



312-49V10^{Q&As}

EC Council Computer Hacking Forensic Investigator (V10)

Pass EC-COUNCIL 312-49V10 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/312-49v10.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

What is a first sector ("sector zero") of a hard disk?

- A. Master boot record
- B. System boot record
- C. Secondary boot record
- D. Hard disk boot record

Correct Answer: A

QUESTION 2

What does the superblock in Linux define?

- A. file synames
- B. disk geometr
- C. location of the first inode
- D. available space

Correct Answer: C

QUESTION 3

Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?

- A. ISO/IEC 16025
- B. ISO/IEC 18025
- C. ISO/IEC 19025
- D. ISO/IEC 17025

Correct Answer: D

QUESTION 4

The following excerpt is taken from a honeypot log. The log captures activities across three days. There



are several intrusion attempts; however, a few are successful.

(Note: The objective of this question is to test whether the student can read basic information from log

entries and interpret the nature of attack.)

Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169 Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482 Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53 Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21 Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53 Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53 Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53 Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111 Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80 Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53 Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53 Apr 26 06:44:25 victim7 PAM_pwd[12509]: (login) session opened for user simple by (uid=0) Apr 26 06:44:36 victim7 PAM_pwd[12521]: (su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080 Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558 From the options given below choose the one which best interprets the following entry: Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

- A. An IDS evasion technique
- B. A buffer overflow attempt
- C. A DNS zone transfer
- D. Data being retrieved from 63.226.81.13

Correct Answer: A

QUESTION 5

Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain specific user information?

- A. Temporary Files
- B. Open files
- C. Cookies
- D. Web Browser Cache

Correct Answer: C

QUESTION 6

Which of the following is not a part of data acquisition forensics Investigation?

- A. Permit only authorized personnel to access



- B. Protect the evidence from extremes in temperature
- C. Work on the original storage medium not on the duplicated copy
- D. Disable all remote access to the system

Correct Answer: C

QUESTION 7

You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?

- A. make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab
- B. make an MD5 hash of the evidence and compare it to the standard database developed by NIST
- C. there is no reason to worry about this possible claim because state labs are certified
- D. sign a statement attesting that the evidence is the same as it was when it entered the lab

Correct Answer: A

QUESTION 8

Which of the following filesystem is used by Mac OS X?

- A. EFS
- B. HFS+
- C. EXT2
- D. NFS

Correct Answer: B

QUESTION 9

Which part of the Windows Registry contains the user's password file?

- A. HKEY_LOCAL_MACHINE
- B. HKEY_CURRENT_CONFIGURATION
- C. HKEY_USER
- D. HKEY_CURRENT_USER



Correct Answer: AD

QUESTION 10

The given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?

```
Administrator: Command Prompt
03/10/2016 03:30 AM <DIR> migration
03/10/2016 03:32 AM 352,136 FNTCACHE.DAT
03/25/2016 08:09 PM 140,098 perfc009.dat
03/25/2016 08:09 PM 746,532 perfh009.dat
03/25/2016 08:09 PM 883,572 PerfStringBackup.INI
04/06/2016 04:54 PM <DIR> DriverStore
04/13/2016 11:27 AM <DIR> catroot2
04/13/2016 12:33 PM 135,176,864 MRT.exe
04/13/2016 12:33 PM <DIR> MRT
04/14/2016 09:36 AM <DIR> config
04/14/2016 03:06 PM <DIR> drivers
04/14/2016 04:02 PM <DIR> .
04/14/2016 04:02 PM <DIR> ..
04/14/2016 04:02 PM 324 pid.dump
04/14/2016 05:51 PM <DIR> sru
3866 File(s) 1,727,891,022 bytes
116 Dir(s) 63,601,328,128 bytes free
C:\WINDOWS\system32>
```

- A. dir /o:d
- B. dir /o:s
- C. dir /o:e
- D. dir /o:n

Correct Answer: A

QUESTION 11

In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?



- A. Policy of separation
- B. Chain of custody
- C. Rules of evidence
- D. Law of probability

Correct Answer: B

QUESTION 12

Which of the following is NOT a part of pre-investigation phase?

- A. Building forensics workstation
- B. Gathering information about the incident
- C. Gathering evidence data
- D. Creating an investigation team

Correct Answer: C

QUESTION 13

Which component in the hard disk moves over the platter to read and write information?

- A. Actuator
- B. Spindle
- C. Actuator Axis
- D. Head

Correct Answer: D

QUESTION 14

What must an attorney do first before you are called to testify as an expert?

- A. Qualify you as an expert witness
- B. Read your curriculum vitae to the jury
- C. Engage in damage control



D. Prove that the tools you used to conduct your examination are perfect

Correct Answer: A

QUESTION 15

Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain the confidentiality of data.

A. True

B. False

Correct Answer: A

[Latest 312-49V10 Dumps](#)

[312-49V10 VCE Dumps](#)

[312-49V10 Exam Questions](#)