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.passapply.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

An organization wants to test its procedure for data recovery. Which of the following will be most effective?

A. Verifying a file can be recovered from backup media

B. Verifying that backup process is running when it should

C. Verifying that network backups can\\'t be read in transit

D. Verifying there are no errors in the backup server logs

Correct Answer: A

QUESTION 2

An administrator looking at a web application\\'s log file found login attempts by the same host over several seconds. Each user ID was attempted with three different passwords. The event took place over 5 seconds.

ROOT TEST ADMIN SQL USER NAGIOSGUEST

What is the most likely source of this event?

A. An IT administrator attempting to use outdated credentials to enter the site

B. An attempted Denial of Service attack by locking out administrative accounts

C. An automated tool that attempts to use a dictionary attack to infiltrate a website

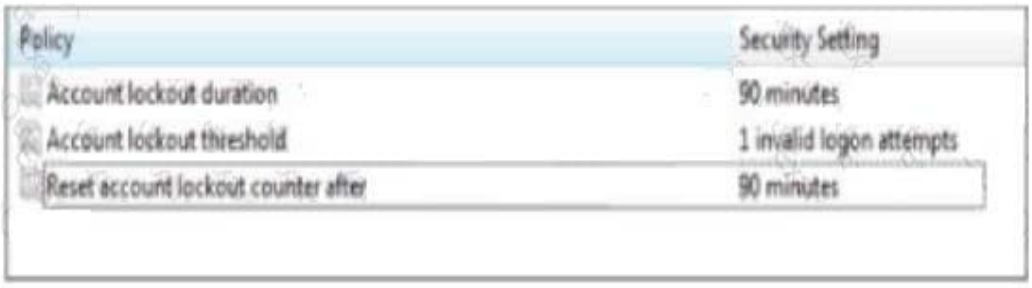
D. An attempt to use SQL Injection to gain information from a web-connected database

Correct Answer: C

QUESTION 3

An organization is implementing a control for the Account Monitoring and Control CIS Control, and have set the Account Lockout Policy as shown below. What is the risk presented by these settings?

(Image)



A. Brute-force password attacks could be more effective.

B. Legitimate users could be unable to access resources.

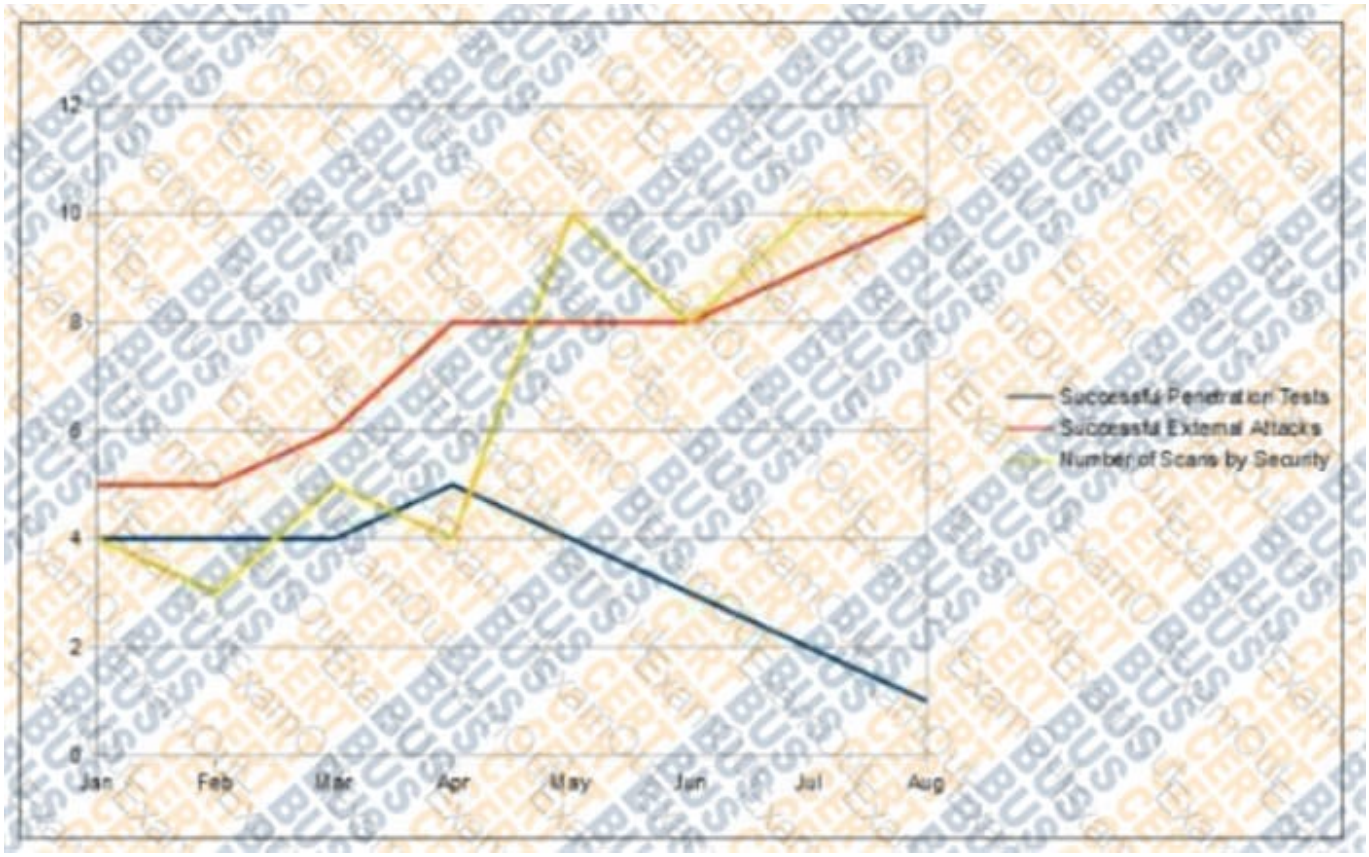
C. Password length and complexity will be automatically reduced.

