312-49 Q&As

ECCouncil Computer Hacking Forensic Investigator (V9)

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

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

https://www.leads4pass.com/312-49.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

You have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company IT department, you search through the server log files to find any trace of the intrusion. After that you decide to telnet into one of the company routers to see if there is any evidence to be found. While connected to the router, you see some unusual activity and believe that the attackers are currently connected to that router. You start up an ethereal session to begin capturing traffic on the router that could be used in the investigation. At what layer of the OSI model are you monitoring while watching traffic to and from the router?

A. Network

B. Transport

C. Data Link

D. Session

Correct Answer: A

QUESTION 2

Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

A. Accunetix

B. Nikto

C. Snort

D. Kismet

Correct Answer: C

QUESTION 3

When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A. Multiple access points can be set up on the same channel without any issues

B. Avoid over-saturation of wireless signals

C. So that the access points will work on different frequencies

D. Avoid cross talk

Correct Answer: D

QUESTION 4

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

A. The registry

B. The swap file

C. The recycle bin

D. The metadata

Correct Answer: B

QUESTION 5

Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

A. FAT File System

B. ReFS

C. exFAT

D. NTFS File System

Correct Answer: D

312-49 PDF Dumps   312-49 Practice Test   312-49 Exam Questions