DUMPSBOSS.

Ethical Hacking and Countermeasures V8

ECCouncil EC0-350

Version Demo

Total Demo Questions: 20

Total Premium Questions: 878

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

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

Jim's organization has just completed a major Linux roll out and now all of the organization's systems are running the Linux 2.5 kernel. The roll out expenses has posed constraints on purchasing other essential security equipment and software. The organization requires an option to control network traffic and also perform stateful inspection of traffic going into and out of the DMZ.

Which built-in functionality of Linux can achieve this?

A. IP Tables

B. IP Chains

C. IP Sniffer

D. IP ICMP

ANSWER: A

QUESTION NO: 2

What type of port scan is shown below?

```
Scan directed at open port:

     Client                                  Server
192.5.2.92:4079 ----FIN/URG/PSH---->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/URG/PSH---->192.5.2.110:23
192.5.2.92:4079<------RST/ACK-------192.5.2.110:23
```

A. Idle Scan

B. Windows Scan

C. XMAS Scan

D. SYN Stealth Scan

ANSWER: C

QUESTION NO: 3

Which of the following describes the characteristics of a Boot Sector Virus?

A. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

B. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR

C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program

D. Overwrites the original MBR and only executes the new virus code

ANSWER: B

QUESTION NO: 4

A circuit level gateway works at which of the following layers of the OSI Model?

A. Layer 5 - Application

B. Layer 4 – TCP

C. Layer 3 – Internet protocol

D. Layer 2 – Data link

ANSWER: B

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

In the following example, which of these is the "exploit"?

Today, Microsoft Corporation released a security notice. It detailed how a person could bring down the Windows 2003 Server operating system, by sending malformed packets to it. They detailed how this malicious process had been automated using basic scripting. Even worse, the new automated method for bringing down the server has already been used to perform denial of service attacks on many large commercial websites.

Select the best answer.

A. Microsoft Corporation is the exploit.

B. The security "hole" in the product is the exploit.

C. Windows 2003 Server

D. The exploit is the hacker that would use this vulnerability.

E. The documented method of how to use the vulnerability to gain unprivileged access.

ANSWER: E

QUESTION NO: 7

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: 8

Several of your co-workers are having a discussion over the etc/passwd file. They are at odds over what types of encryption are used to secure Linux passwords.(Choose all that apply.

A. Linux passwords can be encrypted with MD5

B. Linux passwords can be encrypted with SHA

C. Linux passwords can be encrypted with DES

D. Linux passwords can be encrypted with Blowfish

E. Linux passwords are encrypted with asymmetric algrothims

ANSWER: A C D

QUESTION NO: 9

While footprinting a network, what port/service should you look for to attempt a zone transfer?

A. 53 UDP

B. 53 TCP

C. 25 UDP

D. 25 TCP

E. 161 UDP

F. 22 TCP

G. 60 TCP

ANSWER: B

QUESTION NO: 10

What makes web application vulnerabilities so aggravating? (Choose two)

A. They can be launched through an authorized port.

B. A firewall will not stop them.

C. They exist only on the Linux platform.

D. They are detectable by most leading antivirus software.

ANSWER: A B

QUESTION NO: 11

Information gathered from social networking websites such as Facebook, Twitter and LinkedIn can be used to launch which of the following types of attacks? (Choose two.)

A. Smurf attack

B. Social engineering attack

C. SQL injection attack

D. Phishing attack

E. Fraggle attack

F. Distributed denial of service attack

ANSWER: B D

QUESTION NO: 12

Which of the following buffer overflow exploits are related to Microsoft IIS web server? (Choose three)

A. Internet Printing Protocol (IPP) buffer overflow

B. Code Red Worm

C. Indexing services ISAPI extension buffer overflow

D. NeXT buffer overflow

ANSWER: A B C

QUESTION NO: 13

There is some dispute between two network administrators at your company. Your boss asks you to come and meet with the administrators to set the record straight. Which of these are true about PKI and encryption?

Select the best answers.

A. PKI provides data with encryption, compression, and restorability.

B. Public-key encryption was invented in 1976 by Whitfield Diffie and Martin Hellman.

C. When it comes to eCommerce, as long as you have authenticity, and authenticity, you do not need encryption.

D. RSA is a type of encryption.

ANSWER: B D

QUESTION NO: 14

A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

A. Ignore the problem completely and let someone else deal with it.

B. Create a document that will crash the computer when opened and send it to friends.

C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.

