

Exam : CIW 1D0-470

Title : CIW SECURITY PROFESSIONAL

Update : Demo

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: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: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: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: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: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: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: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: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: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: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: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: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: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: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: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: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: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: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: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:A

21.Helga's Web server is placed behind her corporate firewall. Currently, her firewall allows only VPN connections from other remote clients and networks. She wants to open the Internet-facing interface on her firewall so that it allows all users on the Internet to access her Web server. Which of the following must Helga's rule contain?

- A.Instructions allowing all UDP connections with a destination port of 80 and a source port of 1024
- B.Instructions allowing all UDP connections with a source port of 80 on the external interface and a destination port of 1024
- C.Instructions allowing all TCP connections with a source port of 80 on the internal interface and a destination port of 80
- D.Instructions allowing all TCP connections with a source port higher than 1024 and a destination port of 80

Correct:D

22.Which type of attack can use a worm or packet sniffer to crash systems, reducing resources and/or consuming bandwidth?

- A.Denial-of-service attack
- B.Illicit server attack
- C.Man-in-the-middle attack
- D.Virus attack

Correct:A

23.Which choice lists the ports used by Microsoft internal networking that should be blocked from outside access?

- A.UDP 137 and 138, and TCP 139
- B.Ports 11, 112 and 79
- C.UDP 1028, 31337 and 6000
- D.Port 80, 134 and 31337

Correct:A

24.What is the major security issue with standard NIS (Network Information System)?

- A.It is impossible to enforce a centralized login scheme.
- B.NIS provides no authentication requirement in its native state.
- C.There is no way to encrypt data being transferred.
- D.NIS is a legacy service used only in older, less secure operating systems and networks.

Correct:C

25.What is problematic about a new NTFS partition?

- A.The "everyone" group has unrestricted access permissions on the new partition, thus restricting access to the new partition becomes problematic.
- B.NTFS cannot read user/group permission tables on FAT systems, thus the group permission file must be kept in the same file format as the new partition.
- C.The "admin" group has exclusive access to the new partition, thus getting client machines to see the new partitions can be problematic.
- D.NTFS allows only the root user to access it, thus it is difficult to divide the new partition.

Correct:A

26.Helga is logging on to her network. Her network does not employ traffic padding mechanisms. Why will it be easy for someone to steal her password?

- A.Because her password could be more than two weeks old
- B.Because of the predictability of the login length and password prompts
- C.Because the cleartext user name and password are not encrypted
- D.Because there is no provision for log analysis without traffic padding, thus no accountability when passwords are lost

Correct:B

27.Andreas wants to choose a strong password for his computer. Which of the following should he include in his password?

- A.A mixture of uppercase and lowercase letters, symbols and numbers
- B.An arcane phrase only he can remember
- C.An incorrect spelling of a word or a phrase
- D.A mixture of random words that form non-sense

Correct:A

28.Why is password lockout an effective deterrent to cracking attempts?

- A.Passwords cannot be changed through brute-force methods.
- B.A limited number of login attempts before lockout reduces the number of guesses the potential cracker can make.
- C.Passwords protected in this manner are impossible to find because they are locked out of the main flow of information on the WAN.
- D.Password lockout provides no real improvement over traditional locking methods.

Correct:B

29.What is the difference between digital signature mechanisms and simple encryption?

- A.Digital signatures generally use 128-bit encryption, whereas simple encryption generally uses 56 bits.
- B.Digital signatures are verified by third parties that vouch for the veracity of the sender and the contents.
- C.Digital signatures carry timestamps, whereas standard encryption does not.
- D.Standard encryption mechanisms have no provision for traffic padding to thwart password sniffers.

Correct:B

30.Why would a Windows NT/2000 administrator place the operating system, the program files and the data on different, discrete directories?

- A.To avoid confusion and duplication of upgrades between applications and the operating system
- B.To enhance security by modifying permissions for each resource as needed
- C.To restrict users from accidentally overwriting critical files (if they fill their home directories to capacity), which makes the operating system vulnerable to hacker attacks
- D.To keep the operating system partition from becoming overwhelmed with user program libraries and DLLs

Correct:B