Vendor: EC-Council

Exam Code: 312-50v7

Exam Name: Ethical Hacking and Countermeasures (CEHv7) VUE

Version: DEMO

QUESTION 1
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 2
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 3
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 4
The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user:

```
var Shipcity;
ShipCity = Request.form ("ShipCity");
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:

```
SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'
```

How will you delete the OrdersTable from the database using SQL Injection?

A. Chicago'; drop table OrdersTable --
B. Delete table'blah'; OrdersTable --
C. EXEC; SELECT * OrdersTable > DROP --
D. cmdshell'; 'del c:\sql\mydb\OrdersTable' //

Answer: A

QUESTION 5
What are the limitations of Vulnerability scanners? (Select 2 answers)

A. There are often better at detecting well-known vulnerabilities than 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

QUESTION 6
Stephanie works as senior security analyst for a manufacturing company in Detroit. Stephanie manages network security throughout the organization. Her colleague Jason told her in confidence that he was able to see confidential corporate information posted on the external website http://www.jeansclothesman.com. He tries random URLs on the company's website and finds confidential information leaked over the web. Jason says this happened about a month ago. Stephanie visits the said URLs, but she finds nothing. She is very concerned about this, since someone should be held accountable if there was sensitive information posted on the website. Where can Stephanie go to see past versions and pages of a website?

A. She should go to the web page Samspade.org to see web pages that might no longer be on the website
B. If Stephanie navigates to Search.com; she will see old versions of the company website
C. Stephanie can go to Archive.org to see past versions of the company website
D. AddressPast.com would have any web pages that are no longer hosted on the company's website

Answer: C

QUESTION 7
Dan is conducting penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting vulnerability. Dan wants to replay this token. However, the session ID manager (on the server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?

A. Dan cannot spoof his IP address over TCP network

B. The scenario is incorrect as Dan can spoof his IP and get responses
C. The server will send replies back to the spoofed IP address
D. Dan can establish an interactive session only if he uses a NAT

Answer: C

QUESTION 8
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 9
What type of Virus is shown here?

A. Cavity Virus