D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

ANSWER: D

QUESTION NO: 15

Finding tools to run dictionary and brute forcing attacks against FTP and Web servers is an easy task for hackers. They use tools such as arhontus or brutus to break into remote servers.

```
CEH# ./rpa
Remote Password Assassin V 1.0
Roses Labs / w00w00
Usage: ./rpa <host> (options)
Options:
-l : Login file to use.
-s : Use the same login.
-c : Password file to use.
-r : Attack FlowPoint Router.
-t : Attack Telnet Port.
-f : Attack FTP Port.
-p : Attack POP Port.
CEH# ./rpa 10.0.0.34 -t -f -c passwords.txt -s linksys
```

A command such as this, will attack a given 10.0.0.34 FTP and Telnet servers simultaneously with a list of passwords and a single login namE. linksys. Many FTP-specific password-guessing tools are also available from major security sites.

What defensive measures will you take to protect your network from these attacks?

A. Never leave a default password

B. Never use a password that can be found in a dictionary

C. Never use a password related to your hobbies, pets, relatives, or date of birth.

D. Use a word that has more than 21 characters from a dictionary as the password

E. Never use a password related to the hostname, domain name, or anything else that can be found with whois

ANSWER: A B C E

QUESTION NO: 16

This method is used to determine the Operating system and version running on a remote target system. What is it called?

A. Service Degradation

B. OS Fingerprinting

C. Manual Target System

D. Identification Scanning

ANSWER: B

QUESTION NO: 17

What does a type 3 code 13 represent?(Choose two.

A. Echo request

B. Destination unreachable

C. Network unreachable

D. Administratively prohibited

E. Port unreachable

F. Time exceeded

ANSWER: B D

QUESTION NO: 18

You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account

B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer

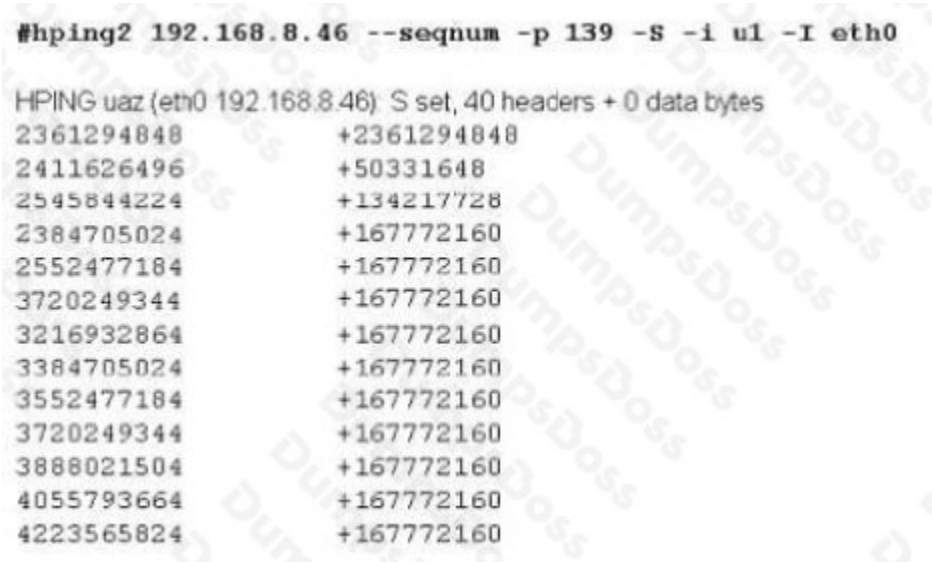
C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques

D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

ANSWER: C

QUESTION NO: 19

Exhibit



```
#hping2 192.168.8.46 --seqnum -p 139 -S -i u1 -I eth0

HPING uaz (eth0 192.168.8.46): S set, 40 headers + 0 data bytes
2361294848          +2361294848
2411626496          +50331648
2545844224          +134217728
2384705024          +167772160
2552477184          +167772160
3720249344          +167772160
3216932864          +167772160
3384705024          +167772160
3552477184          +167772160
3720249344          +167772160
3888021504          +167772160
4055793664          +167772160
4223565824          +167772160
```

Joe Hacker runs the hping2 hacking tool to predict the target host's sequence numbers in one of the hacking session.

What does the first and second column mean? Select two.

A. The first column reports the sequence number

B. The second column reports the difference between the current and last sequence number

C. The second column reports the next sequence number

D. The first column reports the difference between current and last sequence number

ANSWER: A B

QUESTION NO: 20

Data hiding analysis can be useful in

A. determining the level of encryption used to encrypt the data.

B. detecting and recovering data that may indicate knowledge, ownership or intent.

C. identifying the amount of central processing unit (cpu) usage over time to process the data.

D. preventing a denial of service attack on a set of enterprise servers to prevent users from accessing the data.

ANSWER: B