GCIA Q&As

GIAC Certified Intrusion Analyst

Pass GIAC GCIA Exam with 100% Guarantee

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

https://www.geekcert.com/gcia.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

Adam works as a Computer Hacking Forensic Investigator in a law firm. He has been assigned with his first project. Adam collected all required evidences and clues. He is now required to write an investigative report to present before court

for further prosecution of the case. He needs guidelines to write an investigative report for expressing an opinion. Which of the following are the guidelines to write an investigative report in an efficient way?

Each correct answer represents a complete solution. Choose all that apply.

A. All ideas present in the investigative report should flow logically from facts to conclusions.

B. Opinion of a lay witness should be included in the investigative report.

C. The investigative report should be understandable by any reader.

D. There should not be any assumptions made about any facts while writing the investigative report.

Correct Answer: ACD

QUESTION 2

Which of the following methods is used by forensic investigators to acquire an image over the network in a secure manner?

A. Linux Live CD

B. DOS boot disk

C. Secure Authentication for EnCase (SAFE)

D. EnCase with a hardware write blocker

Correct Answer: C

QUESTION 3

Which of the following commands displays the IPX routing table entries?

A. sh ipx traffic

B. sh ipx int e0

C. sh ipx route

D. sho ipx servers

Correct Answer: C

QUESTION 4

You work as a Network Administrator for PassGuide Inc. The company has deployed an ASA at the network perimeter. Which of the following types of firewall will you use to create two different communications, one between the client and the firewall, and the other between the firewall and the end server?

A. Proxy-based firewall

B. Endian firewall

C. Stateful firewall

D. Packet filter firewall

Correct Answer: A

QUESTION 5

Adam works as a professional Computer Hacking Forensic Investigator. He has been assigned with a project to investigate a computer in the network of SecureEnet Inc. The compromised system runs on Windows operating system. Adam decides to use Helix Live for Windows to gather data and electronic evidences starting with retrieving volatile data and transferring it to server component via TCP/IP. Which of the following application software in Helix Windows Live will he use to retrieve volatile data and transfer it to the server component via TCP/IP?

A. FAU

B. FTK imager

C. Drive Manager

D. FSP

Correct Answer: D