EC-Council EC1-350

Ethical Hacking and Countermeasures V7

Version: 4.4

Topic 1, Volume A

QUESTION NO: 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
Explanation:

QUESTION NO: 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 anoperating 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 withhigher-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
Explanation:

QUESTION NO: 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?

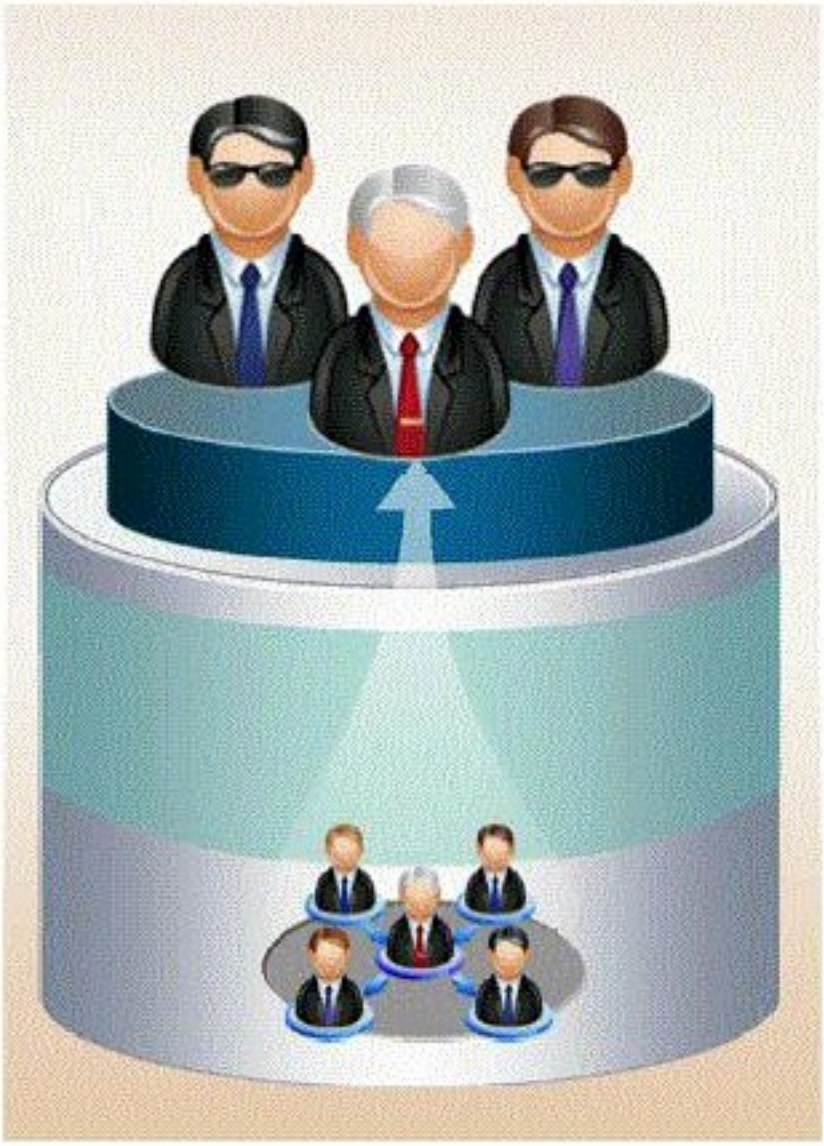
A. IP Routing or Packet Dropping
B. IDS Spoofing or Session Assembly
C. IP Fragmentation or Session Splicing
D. IP Splicing or Packet Reassembly

Answer: C

Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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. IPFragment Scanning
C. Inverse TCP flag scanning
D. ACK flag scanning

Answer: B
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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.

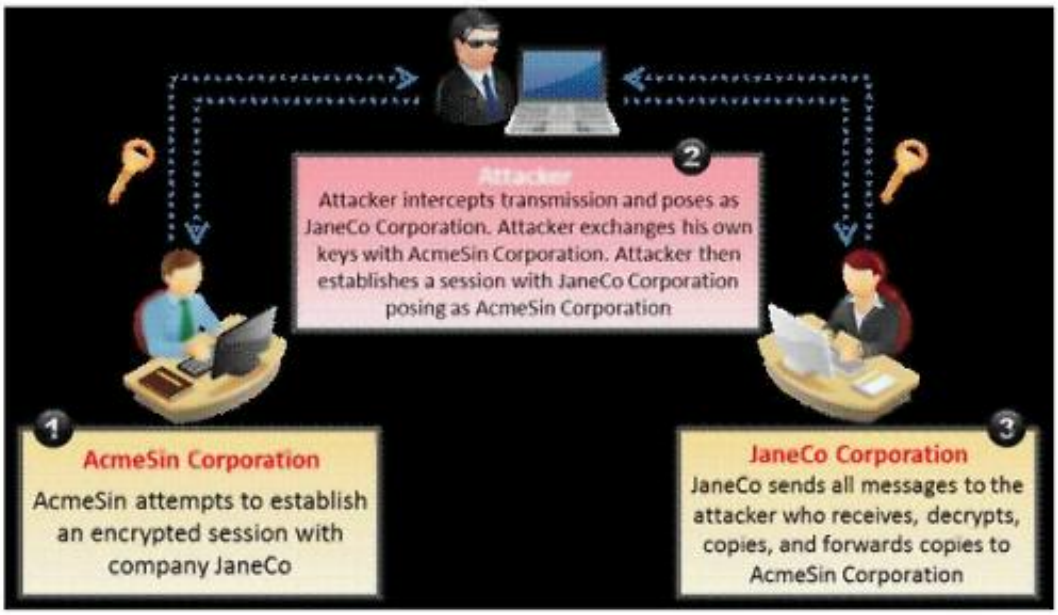
In which situations would you want to use anonymizer? (Select 3 answers)

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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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 notfrom internal hosts.

