EC0-349 Q&As

Computer Hacking Forensic Investigator

Pass EC-COUNCIL EC0-349 Exam with 100% Guarantee

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

https://www.pass2lead.com/ec0-349.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

After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

A. Enable direct broadcasts

B. Disable direct broadcasts

C. Disable BGP

D. Enable BGP

Correct Answer: B

QUESTION 2

To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

A. Computer Forensics Tools and Validation Committee (CFTVC)

B. Association of Computer Forensics Software Manufactures (ACFSM)

C. National Institute of Standards and Technology (NIST)

D. Society for Valid Forensics Tools and Testing (SVFTT)

Correct Answer: C

QUESTION 3

Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:

A. HKEY_LOCAL_MACHINE\hardware\windows\start

B. HKEY_LOCAL_USERS\Software\Microsoft\old\Version\Load

C. HKEY_CURRENT_USER\Microsoft\Default

D. HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run

Correct Answer: D

QUESTION 4

What must an investigator do before disconnecting an iPod from any type of computer?

A. Unmount the iPod

B. Mount the iPod

C. Disjoin the iPod

D. Join the iPod

Correct Answer: A

QUESTION 5

When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz format, what does the nnn denote?

A. The year the evidence was taken

B. The sequence number for the parts of the same exhibit

C. The initials of the forensics analyst

D. The sequential number of the exhibits seized

Correct Answer: D