312-49V10^{Q&As}

ECCouncil 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

QUESTION 1

Which tool allows dumping the contents of process memory without stopping the process?

A. psdump.exe

B. pmdump.exe

C. processdump.exe

D. pdump.exe

Correct Answer: B

Reference: https://www.sciencedirect.com/topics/computer-science/memory-dump-file#:~:text=Post%20Mortem%20Dump%20or%20PMDump,analysis%20of%20a%20dump%20file

QUESTION 2

What is cold boot (hard boot)?

A. It is the process of starting a computer from a powered-down or off state

B. It is the process of restarting a computer that is already turned on through the operating system

C. It is the process of shutting down a computer from a powered-on or on state

D. It is the process of restarting a computer that is already in sleep mode

Correct Answer: A

QUESTION 3

What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?

A. Jump instruction and the OEM ID

B. BIOS Parameter Block (BPB) and the OEM ID

C. BIOS Parameter Block (BPB) and the extended BPB

D. Bootstrap code and the end of the sector marker

Correct Answer: C

Reference: http://ntfs.com/ntfs-partition-boot-sector.htm

QUESTION 4

What type of equipment would a forensics investigator store in a StrongHold bag?

A. PDAPDA?

B. Backup tapes

C. Hard drives

D. Wireless cards

Correct Answer: D

QUESTION 5

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?

A. Dig

B. Ping sweep

C. Netcraft

D. Nmap

Correct Answer: C

Latest 312-49V10 Dumps   312-49V10 Practice Test   312-49V10 Exam Questions