D. Once accounts are locked, they cannot be unlocked.

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 of the following is a requirement in order to implement the principle of least privilege?

A. Mandatory Access Control (MAC)

B. Data normalization

C. Data classification

D. Discretionary Access Control (DAC)

Correct Answer: C

QUESTION 6

Which approach is recommended by the CIS Controls for performing penetration tests?

A. Document a single vulnerability per system

B. Utilize a single attack vector at a time

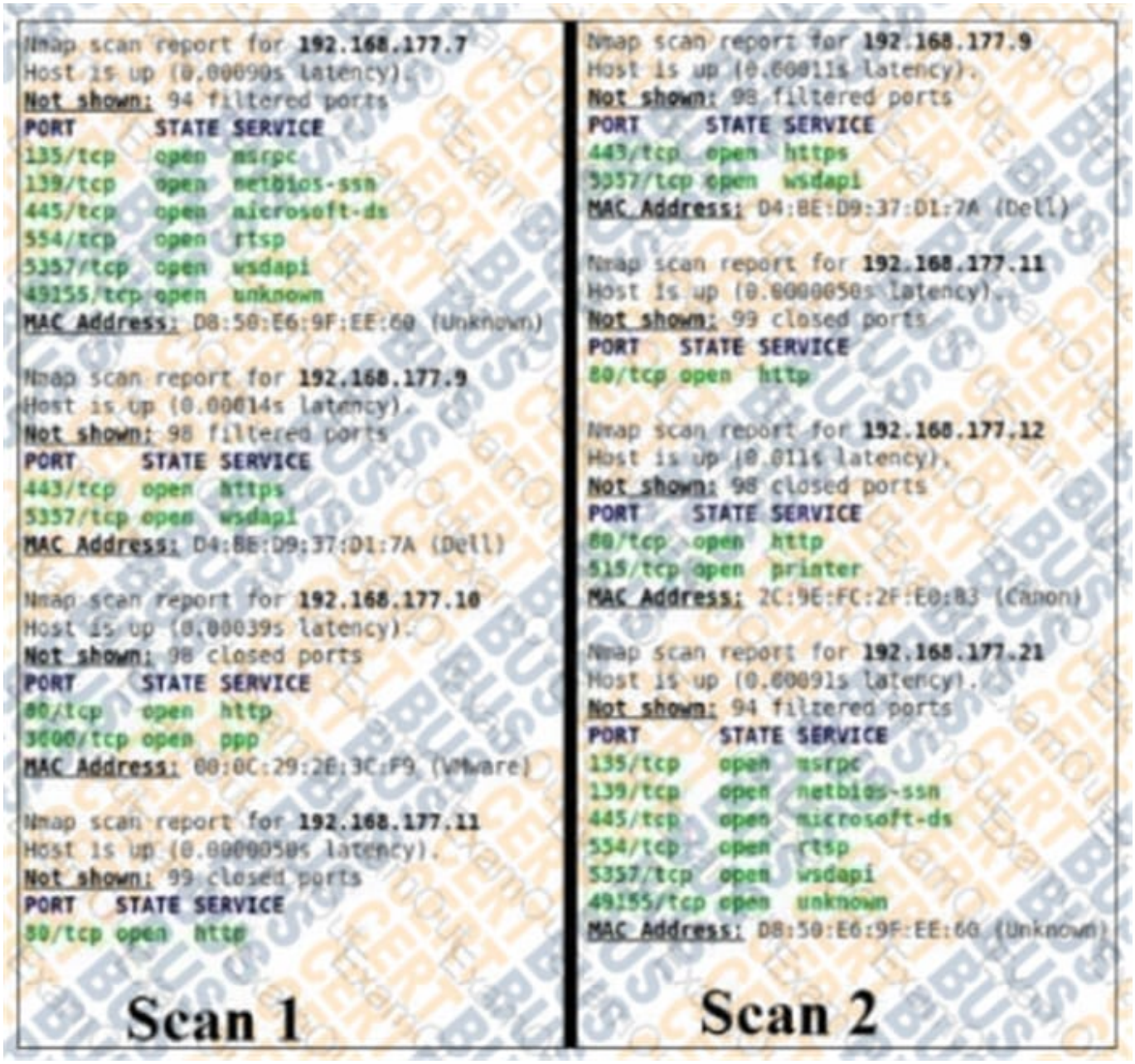
C. Complete intrusive tests on test systems

