DUMPS ARENA

Certified Ethical Hacker (CEH)

GAQM CEH-001

Version Demo

Total Demo Questions: 20

Total Premium Questions: 878

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	99
Topic 2, Volume B	100
Topic 3, Volume C	100
Topic 4, Volume D	100
Topic 5, Volume E	100
Topic 6, Volume F	100
Topic 7, Volume G	100
Topic 8, Volume H	179
Total	878

QUESTION NO: 1

For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key

B. Receiver's private key

C. Receiver's public key

D. Sender's private key

ANSWER: D

QUESTION NO: 2

A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

A. Forensic attack

B. ARP spoofing attack

C. Social engineering attack

D. Scanning attack

ANSWER: C

QUESTION NO: 3

While scanning a network you observe that all of the web servers in the DMZ are responding to ACK packets on port 80.

What can you infer from this observation?

A. They are using Windows based web servers.

B. They are using UNIX based web servers.

C. They are not using an intrusion detection system.

D. They are not using a stateful inspection firewall.

ANSWER: D

QUESTION NO: 4

A remote user tries to login to a secure network using Telnet, but accidently types in an invalid user name or password. Which responses would NOT be preferred by an experienced Security Manager? (multiple answer)

A. Invalid Username

B. Invalid Password

C. Authentication Failure

D. Login Attempt Failed

E. Access Denied

ANSWER: A B

Explanation:

As little information as possible should be given about a failed login attempt. Invalid username or password is not desirable.

QUESTION NO: 5

How do you defend against Privilege Escalation?

A. Use encryption to protect sensitive data

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

QUESTION NO: 6

Which types of detection methods are employed by Network Intrusion Detection Systems (NIDS)? (Choose two.)

A. Signature

B. Anomaly

C. Passive

D. Reactive

ANSWER: A B

QUESTION NO: 7

Smart cards use which protocol to transfer the certificate in a secure manner?

A. Extensible Authentication Protocol (EAP)

B. Point to Point Protocol (PPP)

C. Point to Point Tunneling Protocol (PPTP)

D. Layer 2 Tunneling Protocol (L2TP)

ANSWER: A

QUESTION NO: 8

Which of the following tools can be used to perform a zone transfer?

