GCCC Q&As

GCCC - GIAC Critical Controls Certification (GCCC)

Pass GIAC GCCC Exam with 100% Guarantee

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

https://www.geekcert.com/gccc.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 statements is appropriate in an incident response report?

A. There had been a storm on September 27th that may have caused a power surge

B. The registry entry was modified on September 29th at 22:37

C. The attacker may have been able to access the systems due to missing KB2965111

D. The backup process may have failed at 2345 due to lack of available bandwidth

Correct Answer: B

QUESTION 2

As part of a scheduled network discovery scan, what function should the automated scanning tool perform?

A. Uninstall listening services that have not been used since the last scheduled scan

B. Compare discovered ports and services to a known baseline to report deviations

C. Alert the incident response team on ports and services added since the last scan

D. Automatically close ports and services not included in the current baseline

Correct Answer: B

QUESTION 3

IDS alerts at Service Industries are received by email. A typical day process over 300 emails with fewer than 50 requiring action. A recent attack was successful and went unnoticed due to the number of generated alerts.

What should be done to prevent this from recurring?

A. Tune the IDS rules to decrease false positives.

B. Increase the number of staff responsible for processing IDS alerts.

C. Change the alert method from email to text message.

D. Configure the IDS alerts to only alert on high priority systems.

Correct Answer: A

QUESTION 4

Which of the following archiving methods would maximize log integrity?

A. DVD-R

B. USB flash drive

C. Magnetic Tape

D. CD-RW

Correct Answer: A

QUESTION 5

What is a recommended defense for the CIS Control for Application Software Security?

A. Keep debugging code in production web applications for quick troubleshooting

B. Limit access to the web application production environment to just the developers

C. Run a dedicated vulnerability scanner against backend databases

D. Display system error messages for only non-kernel related events

Correct Answer: C