D. Execute all tests during network maintenance windows

Correct Answer: C

QUESTION 7

Scan 1 was taken on Monday. Scan 2 was taken of the same network on Wednesday. Which of the following findings is accurate based on the information contained in the scans?



A. The host located at 192.168.177.7 is no longer on the network

B. The host with MAC Address D8:50:E6:9F:EE:60 is no longer on the network

C. The host located at 192.168.177.21 is a new host on the network

D. The host with MAC Address D8:50:E6:9F:EE:60 had an IP address change

Correct Answer: D

QUESTION 8

Which of the following is a benefit of stress-testing a network?

A. To determine device behavior in a DoS condition.

B. To determine bandwidth needs for the network.

C. To determine the connectivity of the network

D. To determine the security configurations of the network

Correct Answer: A

QUESTION 9

An auditor is focusing on potential vulnerabilities. Which of the following should cause an alert?

A. Workstation on which a domain admin has never logged in

B. Windows host with an uptime of 382 days

C. Server that has zero browser plug-ins

D. Fully patched guest machine that is not in the asset inventory

Correct Answer: B

QUESTION 10

When evaluating the Wireless Access Control CIS Control, which of the following systems needs to be tested?

A. Log management system

B. 802.1x authentication systems

C. Data classification and access baselines

D. PII data scanner

Correct Answer: B

QUESTION 11

If an attacker wanted to dump hashes or run wmic commands on a target machine, which of the following tools would he use?

A. Mimikatz

B. OpenVAS

C. Metasploit

Correct Answer: C

QUESTION 12

Which of the following is used to prevent spoofing of e-mail addresses?

A. Sender Policy Framework

B. DNS Security Extensions

C. Public-Key Cryptography

D. Simple Mail Transfer Protocol

Correct Answer: A

QUESTION 13

Implementing which of the following will decrease spoofed e-mail messages?

A. Finger Protocol

B. Sender Policy Framework

C. Network Address Translation

D. Internet Message Access Protocol

Correct Answer: B

QUESTION 14

An organization is implementing an application software security control their custom-written code that provides web--based database access to sales partners. Which action will help mitigate the risk of the application being compromised?

A. Providing the source code for their web application to existing sales partners

B. Identifying high-risk assets that are on the same network as the web application server

C. Creating signatures for their IDS to detect attacks specific to their web application

D. Logging the connection requests to the web application server from outside hosts

Correct Answer: C

QUESTION 15

An organization has implemented a policy to detect and remove malicious software from its network. Which of the following actions is focused on correcting rather than preventing attack?

A. Configuring a firewall to only allow communication to whitelisted hosts and ports

B. Using Network access control to disable communication by hosts with viruses

C. Disabling autorun features on all workstations on the network

D. Training users to recognize potential phishing attempts

Correct Answer: B