Exam : **1D0-570**

Title : CIW v5 Security Professional Exam

Version : DEMO

1. The chief operations officer (COO) has questioned the need for end-user training. Which of the following is the most effective response?
A.Indicate that you will not be responsible for the next virus outbreak.
B.Remind the CEO about the last virus attack and the expense incurred.
C.Explain that the cost of end-user training is a fraction of the cost of the last security breach caused by end users.
D.Provide statistics that definitively show how end-user training reduces the likelihood of security breaches on the corporate network.
Answer: C

2. Consider the following sequence:
user1@zeppelin:/public$ su -
root@zeppelin:# chmod 1777 /public
root@zeppelin:# exit
Which of the following most accurately describes the result of this command?
A.Only the root user can create and delete files in the /public directory.
B.All users can create, delete and read files in the /public directory, but only root has execute permissions.
C.All users can create and read files in the /public directory, but only root can delete another user's file.
D.Any user can create files in the / directory, but no user can delete a file in this directory unless root permissions are obtained.
Answer: C

3. What is the first step of a gap analysis?
A.Scan the firewall.
B.Review antivirus settings.
C.Review the security policy.
D.Review intrusion-detection software settings.
Answer: C

4. Consider the following firewall rules:
Incoming traffic:
TCP Port 25
TCP Port 139: Denied
UDP Port 137: Denied
UDP Port 138: Denied
ICMP echo request: Denied
ICMP echo reply: Denied
Outgoing traffic:
TCP Ports 1024 through 65,535 to port 80: Denied
TCP Port 80: Denied
ICMP echo request: Denied
ICMP echo reply: Denied
TCP Port 139: Denied

UDP Port 137: Denied
UDP Port 138: Denied
All company production servers reside behind the corporate firewall. However, you discover that the Web server performance is very low. After sniffing the traffic to the Web server, you learn that the Web server is experiencing a distributed denial-of-service attack in which millions of ping packets are being directed at the server. Which of the following is the most plausible explanation for this situation?
A.There is a flaw in the firewall rule set.
B.The firewall is not configured to block ICMP packets generated by the ping command.
C.The attack is originating from a wireless access point (WAP) connected to the corporate network.
D.The attack is originating from a Web server that has not been properly updated, and which has been infected with a Trojan horse.
Answer: C

5. A Linux system running Apache Server has received millions of SYN packets that it can no longer respond to, because the client's operator is maliciously withholding thenecessary reply packet. What is the most common solution for this problem?
A.Implement SSL.
B.Implement SYN cookie support.
C.Upgrade the TCP/IP stack with new software.
D.Upgrade the operating system to support IPsec.
Answer: B

6. Two routers in your company network require a firmware upgrade. Which of the following upgrade strategies will reduce downtime?
A.Conducting the upgrade while the routers are still running
B.Upgrading the routers using the latest upgrade software
C.Conducting the upgrade after rebooting the router
D.Upgrading the routers after business hours
Answer: D

7. You and your team have created a security policy document that is 120 pages long. Which of the following techniques will help ensure that upper-level managers read the essential policy elements?
A.Including a sign-off sheet
B.Including an executive summary
C.Using bold type to emphasize essential elements
D.Using italic type to emphasize essential elements
Answer: B

8. Which of the following is a main function of a company's information security policy?
A.It obligates the IT department to basic services.
B.It defines basic responsibilities for all stakeholders.
C.It defines the responsibilities of employees and managers.
D.It defines basic responsibilities for executive management.
Answer: B

9. After consulting with the IT department, you have determined that a particular security solution is quite effective for protecting a particular resource, but not necessary due to the expense. Which of the following was conducted to enable this conclusion?
A.Risk analysis
B.Cost-to-benefit analysis
C.Physical security analysis
D.Resource priority analysis
Answer: B

10. You want to learn more about a security breach that was recently discovered in a Windows server. Which organization should you consult?
A.ISO
B.SANS
C.CERT
D.IETF
Answer: C

