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.leads4pass.com/gcih.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

In general, which method is the fastest for cracking a password?

A. Brute Force

B. Dictionary

C. Manual guessing

D. Hybrid

Correct Answer: B

The dictionary method is fastest for cracking a password, particularly if you have a good dictionary or the users have very weak passwords.

QUESTION 2

During the lessons learned phase which of the following represents the best choice for what you should do to resolve the issue(s) that caused an incident?

A. You must go to management and make a compelling case for fixing the problem that caused the incident in the first place

B. You must fix the problem that caused the incident in the first place by using funds in your yearly budget

C. You must fix the problem that caused the incident in the first place and then tell management how much it cost

D. You must fix the problem that caused the incident in the first place and charge the department responsible for the system(s) that were breached

Correct Answer: A

We want to have constant improvement, so the cause of the incident can be eliminated or minimized. You must go to management and make a compelling case for fixing the problem that caused the incident in the first place. This may mean an alteration to the processes or technology in your environment.

QUESTION 3

Which of the following rootkits adds additional code or replaces portions of an operating system, including both the kernel and associated device drivers?

A. Hypervisor rootkit

B. Boot loader rootkit

C. Kernel level rootkit

D. Library rootkit

Correct Answer: C

QUESTION 4

What advantage does running netstat with the flags "-nao" have over running netstat with the "-na" flags in Windows?

A. The "o" flag shows the socket state

B. The "o" flag shows the process ID (PID)

C. The "o" flag shows UDP connections only

D. The "o" flag shows the user ID (UID) of the owner of the socket

Correct Answer: B

The "-o" flag of netstat, as in "netstat -nao" shows the listening ports, as well as the Process ID of the listening process.

QUESTION 5

Which of the following occurs when a penetration tester attempts to connect to a host with the following command?

net use \\192.168.44.213

A. Guest user account permissions will be granted

B. Local logon credentials will be sent to 192.168.44.213

C. IPC$ share returns a list of running processes

D. Host at 192.168.44.213 will exchange a temporary authentication key

Correct Answer: C

Reference: https://www.programmersought.com/article/23265489705/