B. Macro Virus
C. Boot Sector Virus
D. Metamorphic Virus
E. Sparse Infector Virus

Answer: E

QUESTION 10
An attacker finds a web page for a target organization that supplies contact information for the

company. Using available details to make the message seem authentic, the attacker drafts e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator. The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming. Google's Gmail was hacked using this technique and attackers stole source code and sensitive data from Google servers. This is highly sophisticated attack using zero-day exploit vectors, social engineering and malware websites that focused on targeted individuals working for the company. What is this deadly attack called?

A. Spear phishing attack
B. Trojan server attack
C. Javelin attack
D. Social networking attack

Answer: A

QUESTION 11
How does traceroute map the route a packet travels from point A to point B?

A. Uses a TCP timestamp packet that will elicit a time exceeded in transit message
B. Manipulates the value of the time to live (TTL) within packet to elicit a time exceeded in transit message
C. Uses a protocol that will be rejected by gateways on its way to the destination
D. Manipulates the flags within packets to force gateways into generating error messages

Answer: B

QUESTION 12
The SYN flood attack sends TCP connections requests faster than a machine can process them.

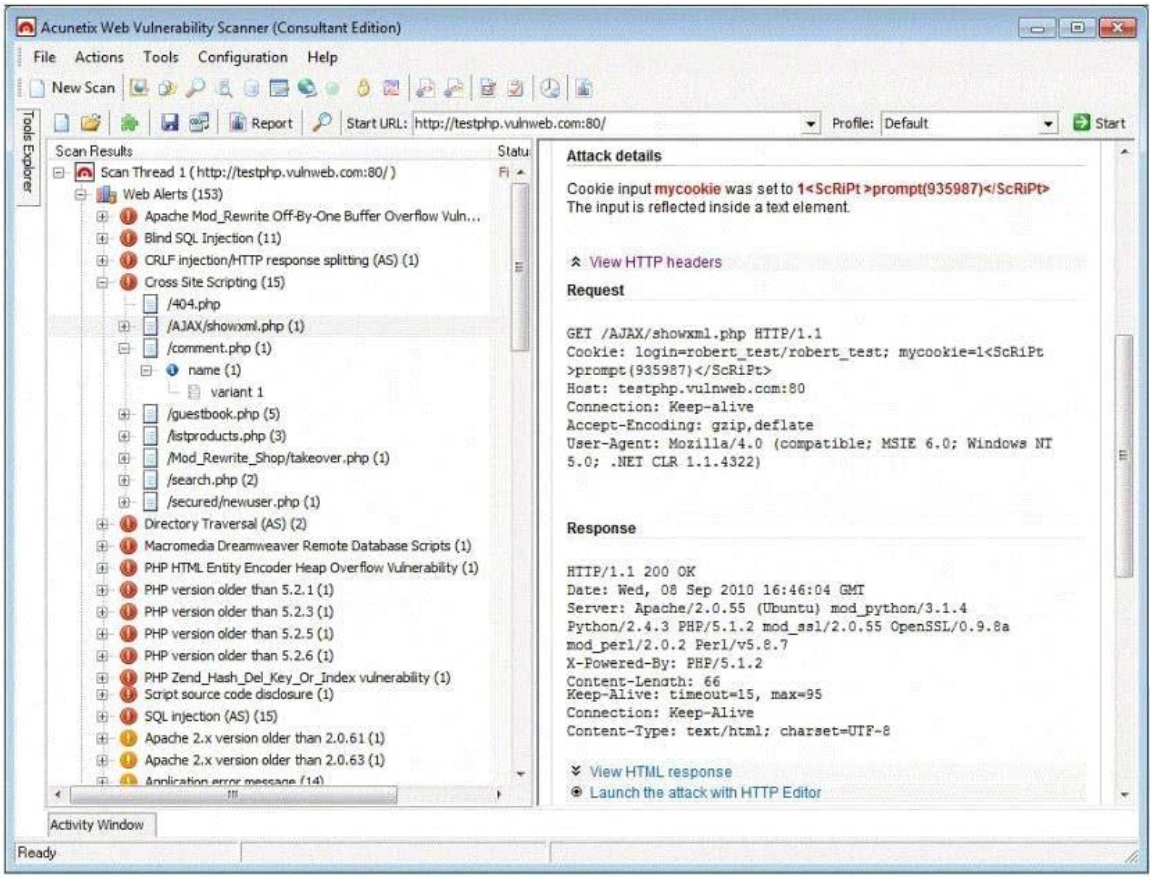
Attacker creates a random source address for each packet
SYN flag set in each packet is a request to open a new connection to the server from the spoofed IP address
Victim responds to spoofed IP address, then waits for confirmation that never arrives (timeout wait is about 3 minutes)
Victim's connection table fills up waiting for replies and ignores 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 sequence
number 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 Complete
server then verifies. Thus, the server first allocates memory on the 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 the client is valid
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 order to 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 13
Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfigurations of hosts. They also provide information regarding mitigating discovered vulnerabilities.

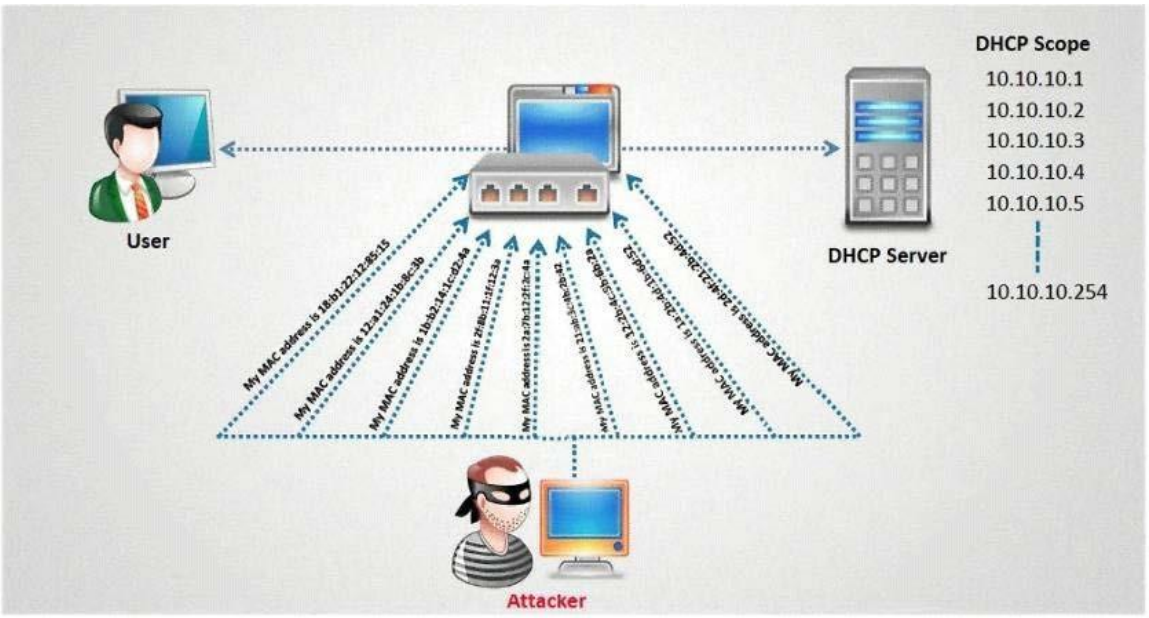


Which of the following statements is incorrect?

A. Vulnerability scanners attempt to identify vulnerabilities in the hosts scanned.
B. Vulnerability scanners can help identify out-of-date software versions, missing patches, or system upgrades
C. They can validate compliance with or deviations from the organization's security policy
