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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

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 information must the fragments carry for the destination host to reassemble them back to the original unfragmented state? Each correct answer represents a complete solution. Choose all that apply.

A. MF flag

B. Offset field

C. MAC address

D. Length of the data

E. IP address

F. IP identification number

Correct Answer: ABDF

QUESTION 3

In which of the following IDS evasion attacks does an attacker send a data packet such that IDS accepts the data packet but the host computer rejects it?

A. Fragmentation overlap attack

B. Evasion attack

C. Fragmentation overwrite attack

D. Insertion attack

Correct Answer: D

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

Which of the following partitions contains the system files that are used to start the operating system?

A. Secondary partition

B. Boot partition

C. Primary partition

D. System partition

Correct Answer: B