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.pass2lead.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

Which of the following is the ability of a hacker to determine the nature of the network?

A. Investigating

B. Profiling

C. Sniffing

D. Intruding

Correct Answer: B

QUESTION 2

You work as a professional Computer Hacking Forensic Investigator. A project has been assigned to you to investigate the DoS attack on a computer network of SecureEnet Inc. Which of the following methods will you perform to accomplish

the task?

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

A. Look for core files or crash dumps on the affected systems.

B. Sniff network traffic to the failing machine.

C. Seize all computers and transfer them to the Forensic lab.

D. Look for unusual traffic on Internet connections and network segments.

Correct Answer: ABD

QUESTION 3

John works as a Network Security Administrator for NetPerfect Inc. The manager of the company has told John that the company\\'s phone bill has increased drastically. John suspects that the company\\'s phone system has been cracked by a malicious hacker. Which attack is used by malicious hackers to crack the phone system?

A. War dialing

B. Sequence++ attack

C. Phreaking

D. Man-in-the-middle attack

Correct Answer: C

QUESTION 4

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 5

Which of the following distributes incorrect IP address to divert the traffic?

A. IP spoofing

B. Domain name server (DNS) poisoning

C. Reverse Address Resolution Protocol

D. Route table poisoning

Correct Answer: B