312-49Q&As

ECCouncil Computer Hacking Forensic Investigator (V9)

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

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

https://www.passapply.com/312-49.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An executive has leaked the company trade secrets through an external drive. What process should the investigation team take if they could retrieve his system?

A. Postmortem Analysis

B. Real-Time Analysis

C. Packet Analysis

D. Malware Analysis

Correct Answer: A

QUESTION 2

How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

A. 128

B. 64

C. 32

D. 16

Correct Answer: C

QUESTION 3

A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?

A. They examined the actual evidence on an unrelated system

B. They attempted to implicate personnel without proof

C. They tampered with evidence by using it

D. They called in the FBI without correlating with the fingerprint data

Correct Answer: C

QUESTION 4

Which program is the bootloader when Windows XP starts up?

A. KERNEL.EXE

B. NTLDR

C. LOADER

D. LILO

Correct Answer: B

QUESTION 5

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