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.passapply.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

Which of the following tools is used to download the Web pages of a Website on the local system?

A. wget

B. jplag

C. Nessus

D. Ettercap

Correct Answer: A

QUESTION 2

During the eradication phase, what information should be analyzed to determine the cause and symptoms of an incident?

A. The information gathered during the preparation and recovery phases

B. The information gathered during the identification and containment phases

C. The results of a vulnerability scan conducted during the recovery phase

D. The interviews conducted with the system owners

Correct Answer: B

QUESTION 3

Which UNIX log file contains information about currently logged in users?

A. wtmp

B. btmp

C. utmp

D. lastlog

Correct Answer: A

Reference: https://www.cyberciti.biz/faq/unix-linux-list-current-logged-in-users/

QUESTION 4

In the event there is a disagreement on the events of the incident, how should it be handled in the final report?

A. Have the dissenting individual(s) write and sign a statement detailing the alternate version of events

B. Continue negotiations until all disagreements about events are resolved before submitting the final report

C. Omit any facts or events in dispute entirely from the final report

D. Submit the report with the version of events agreed upon by the majority of team members

Correct Answer: A

If anyone has a strong disagreement about the facts of the matter, he can submit that, and his statement can remain a part of the incident record. It is better to find out that you have a lack of consensus before going to court than during court.

QUESTION 5

Your IDS discovers that an intruder has gained access to your system. You immediately stop that access, change passwords for administrative accounts, and secure your network. You discover an odd account (not administrative) that has permission to remotely access the network. What is this most likely?

A. An example of privilege escalation.

B. A normal account you simply did not notice before. Large networks have a number of accounts; it is hard to track them all.

C. A backdoor the intruder created so that he can re-enter the network.

D. An example of IP spoofing.

Correct Answer: C