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.passapply.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

QUESTION 1

Which of the following setups should a tester choose to analyze malware behavior?

A. A virtual system with internet connection

B. A normal system without internet connect

C. A normal system with internet connection

D. A virtual system with network simulation for internet connection

Correct Answer: D

QUESTION 2

Your company\\'s network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Block all internal MAC address from using SNMP

B. Block access to UDP port 171

C. Block access to TCP port 171

D. Change the default community string names

Correct Answer: D

QUESTION 3

You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disk?

A. Throw the hard disk into the fire

B. Run the powerful magnets over the hard disk

C. Format the hard disk multiple times using a low level disk utility

D. Overwrite the contents of the hard disk with Junk data

Correct Answer: A

QUESTION 4

Gill is a computer forensics investigator who has been called upon to examine a seized computer. This computer, according to the police, was used by a hacker who gained access to numerous banking institutions to steal customer information. After preliminary investigations, Gill finds in the computer\\'s log files that the hacker was able to gain access to these banks through the use of Trojan horses. The hacker then used these Trojan horses to obtain remote access to the companies\\' domain controllers. From this point, Gill found that the hacker pulled off the SAM files from the domain controllers to then attempt and crack network passwords. What is the most likely password cracking technique used by this hacker to break the user passwords from the SAM files?

A. Syllable attack

B. Hybrid attack

C. Brute force attack

D. Dictionary attack

Correct Answer: D

QUESTION 5

Which rule requires an original recording to be provided to prove the content of a recording?

A. 1004

B. 1002

C. 1003

D. 1005

Correct Answer: B