GAQM

CPEH-001 Exam

GAQM Certified Professional Ethical Hacker (CPEH) Exam

Questions & Answers
Demo

Version: 4.0

Question: 1

Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

A. Configure Port Security on the switch
B. Configure Port Recon on the switch
C. Configure Switch Mapping
D. Configure Multiple Recognition on the switch

Answer: A

Question: 2

Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database. What technique does Jimmy use to compromise a database?

A. Jimmy can submit user input that executes an operating system command to compromise a target system
B. Jimmy can gain control of system to flood the target system with requests, preventing legitimate users from gaining access
C. Jimmy can utilize an incorrect configuration that leads to access with higher-than expected privilege of the database
D. Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system

Answer: D

Question: 3

This IDS defeating technique works by splitting a datagram (or packet) into multiple fragments and the IDS will not spot the true nature of the fully assembled datagram. The datagram is not reassembled until it reaches its final destination. It would be a processor-intensive task for IDS to reassemble all fragments itself, and on a busy system the packet will slip through the IDS onto the network. What is this technique called?

A. IP Routing or Packet Dropping

B. IDS Spoofing or Session Assembly
C. IP Fragmentation or Session Splicing
D. IP Splicing or Packet Reassembly

Answer: C

Question: 4

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.
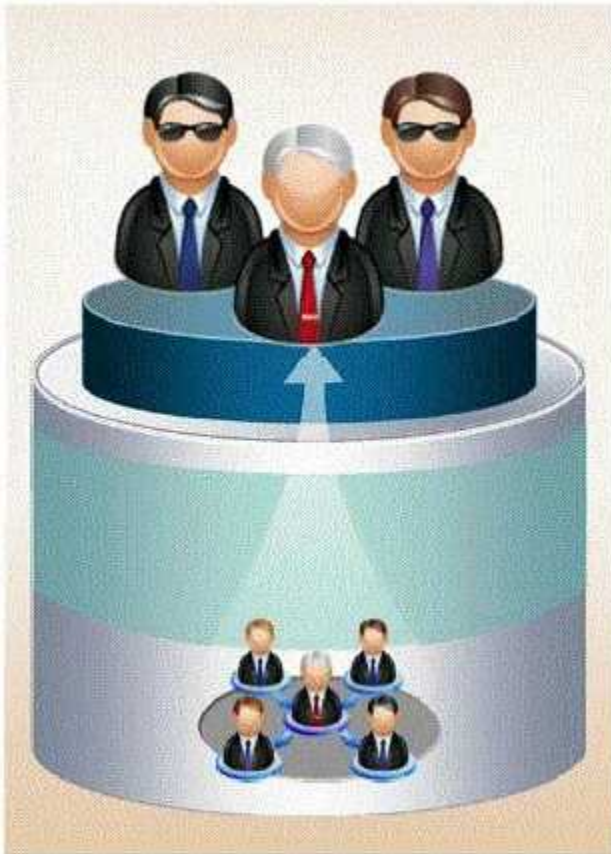
How would you prevent such type of attacks?

A. It is impossible to block these attacks
B. Hire the people through third-party job agencies who will vet them for you
C. Conduct thorough background checks before you engage them
D. Investigate their social networking profiles

Answer: C

Question: 5

This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.

A. UDP Scanning
B. IP Fragment Scanning
C. Inverse TCP flag scanning
D. ACK flag scanning

Answer: B

Question: 6

Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate. How would you call this type of activity?

A. Dumpster Diving
B. Scanning
C. CI Gathering
D. Garbage Scooping
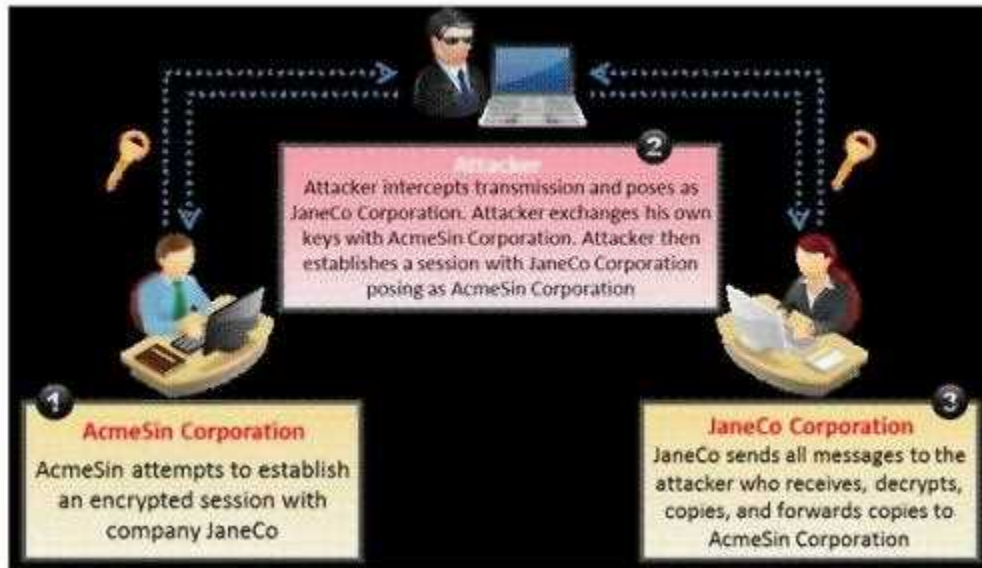
Answer: A

Question: 7

Anonymizer sites access the Internet on your behalf, protecting your personal information from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you, enabling you to remain at least one step removed from the sites you visit. You can visit Web sites without allowing anyone to gather information on sites visited by you. Services that provide anonymity disable pop-up windows and cookies, and conceal visitor's IP address. These services typically use a proxy server to process each HTTP request. When the user requests a Web page by clicking a hyperlink or typing a URL into their browser, the service retrieves and displays the information using its own server. The remote server (where the requested Web page resides) receives information on the anonymous Web surfing service in place of your information. In which situations would you want to use anonymizer? (Select 3 answers)

A. Increase your Web browsing bandwidth speed by using Anonymizer
B. To protect your privacy and Identity on the Internet
C. To bypass blocking applications that would prevent access to Web sites or parts of sites that you want to visit.
D. Post negative entries in blogs without revealing your IP identity

Answer: B, C, D

Question: 8

What type of attack is shown in the following diagram?

A. Man-in-the-Middle (MiTM) Attack
B. Session Hijacking Attack
C. SSL Spoofing Attack
D. Identity Stealing Attack

Answer: A

Question: 9

Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him ''just to double check our records.'' Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.'s computers with a valid user name and password, to steal the cookie recipe. What kind of attack is being illustrated here?

A. Reverse Psychology
B. Reverse Engineering
C. Social Engineering
D. Spoofing Identity
E. Faking Identity

Answer: C

Question: 10

How do you defend against ARP Spoofing? Select three.

A. Use ARPWALL system and block ARP spoofing attacks
B. Tune IDS Sensors to look for large amount of ARP traffic on local subnets
C. Use private VLANS
D. Place static ARP entries on servers, workstation and routers

Answer: A, C, D

Explanation:
ARPwall is used in protecting against ARP spoofing.
Incorrect answer:
IDS option may works fine in case of monitoring the traffic from outside the network but not from internal hosts.