11. Your supervisor asks you to recommend a firewall. The firewall must provide the following services: The ability to filter specific traffic types (e.g., HTTP, SIP, POP3)
User authenticationWeb page caching for later use Which type of firewall would you recommend?
A.Proxy
B.Stateful
C.Packet filter
D.Circuit-based
Answer: A

12. Which type of firewall provides a DMZ?
A.Dual-homed
B.Router-based
C.Single-homed
D.Screened-subnet
Answer: D

13. Company employees have noticed that the quality of voice calls on their Cisco IP phones is greatly reduced at various times during the day. After investigating the problem, you notice that the times when voice quality is reduced coincides with heavy e-mail traffic. Which of the following can you implement on the firewall to alleviate this problem?
A.Stateful inspection
B.Quality of Service (QoS)
C.Network address translation (NAT)
D.Resource Reservation Protocol (RSVP)
Answer: B

14. Consider the following firewall rules:
Incoming traffic:
TCP Port 25: Denied
TCP Port 139: Denied
UDP Port 137: Denied
UDP Port 138: Denied
ICMP echo request: Denied
ICMP echo reply: Denied
Outgoing traffic:
TCP Ports 1024 through 65,535 to port 80: Denied
ICMP echo request: Denied
ICMP echo reply: Denied
TCP Port 139: Denied
UDP Port 137: Denied
UDP Port 138: Denied
All company production servers reside behind the corporate firewall. However, you discover that the Web server
performance is very low. After sniffing the traffic to the Web server, you learn that the Web server is experiencing a distributed denial-of-service attack in which millions of ping packets are being directed at the server. Which is the most plausible explanation for this situation?
A.There is a flaw in the firewall rule set.
B.The attack is being conducted from an internal host.
C.The Web server has been infected with a Trojan horse.
D.The firewall is not configured to block ICMP packets generated by the ping command.
Answer: B

15. A packet is being sent from one computer to the next. This packet is being processed by an application designed to encrypt sensitive data. One of the duties of this application is to ensure that a packet has not been altered by an intruder. Which type of encryption is this application most likely to use to achieve this goal?
A.One-time pad
B.Hash encryption
C.Symmetric-key encryption
D.Asymmetric-key encryption
Answer: B

16. Which of the following is responsible for encrypting the data packets encapsulated in an SSL-enabled HTTP session?
A.One-way encryption
B.One-time pad (OTP)
C.Symmetric-key encryption
D.Asymmetric-key encryption
Answer: C

17. You have used an application called PGP to protect the contents of an e-mail message. Which technology is used to encrypt the key that protects the data in the e-mail message?
A.Symmetric-key encryption
B.Asymmetric-key encryption
C.Diffie-Hellman key exchange protocol
D.Advanced Encryption Standard (AES)
Answer: B

18. Your Web browser issued a warning message that a certificate has not been signed by a recognized authority.
This fact indicates that:
A.an attack is in progress.
B.the ensuing session will not be encrypted.
C.the Certificate Authority (CA) has revoked the certificate.
D.the browser does not recognize the Certificate Authority (CA).
Answer: D

19. A device that provides voice and fax services between your local LAN and the Internet has been installed in the DMZ of your network. However, you cannot send or receive faxes. Which of the following steps is most likely going to solve this problem, while still protecting your network resources?
A.Configure the fax device to use the T.441 protocol.
B.Configure your firewall to allow the T.38 protocol.
C.Move the fax device off the firewall and make it directly accessible to the Internet.
D.Configure your firewall to forward all UDP-based packets from the Internet to the company PBX.
Answer: B

20. Employee computers have been attacked repeatedly. The attacker appears to be working internally, and has been able to scan internal systems for weaknesses. Which of the following will best help you stop these attacks?
A.Installing Webcams
B.Upgrading antivirus software
C.Installing desktop firewalls
D.Establishing a regular auditing schedule
Answer: C