

312-49V8^{Q&As}

Computer Hacking Forensic Investigator Exam

**Pass EC-COUNCIL 312-49V8 Exam with 100%
Guarantee**

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

<https://www.lead4pass.com/312-49v8.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

Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:

- A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion \ProfileList
- B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \NetworkList
- C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentsVersion \setup
- D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule

Correct Answer: A

QUESTION 2

Buffer Overflow occurs when an application writes more data to a block of memory, or buffer, than the buffer is allocated to hold. Buffer overflow attacks allow an attacker to modify the _____ in order to control the process execution, crash the process and modify internal variables.

- A. Target process's address space
- B. Target remote access
- C. Target rainbow table
- D. Target SAM file

Correct Answer: A

QUESTION 3

Damaged portions of a disk on which no read/write operation can be performed is known as _____.

- A. Lost sector
- B. Bad sector
- C. Empty sector
- D. Unused sector

Correct Answer: B

QUESTION 4

In Windows 7 system files, which file reads the Boot.ini file and loads Ntoskrnl.exe, Bootvid.dll, Hal.dll, and boot-start device drivers?

- A. Ntldr
- B. Gdi32.dll
- C. Kernel32.dll
- D. Boot.in

Correct Answer: A

QUESTION 5

File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows7?

- A. The last letter of a file name is replaced by a hex byte code E5h
- B. The operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted
- C. Corresponding clusters in FAT are marked as used
- D. The computer looks at the clusters occupied by that file and does not avails space to store a new file

Correct Answer: B

[312-49V8 VCE Dumps](#)

[312-49V8 Practice Test](#)

[312-49V8 Braindumps](#)