Whois
B.Ping scanner
C.Host
D.Traceroute
Correct Answers: A

14: What common target can be reconfigured to disable interfaces and provide inaccurate IP addresses over the Internet?
A.Routers
B.E-mail servers
C.DNS servers
D.Databases
Correct Answers: A

15: Which of the following do hackers target because it usually communicates in cleartext, and because it often carries sensitive information?
A.Router
B.DNS server
C.FTP server
D.E-mail server
Correct Answers: D

16: Which service, command or tool discovers the IP addresses of all computers or routers between two computers on an Internet/intranet network?
A.Whois

B.Port scanner
C.Traceroute
D.Nslookup
Correct Answers: C

17: Which of the following targets is more vulnerable to hacking attacks because of its location in relation to the firewall?
A.DNS server
B.FTP server
C.E-mail server
D.Router
Correct Answers: B

18: Raul wants to know where to find encrypted passwords in a secured Linux server. Where is this information located on the hard drive?
A./etc/shadow
B./etc/passwd
C./.secure/etc/shadow
D./etc/security/shadow
Correct Answers: A

19: Lucy obtains the latest stable versions of servers, services or applications. Which type of attack does this action help to prevent?
A.Dictionary attack
B.Buffer overflow attack
C.Trojan attack
D.Illicit server attack
Correct Answers: B

20: What is the most secure policy for a firewall?
A.To reject all traffic unless it is explicitly permitted
B.To accept all traffic unless it is explicitly rejected
C.To enable all internal interfaces
D.To enable all external interfaces
Correct Answers: A