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.leads4pass.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 is a responsibility of a change management board?

A. Reviewing log files for unapproved changes

B. Approving system baseline configurations.

C. Providing recommendations for the changes

D. Reviewing configuration of the documents

Correct Answer: B

QUESTION 2

Beta corporation is doing a core evaluation of its centralized logging capabilities. The security staff suspects that the central server has several log files over the past few weeks that have had their contents changed. Given this concern, and the need to keep archived logs for log correction applications, what is the most appropriate next steps?

A. Keep the files in the log archives synchronized with another location.

B. Store the files read-only and keep hashes of the logs separately.

C. Install a tier one timeserver on the network to keep log devices synchronized.

D. Encrypt the log files with an asymmetric key and remove the cleartext version.

Correct Answer: B

QUESTION 3

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

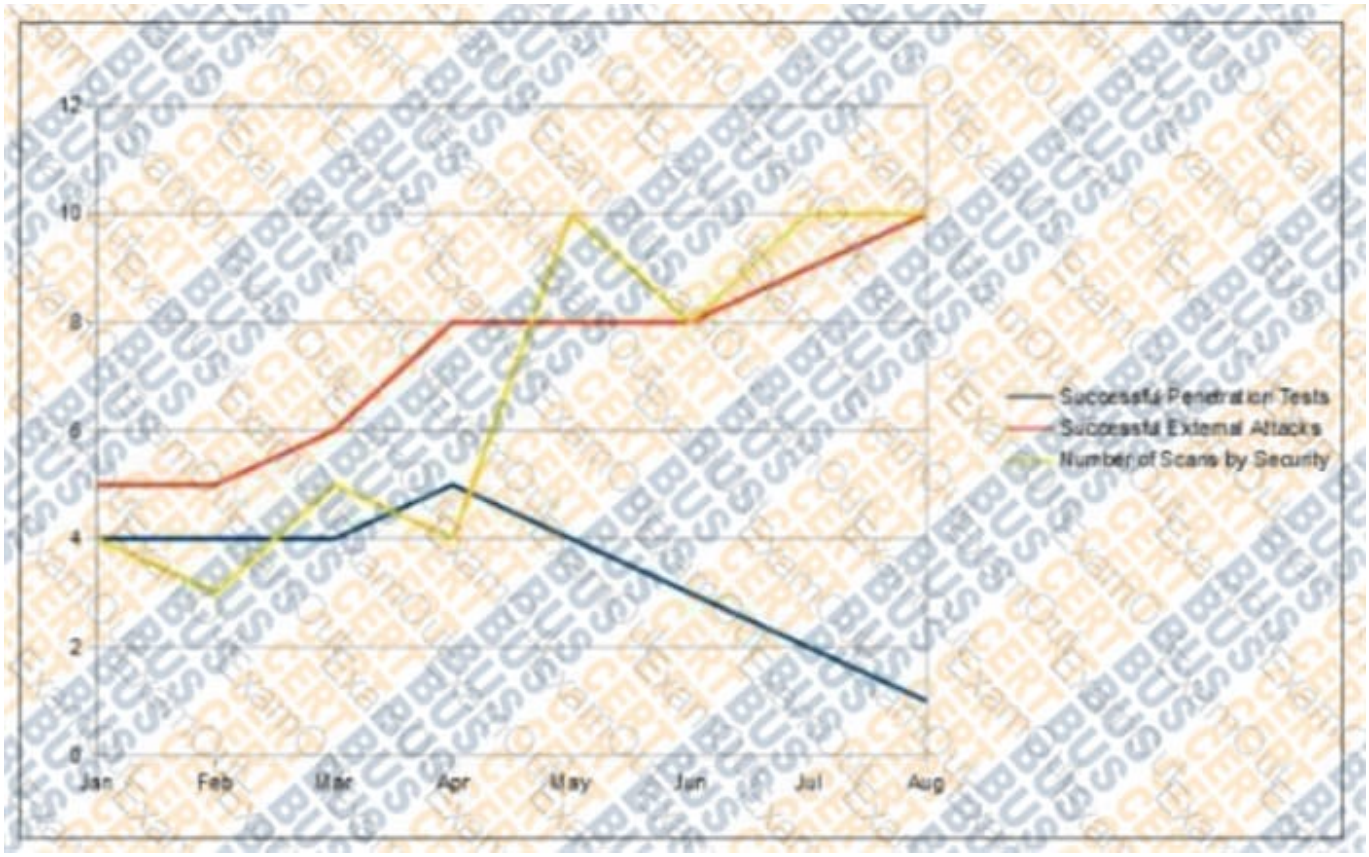
D. The backup process may have failed at 2345 due to lack of available bandwidth

Correct Answer: B

QUESTION 4

An organization has implemented a control for penetration testing and red team exercises conducted on their network. They have compiled metrics showing the success of the penetration testing (Penetration Tests), as well as the number of actual adversary attacks they have sustained (External Attacks). Assess the metrics below and determine the

appropriate interpretation with respect to this control.



A. The blue team is adequately protecting the network

B. There are too many internal penetration tests being conducted

C. The methods the red team is using are not effectively testing the network

D. The red team is improving their capability to measure network security

Correct Answer: C

QUESTION 5

Which type of scan is best able to determine if user workstations are missing any important patches?

A. A network vulnerability scan using aggressive scanning

B. A source code scan

C. A port scan using banner grabbing

D. A web application/database scan

E. A vulnerability scan using valid credentials

Correct Answer: E

GCCC PDF Dumps GCCC Practice Test GCCC Braindumps