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.leads4pass.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

What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

A. Fraggle

B. Smurf scan

C. SYN flood

D. Teardrop

Correct Answer: A

QUESTION 2

What is the target host IP in the following command?

A. 172.16.28.95

B. 10.10.150.1

C. Firewalk does not scan target hosts

D. This command is using FIN packets, which cannot scan target hosts

Correct Answer: A

QUESTION 3

You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data.

What method would be most efficient for you to acquire digital evidence from this network?

A. create a compressed copy of the file with DoubleSpace

B. create a sparse data copy of a folder or file

C. make a bit-stream disk-to-image file

D. make a bit-stream disk-to-disk file

Correct Answer: C

QUESTION 4

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 5

Using Linux to carry out a forensics investigation, what would the following command accomplish? dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror

A. Search for disk errors within an image file

B. Backup a disk to an image file

C. Copy a partition to an image file

D. Restore a disk from an image file

Correct Answer: D

Latest EC0-349 Dumps EC0-349 PDF Dumps EC0-349 Exam Questions