GCIH Q&As

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

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

https://www.geekcert.com/gcih.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 recommended to include in your incident response jump bag?

A. A switch, because they will not route malicious arp packets

B. A hub, because they are far more reliable than switches

C. A router, because they enable you to monitor a network without being detected

D. A TAP, because you cannot easily sniff network traffic through a switch

Correct Answer: B

QUESTION 2

What information is commonly found in both the header and the possession log of a Chain of Custody?

A. Date and time the evidence was requested by the court

B. Date and time the evidence was checked into evidence locker

C. Date and time the evidence was initially collected

D. Date and time the evidence is classified as reliable

Correct Answer: B

QUESTION 3

Which of the following tools can be used to force password complexity in Linux?

A. PAM

B. Password Guardian

C. Fast Lane

D. Passfilt.dll

Correct Answer: A

On most Linux systems, you can use PAM (the "pluggable authentication module") to enforce password complexity.

QUESTION 4

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following steps of the pre-attack phase:

l Information gathering l Determining network range l Identifying active machines l Finding open ports and applications l OS fingerprinting l Fingerprinting services

Now John wants to perform network mapping of the We-are-secure network. Which of the following tools can he use to accomplish his task?

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

A. Ettercap

B. Traceroute

C. Cheops

D. NeoTrace

Correct Answer: BCD

QUESTION 5

Which tool can sniff probe requests from a wireless client, pretend to be the client\\'s legitimate access point, and offer fake network services to the client?

A. InSSider

B. Aircrack-ng

C. Karmetasploit

D. Wellenreiter

Correct Answer: C