312-49^Q&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.geekcert.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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

The process of restarting a computer that is already turned on through the operating system is called?

A. Warm boot

B. Ice boot

C. Hot Boot

D. Cold boot

Correct Answer: A

QUESTION 2

You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?

A. Limited force and library attack

B. Brute Force and dictionary Attack

C. Maximum force and thesaurus Attack

D. Minimum force and appendix Attack

Correct Answer: B

QUESTION 3

A master boot record (MBR) is the first sector ("sector zero") of a data storage device. What is the size of MBR?

A. Depends on the capacity of the storage device

B. 1048 Bytes

C. 4092 Bytes

D. 512 Bytes

Correct Answer: D

QUESTION 4

What malware analysis operation can the investigator perform using the jv16 tool?

A. Files and Folder Monitor

B. Installation Monitor

C. Network Traffic Monitoring/Analysis

D. Registry Analysis/Monitoring

Correct Answer: D

QUESTION 5

What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

A. Cracks every password in 10 minutes

B. Distribute processing over 16 or fewer computers

C. Support for Encrypted File System

D. Support for MD5 hash verification

Correct Answer: B