CIW 1D0-470

CIW 1D0-470 CIW SECURITY PROFESSIONAL

Practice Test

Version 2.0

QUESTION NO: 1

What is the best way to prevent employees on a LAN from performing unauthorized activities or other mischief?

A. Reduce each user's permissions to the minimum needed to perform the tasks required by his or her job
B. Limit thenumber of files that any one user can have open at any given time
C. Limit the number of user logins available to one at a time
D. Implement a strict policy to dismiss employees who load games or other unauthorized software on the company's computers

Answer: A

QUESTION NO: 2

Which port does FTP use for a control connection?

A. 162
B. 21
C. 53
D. 25

Answer: B

QUESTION NO: 3

What host-level information would you want to obtain so you can exploit defaults and patches?

A. Servers
B. Databases
C. Routers and switches
D. Firewall types

Answer: A

QUESTION NO: 4

When assessing the risk to a machine or network, what step should you take first?

A. Evaluating the existing perimeter and internal security
B. Analyzing the use of existing management and control architecture

C. Checking for a written security policy
D. Analyzing, categorizing and prioritizing resources

Answer: C

QUESTION NO: 5

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 there is no provision for log analysis without traffic padding, thus no accountability when passwords are lost
C. Because thecleartext user name and password are not encrypted
D. Because of the predictability of the login length and password prompts

Answer: D

QUESTION NO: 6

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

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

Answer: C

QUESTION NO: 7

What is included in the formula that Windows NT/2000 uses to create the security identifier?

A. A semi-random number generated by the CPU based on the number of processes in the queue
B. The computer name and the current amount of CPU time used by the user mode
C. The octal encryption of the user name and the password
D. A set of numbers based on the serial number of the computer CPU and the serial number of Windows NT

Answer: B

QUESTION NO: 8

You want to secure your SMTP transmissions from sniffing attacks. How can you accomplish this?

A. Use strict bounds checking on arrays.
B. Use an SSL certificate.
C. Enforce masquerading.
D. Forbid relaying.

Answer: B

QUESTION NO: 9

Tavo wants to check the status of failed Telnet-based login attempts on a Linux machine he administers. Which shell command can he use to see only that information?

A. grep login /var/log/messages
B. more /etc/passwd
C. cat /etc/passwd > newfile.txt
D. more /var/log/secure

Answer: A

QUESTION NO: 10

Which service, tool or command allows a remote or local user to learn the directories or files that are accessible on the network?

A. Port scanner
B. Traceroute
C. Share scanner
D. Ping scanner

Answer: C

QUESTION NO: 11

Which type of attack occurs when a hacker obtains passwords and other information from legitimate transactions?

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

Answer: D

QUESTION NO: 12

Which service, command or tool allows a remote user to interface with a system as if he were sitting at the terminal?

A. Host
B. Chargen
C. Finger
D. Telnet

Answer: D

QUESTION NO: 13

What common target can be reconfigured to disable interfaces and provide inaccurate IP addresses over the Internet?

A. E-mail servers
B. Routers
C. Databases
D. DNS servers

Answer: B

QUESTION NO: 14

At which layer of the OSI/RM do packet filters function?

A. Transport layer
B. Data link layer
C. Physical layer
D. Network layer

Answer: D

QUESTION NO: 15

Which of the following is a way to get around a firewall to intrude into a secure network from a remote location?

A. Modem banks
B. Identified network topology
C. Active ports
D. Active IP services

Answer: A

QUESTION NO: 16

Which port does FTP use for a control connection?

A. 21
B. 53
C. 25
D. 162

Answer: A

QUESTION NO: 17

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

Answer: D

QUESTION NO: 18

When assessing the risk to a machine or network, what step should you take first?

A. Evaluating the existing perimeter and internal security
B. Analyzing, categorizing and prioritizing resources
C. Analyzing the use of existing management and control architecture
D. Checking for a written security policy

Answer: D

QUESTION NO: 19

How are servers able to conduct a simple authentication check using DNS?

A. RARP
B. Forward DNS lookup
C. Reverse DNS lookup
D. Nslookup

Answer: C

QUESTION NO: 20

Which of the following is the most desirable goal that UNIX system crackers typically hope to achieve?

A. To gain root privileges
B. To be able to write a message on the compromised computer's Web page
C. To be able to plant a virus that will wipe out the entire user database
D. To alter the /var/log/messages file and thus escape detection

Answer: A

QUESTION NO: 21

Which port or ports are used for SMTP?

A. 25

B. 20 and 21
C. 53
D. 161 and 162

Answer: A

QUESTION NO: 22

In a typical corporate environment, which of the following resources demands the highest level of security on the network?

A. Accounting
B. Engineering
C. Sales
D. Purchasing

Answer: A

QUESTION NO: 23

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

A. To keep the operating system partition from becoming overwhelmed with user program libraries and DLLs
B. To avoid confusion and duplication of upgrades between applications and the operating system
C. To enhance security by modifying permissions for each resource as needed
D. 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

Answer: C

QUESTION NO: 24

What is the name of the risk assessment stage in which you bypass login accounts and passwords?

A. Control
B. Penetration
C. Activation
D. Discovery

Answer: B

QUESTION NO: 25

Tavo is documenting all of his network attributes. He wants to know the type of network-level information that is represented by the locations of access panels, wiring closets and server rooms. Which of the following is the correct term for this activity?

A. Router and switch designation
B. IP service routing
C. War dialing
D. Network mapping

Answer: D

QUESTION NO: 26

Which port does FTP use for a control connection?

A. 162
B. 21
C. 25
D. 53

Answer: B

QUESTION NO: 27

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. Analyzing, categorizing and prioritizing resources
B. Using the existing management and control architecture
C. Evaluating the existing perimeter and internal security
D. Considering the business concerns

Answer: C

QUESTION NO: 28

Lucy obtains the latest stable versions of servers, services or applications. Which type of attack does this action help to prevent?

A. Trojan attack
B. Dictionary attack
C. Illicit server attack
D. Buffer overflow attack

Answer: D

QUESTION NO: 29

What is the most secure policy for a firewall?

A. To enable all internal interfaces
B. To reject all traffic unless it is explicitly permitted
C. To enable all external interfaces
D. To accept all traffic unless it is explicitly rejected

Answer: B

QUESTION NO: 30

Which type of attack uses a database or databases to guess a password in order to gain access to a computer system?

A. Dictionary attack
B. Man-in-the-middle attack
C. Hijacking attack
D. Virus attack

Answer: A

QUESTION NO: 31

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

A. To enhance security by modifying permissions for each resource as needed
B. 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