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.pass4itsure.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

QUESTION 1

Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?

A. bench warrant

B. wire tap

C. subpoena

D. search warrant

Correct Answer: D

QUESTION 2

What does the superblock in Linux define?

A. filesynames

B. diskgeometr

C. location of the firstinode

D. available space

Correct Answer: C

QUESTION 3

What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

A. digital attack

B. denial of service

C. physical attack

D. ARP redirect

Correct Answer: B

QUESTION 4

Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish? dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync

A. Fill the disk with zeros

B. Low-level format

C. Fill the disk with 4096 zeros

D. Copy files from the master disk to the slave disk on the secondary IDE controller

Correct Answer: A

QUESTION 5

When is it appropriate to use computer forensics?

A. If copyright and intellectual property theft/misuse has occurred

B. If employees do not care for their boss management techniques

C. If sales drop off for no apparent reason for an extended period of time

D. If a financial institution is burglarized by robbers

Correct Answer: A