Latest Version: 6.0

Question: 1

What would be the result if you were the recipient of a SYN flood or malformed packet?
Response:

A. You would be unable to access a legitimate service, such as establishing a network connection.
B. The files on your boot sector would be replaced with infected code.
C. A virus would be unleashed on your system at the time the SYN flood or malformed packet was received.
D. You would be misdirected to a fraudulent Web site without your knowledge or consent.

Answer: A

Question: 2

At what layer of the OSI/RM does a packet filter operate?
Response:

A. Layer 1
B. Layer 3
C. Layer 5
D. Layer 7

Answer: B

Question: 3

You have determined that an attack is currently underway on your database server. An attacker is currently logged in, modifying data. You want to preserve logs, caching and other data on this affected server.
Which of the following actions will best allow you to stop the attack and still preserve data?
Response:

A. Pull the server network cable
B. Shut down the server
C. Back up the system logs
D. Force an instant password reset

Answer: A

Question: 4

Which of the following constitutes a problem when conducting a reverse scan?
Response:

A. IP address spoofing
B. SYN floods
C. Default settings on target systems
D. An older system kernel

Answer: A

Question: 5

Which type of encryption poses challenges to key transport?
Response:

A. Asymmetric-key encryption
B. Hash encryption
C. Symmetric-key encryption
D. Diffie-Hellman

Answer: C

Question: 6

Your firewall is configured to forbid all internal traffic from going out to the Internet. You want to allow internal clients to access all Web traffic. At a minimum, what ports must you open in regards to the internal systems?
Response:

A. TCP Port 80 and all ports above 1023
B. TCP Ports 80 and 443, and all ports above 1023
C. All TCP ports above 80 and below 1023
D. TCP Ports 80 and 443

Answer: B

Question: 7

How do activity logs help to implement and maintain a security plan?
Response:

A. Activity logs provide advice on firewall installation, because they enable network baseline creation.
B. Activity logs remind users to log on with strong passwords, because the logs can be analyzed to see if users are complying with policy.
C. Activity logs allow you to determine if and how an unauthorized activity occurred.
D. Activity logs dissuade would-be hackers from breaching your security.

Answer: C

Question: 8

Which of the following is a primary auditing activity?
Response:

A. Encrypting data files
B. Changing login accounts
C. Checking log files
D. Configuring the firewall

Answer: C

Question: 9

Which two protocols can be found at the transport layer of the TCP/IP stack?
Response:

A. File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP)
B. Internet Protocol (IP) and Internet Control Message Protocol (ICMP)
C. Post Office Protocol 3 (POP3) and Simple Mail Transfer Protocol (SMTP)
D. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

Answer: D

Question: 10

To implement a successful security system, you should:
Response:

A. use as many security principles and techniques as you can to protect each resource.

B. place your firewall and network in a public area so that authorized users have easy access to them to solve problems as they occur.
C. implement beta software and operating systems that hold the promise of enhanced security measures.
D. find a product that can offer full protection against all threats.

Answer: A