A. NSLookup

B. Finger

C. Dig

D. Sam Spade

E. Host

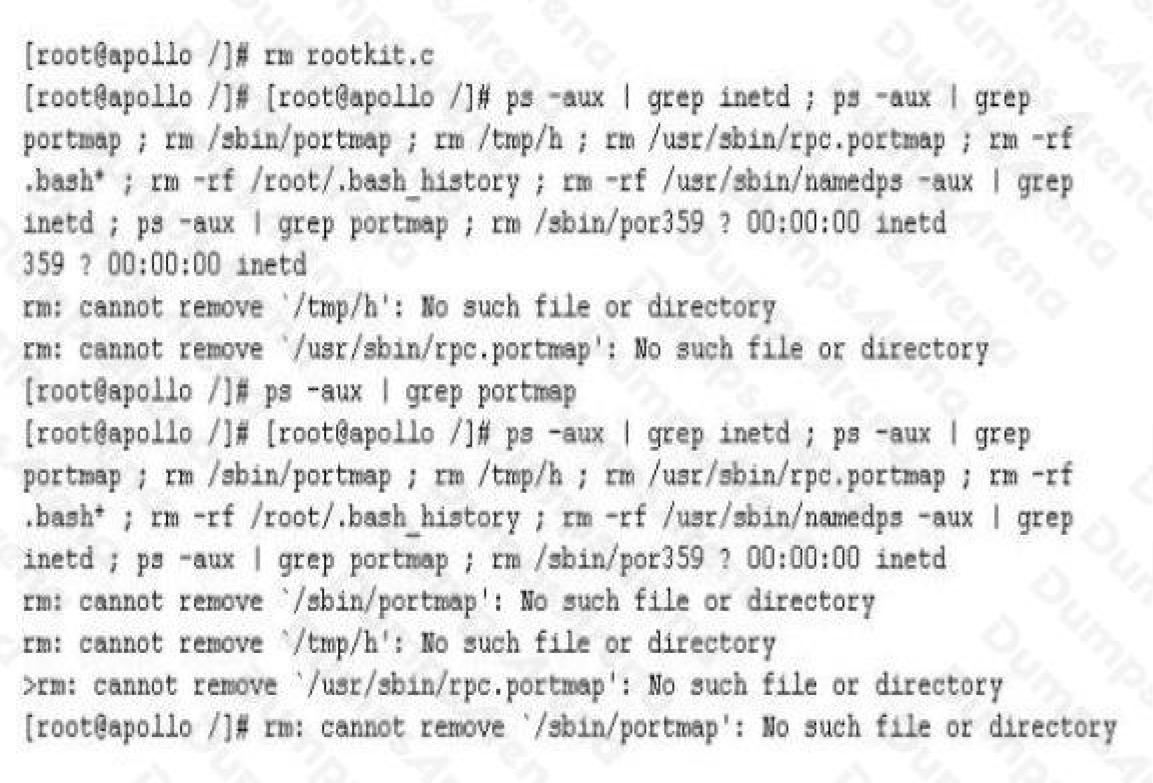
F. Netcat

G. Neotrace

ANSWER: A C D E

QUESTION NO: 9

John is the network administrator of XSECURITY systems. His network was recently compromised. He analyzes the log files to investigate the attack. Take a look at the following Linux log file snippet. The hacker compromised and "owned" a Linux machine. What is the hacker trying to accomplish here?



```
[root@apollo /]# rm rootkit.c
[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ; ps -aux | grep
portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf
.bash* ; rm -rf /root/.bash_history ; rm -rf /usr/sbin/namedps -aux | grep
inetd ; ps -aux | grep portmap ; rm /sbin/por359 ? 00:00:00 inetd
359 ? 00:00:00 inetd
rm: cannot remove `/tmp/h': No such file or directory
rm: cannot remove `/usr/sbin/rpc.portmap': No such file or directory
[root@apollo /]# ps -aux | grep portmap
[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ; ps -aux | grep
portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf
.bash* ; rm -rf /root/.bash_history ; rm -rf /usr/sbin/namedps -aux | grep
inetd ; ps -aux | grep portmap ; rm /sbin/por359 ? 00:00:00 inetd
rm: cannot remove `/sbin/portmap': No such file or directory
rm: cannot remove `/tmp/h': No such file or directory
>rm: cannot remove `/usr/sbin/rpc.portmap': No such file or directory
[root@apollo /]# rm: cannot remove `/sbin/portmap': No such file or directory
```

A. The hacker is attempting to compromise more machines on the network

B. The hacker is planting a rootkit

C. The hacker is running a buffer overflow exploit to lock down the system

D. The hacker is trying to cover his tracks

ANSWER: D

QUESTION NO: 10

Samantha was hired to perform an internal security test of XYZ. She quickly realized that all networks are making use of switches instead of traditional hubs. This greatly limits her ability to gather information through network sniffing.

Which of the following techniques can she use to gather information from the switched network or to disable some of the traffic isolation features of the switch? (Choose two)

A. Ethernet Zapping

B. MAC Flooding

C. Sniffing in promiscuous mode

D. ARP Spoofing

ANSWER: B D

QUESTION NO: 11

Botnets are networks of compromised computers that are controlled remotely and surreptitiously by one or more cyber criminals. How do cyber criminals infect a victim's computer with bots? (Select 4 answers)

A. Attackers physically visit every victim's computer to infect them with malicious software

B. Home computers that have security vulnerabilities are prime targets for botnets

C. Spammers scan the Internet looking for computers that are unprotected and use these "open-doors" to install malicious software

D. Attackers use phishing or spam emails that contain links or attachments

E. Attackers use websites to host the bots utilizing Web Browser vulnerabilities

ANSWER: B C D E

QUESTION NO: 12

Which of the following tools are used for footprinting? (Choose four)

A. Sam Spade

B. NSLookup

C. Traceroute

D. Neotrace

E. Cheops

ANSWER: A B C D

QUESTION NO: 13

Which of the following are variants of mandatory access control mechanisms? (Choose two.)