QUESTION NO: 11

TCP SYN Flood attack uses the three-way handshake mechanism.

1. An attacker at system A sends a SYN packet to victim at system B.

2. System B sends a SYN/ACK packet to victim A.

3. As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.

This status of client B is called _____

A. "half-closed"
B. "half open"
C. "full-open"
D. "xmas-open"

Answer: B
Explanation:

QUESTION NO: 12

Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company.

She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks

down the actual emails sent and upon opening them, only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture.

What technique was used by the Kiley Innovators employee to send information to the rival marketing company?

A. The Kiley Innovators employee used cryptography to hide the information in the emails sent
B. The method used by the employee to hide the information was logical watermarking
C. The employee used steganography to hide information in the picture attachments
D. By using the pictures to hide information, the employee utilized picture fuzzing

Answer: C
Explanation:

QUESTION NO: 13

You run nmap port Scan on 10.0.0.5 and attempt to gain banner/server information from services running on ports 21, 110 and 123.

Here is the output of your scan results:

```
PORT        STATE       SERVICE     VERSION
21/tcp      open        ftp         vsftpd 2.0.7
110/tcp     open        pop3        Courier pop3d
123/tcp     closed      ntp

Device type: general purpose
Running: Linux 2.8.X

OS details: Linux 2.8.18, Linux 2.8.20 - 2.8.24
Uptime: 65.658 days (since Mon Jun 19 00:43:29 2011)
Network Distance: 0 hops
Service Info: OS: Unix
```

Which of the following nmap command did you run?

A. nmap -A-sV -p21,110,123 10.0.0.5
B. nmap -F -sV -p21,110,123 10.0.0.5
C. nmap -O -sV -p21,110,123 10.0.0.5
D. nmap -T -sV -p21,110,123 10.0.0.5

Answer: C
Explanation:

QUESTION NO: 14

How do you defend against Privilege Escalation?

A. Use encryption to protect sensitivedata
B. Restrict the interactive logon privileges
C. Run services as unprivileged accounts
D. Allow security settings of IE to zero or Low
E. Run users and applications on the least privileges

Answer: A,B,C,E
Explanation:

QUESTION NO: 15

What does ICMP (type 11, code 0) denote?

A. Source Quench
B. Destination Unreachable
C. Time Exceeded
D. Unknown Type

Answer: C
Explanation:

QUESTION NO: 16

You are the security administrator of Jaco Banking Systems located in Boston. You are setting up e-banking website (http://www.ejacobank.com) authentication system. Instead of issuing banking customer with a single password, you give them a printed list of 100 unique passwords. Each time the customer needs to log into the e-banking system website, the customer enters the next password on the list. If someone sees them type the password using shoulder surfing, MiTM or keyloggers, then no damage is done because the password will not be accepted a second time. Once the list of 100 passwords is almost finished, the system automatically sends out a new password list by encrypted e-mail to the customer.

You are confident that this security implementation will protect the customer from password abuse.

Two months later, a group of hackers called "HackJihad" found a way to access the one-time password list issued to customers of Jaco Banking Systems. The hackers set up a fake website (http://www.e-jacobank.com) and used phishing attacks to direct ignorant customers to it. The fake website asked users for their e-banking username and password, and the next unused entry from their one-time password sheet. The hackers collected 200 customer's username/passwords this way. They transferred money from the customer's bank account to various offshore accounts.

Your decision of password policy implementation has cost the bank with USD 925,000 to hackers. You immediately shut down the e-banking website while figuring out the next best security solution

What effective security solution will you recommend in this case?

A. Implement Biometrics based passwordauthentication system. Record the customers face image to the authentication database
B. Configure your firewall to block logon attempts of more than three wrong tries
C. Enable a complex password policy of 20 characters and ask the user to change the password immediately after they logon and do not store password histories
D. Implement RSA SecureID based authentication system

Answer: D
Explanation:

QUESTION NO: 17

More sophisticated IDSs look for common shellcode signatures. But even these systems can be bypassed, by using polymorphic shellcode. This is a technique common among virus writers ?it basically hides the true nature of the shellcode in different disguises.

How does a polymorphic shellcode work?

A. They encrypt the shellcode by XORing values over the shellcode, using loader code to decrypt the shellcode, and then executing the decrypted shellcode
B. They convert the shellcode into Unicode, using loader to convert back to machine code then executing them
C. They reverse the working instructions into opposite order by masking the IDS signatures
D. They compress shellcode into normal instructions, uncompress the shellcode using loader code and then executing the shellcode

Answer: A