D. Vulnerability scanners can identify weakness and automatically fix and patch the vulnerabilities without
user intervention

Answer: D

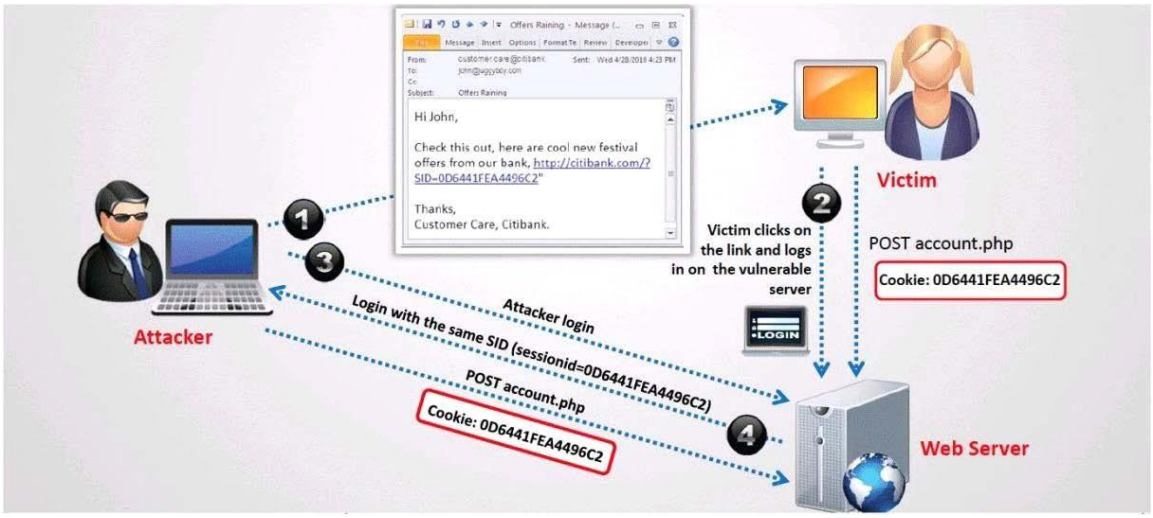
QUESTION 14
How do you defend against DHCP Starvation attack?



A. Enable ARP-Block on the switch
B. Enable DHCP snooping on the switch
C. Configure DHCP-BLOCK to 1 on the switch
D. Install DHCP filters on the switch to block this attack

Answer: B

QUESTION 15
What type of session hijacking attack is shown in the exhibit?



A. Cross-site scripting Attack
B. SQL Injection Attack
C. Token sniffing Attack
D. Session Fixation Attack

Answer: D

QUESTION 16
What type of port scan is shown below?

Scan directed at open port:
Client Server
192.5.2.92:4079 ---------FIN---------->192.5.2.110:23
192.5.2.92:4079 <----NO RESPONSE------192.5.2.110:23

Scan directed at closed port:
Client Server
192.5.2.92:4079 ---------FIN---------->192.5.2.110:23
192.5.2.92:4079<-----RST/ACK----------192.5.2.110:23

A. Idle Scan
B. FIN Scan
C. XMAS Scan
D. Windows Scan

Answer: B

QUESTION 17
Stephanie works as a records clerk in a large office building in downtown Chicago. On Monday, she went to a mandatory security awareness class (Security5) put on by her company's IT department. During the class, the IT department informed all employees that everyone's Internet activity was thenceforth going to be monitored. Stephanie is worried that her Internet activity might give her supervisor reason to write her up, or worse get her fired. Stephanie's daily work duties only consume about four hours of her time, so she usually spends the rest of the day surfing the web. Stephanie really enjoys surfing the Internet but definitely does not want to get fired for it. What should Stephanie use so that she does not get in trouble for surfing the Internet?

A. Stealth IE
B. Stealth Anonymizer
C. Stealth Firefox
D. Cookie Disabler

Answer: B

QUESTION 18
Neil is a network administrator working in Istanbul. Neil wants to setup a protocol analyzer on his network that will receive a copy of every packet that passes through the main office switch. What type of port will Neil need to setup in order to accomplish this?

A. Neil will have to configure a Bridged port that will copy all packets to the protocol analyzer.
B. Neil will need to setup SPAN port that will copy all network traffic to the protocol analyzer.
C. He will have to setup an Ether channel port to get a copy of all network traffic to the analyzer.
D. He should setup a MODS port which will copy all network traffic.

Answer: B

QUESTION 19
In TCP communications there are 8 flags; FIN, SYN, RST, PSH, ACK, URG, ECE, CWR. These

flags have decimal numbers assigned to them:

```
FIN = 1
SYN = 2
RST = 4
PSH = 8
ACK = 16
URG = 32
ECE = 64
CWR = 128
```

Jason is the security administrator of ASPEN Communications. He analyzes some traffic using Wireshark and has enabled the following filters.

```
((tcp.flags == 0x02) || (tcp.flags == 0x12) ) || ((tcp.flags == 0x10) && (tcp.ack==1) && (tcp.len==0))
```

What is Jason trying to accomplish here?

A. SYN, FIN, URG and PSH
B. SYN, SYN/ACK, ACK
C. RST, PSH/URG, FIN
D. ACK, ACK, SYN, URG

Answer: B

QUESTION 20
Peter extracts the SID list from Windows 2008 Server machine using the hacking tool "SIDExtracter".
Here is the output of the SIDs:

```
S-1-5-21-1125394485-807628933-549785860-100 John
S-1-5-21-1125394485-807628933-549785860-652 Rebecca
S-1-5-21-1125394485-807628933-549785860-412 Sheela
S-1-5-21-1125394485-807628933-549785860-999 Shawn
S-1-5-21-1125394485-807628933-549785860-777 Somia
S-1-5-21-1125394485-807628933-549785860-500 Chang
S-1-5-21-1125394485-807628933-549785860-555 Micah
```

From the above list identify the user account with System Administrator privileges?

A. John
B. Rebecca
C. Sheela
D. Shawn
E. Somia
F. Chang
G. Micah

Answer: F

Thank You for Trying Our Product

Lead2pass 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.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**