A. Two factor authentication

B. Acceptable use policy

C. Username / password

D. User education program

E. Sign in register

ANSWER: A C

QUESTION NO: 14

Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn an interactive shell and plans to deface the main web page. He first attempts to use the "echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page in which also he remains unsuccessful. What is the probable cause of Bill's problem?

A. You cannot use a buffer overflow to deface a web page

B. There is a problem with the shell and he needs to run the attack again

C. The HTML file has permissions of read only

D. The system is a honeypot

ANSWER: C

QUESTION NO: 15

What flags are set in a X-MAS scan?(Choose all that apply.

A. SYN

B. ACK

C. FIN

D. PSH

E. RST

F. URG

ANSWER: C D F

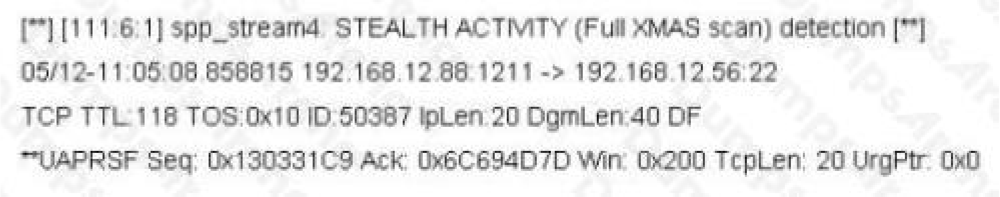
Explanation:

FIN, URG, and PSH are set high in the TCP packet for a X-MAS scan

QUESTION NO: 16

Jason is the network administrator of Spears Technology. He has enabled SNORT IDS to detect attacks going through his network. He receives Snort SMS alerts on his iPhone whenever there is an attempted intrusion to his network.

He receives the following SMS message during the weekend.



```
[**] [111:6:1] spp_stream4: STEALTH ACTIVITY (Full XMAS scan) detection [**]
05/12-11:05:08.858815 192.168.12.88:1211 -> 192.168.12.56:22
TCP TTL:118 TOS:0x10 ID:50387 IpLen:20 DgmLen:40 DF
**UAPRSF Seq: 0x130331C9 Ack: 0x6C694D7D Win: 0x200 TcpLen: 20 UrgPtr: 0x0
```

An attacker Chew Siew sitting in Beijing, China had just launched a remote scan on Jason's network with the hping command.

Which of the following hping2 command is responsible for the above snort alert?

