Vendor: EC-Council

Exam Code: EC1-350

Exam Name: Ethical Hacking and Countermeasures V7

Version: DEMO

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 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

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
This attack uses social engineering techniques to trick users into accessing a fake Web site and divulging personal information. Attackers send a legitimate-looking e-mail asking users to update their information on the company's Web site, but the URLs in the e-mail actually point to a false Web site.

A. Wiresharp attack
B. Switch and bait attack
C. Phishing attack

D. Man-in-the-Middle attack

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. IPFragment 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: BCD

QUESTION 8
The SYN flood attack sends TCP connections requests faster than a machine can process them.

- Attacker creates a random source address for each packet
- SYN flag set in each packet isa request to open a new connection to the server from the spoofed IP address
- Victim responds to spoofed IP address, then waits for confirmation that never arrives (timeout wait is about 3 minutes)
- Victim's connection table fills up waiting for replies andignores new connections
- Legitimate users are ignored and will not be able to access the server

How do you protect your network against SYN Flood attacks?

A. SYN cookies. Instead of allocating a record, send a SYN-ACK with a carefully constructed sequencenumber generated as a hash of the clients IP address, port number, and other information. When the client responds with a normal ACK, that special sequence number will be included, which the server then verifies. Thus, the server first allocates memory onthe third packet of the handshake, not the first.
B. RST cookies - The server sends a wrong SYN/ACK back to the client. The client should then generate a RST packet telling the server that something is wrong. At this point, the server knows "Pass Any Exam. Any Time." - www.actualtests.com 18
ECCouncil EC1-350 Exam
the client isvalid and will now accept incoming connections from that client normally
C. Check the incoming packet's IP address with the SPAM database on the Internet and enable the filter using ACLs at the Firewall
D. Stack Tweaking. TCP stacks can be tweaked in orderto reduce the effect of SYN floods. Reduce the timeout before a stack frees up the memory allocated for a connection
E. Micro Blocks. Instead of allocating a complete connection, simply allocate a micro record of 16-bytes for the incoming SYN object

Answer: ABDE

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: ACD
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 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

QUESTION 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

QUESTION 13
Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company's largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason's client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor.

Without any proof, Jason's company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason's company can finish the project. Once again, Jason says that he had nothing to do with it and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on.

Jason's supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing else. Jason's supervisor opens the picture files, but cannot find anything out of the ordinary with them.

What technique has Jason most likely used?

A. Stealth Rootkit Technique
B. ADS Streams Technique
C. Snow Hiding Technique
D. Image Steganography Technique

Answer: D

QUESTION 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: ABCE

QUESTION 15
What does ICMP (type 11, code 0) denote?

A. Source Quench

B. Destination Unreachable
C. Time Exceeded
D. Unknown Type

Answer: C

QUESTION 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

QUESTION 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

QUESTION 18
SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains:

A. The source and destination address having the same value
B. A large number of SYN packets appearing on a network without the corresponding reply packets
C. The source and destination port numbers having the same value
D. A large number of SYN packets appearing on a network with the corresponding reply packets

Answer: B

QUESTION 19
Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?

A. Port Scanning
B. Single Scanning
C. External Scanning
D. Vulnerability Scanning

Answer: D

QUESTION 20
What are the limitations of Vulnerability scanners? (Select 2 answers)

A. There are often better at detecting well-known vulnerabilitiesthan more esoteric ones
B. The scanning speed of their scanners are extremely high
C. It is impossible for any, one scanning product to incorporate all known vulnerabilities in a timely manner
D. The more vulnerabilities detected, the more tests required
E. They are highly expensive and require per host scan license

Answer: AC

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: BDNT2014