A. chenrocks:/home/siew # hping -S -R -P -A -F -U 192.168.2.56 -p 22 -c 5 -t 118

B. chenrocks:/home/siew # hping -F -Q -J -A -C -W 192.168.2.56 -p 22 -c 5 -t 118

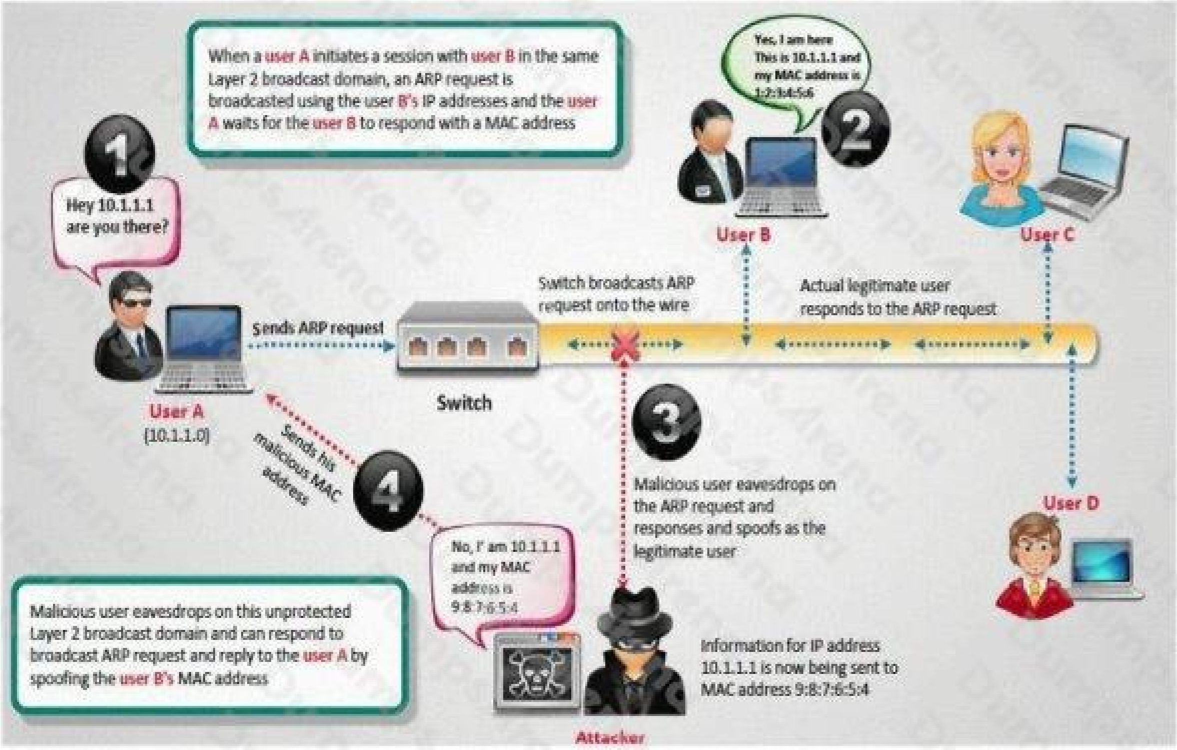
C. chenrocks:/home/siew # hping -D -V -R -S -Z -Y 192.168.2.56 -p 22 -c 5 -t 118

D. chenrocks:/home/siew # hping -G -T -H -S -L -W 192.168.2.56 -p 22 -c 5 -t 118

ANSWER: A

QUESTION NO: 17

How do you defend against ARP Poisoning attack? (Select 2 answers)



When a user A initiates a session with user B in the same Layer 2 broadcast domain, an ARP request is broadcasted using the user B's IP addresses and the user A waits for the user B to respond with a MAC address
1
Hey 10.1.1.1 are you there?
Yes, I am here This is 10.1.1.1 and my MAC address is 1:2:3:4:5:6
2
User B
User C
Switch broadcasts ARP request onto the wire
Actual legitimate user responds to the ARP request
Sends ARP request
Switch
User A
(10.1.1.0)
Sends his malicious MAC address
4
3
Malicious user eavesdrops on the ARP request and responses and spoofs as the legitimate user
User D
No, I' am 10.1.1.1 and my MAC address is 9:8:7:6:5:4
Malicious user eavesdrops on this unprotected Layer 2 broadcast domain and can respond to broadcast ARP request and reply to the user A by spoofing the user B's MAC address
Information for IP address 10.1.1.1 is now being sent to MAC address 9:8:7:6:5:4
Attacker

A. Enable DHCP Snooping Binding Table

B. Restrict ARP Duplicates

C. Enable Dynamic ARP Inspection

D. Enable MAC snooping Table

ANSWER: A C

QUESTION NO: 18

You are trying to package a RAT Trojan so that Anti-Virus software will not detect it. Which of the listed technique will NOT be effective in evading Anti-Virus scanner?

A. Convert the Trojan.exe file extension to Trojan.txt disguising as text file

B. Break the Trojan into multiple smaller files and zip the individual pieces

C. Change the content of the Trojan using hex editor and modify the checksum

D. Encrypt the Trojan using multiple hashing algorithms like MD5 and SHA-1

ANSWER: A

QUESTION NO: 19

Which of the following is NOT part of CEH Scanning Methodology?

A. Check for Live systems

B. Check for Open Ports

C. Banner Grabbing

D. Prepare Proxies

E. Social Engineering attacks

F. Scan for Vulnerabilities

G. Draw Network Diagrams

ANSWER: E

QUESTION NO: 20

A hacker is attempting to see which IP addresses are currently active on a network. Which NMAP switch would the hacker use?

A. -sO

B. -sP

C. -sS

D. -sU

ANSWER: B