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.pass4itsure.com/gccc.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

After installing a software package on several workstations, an administrator discovered the software opened network port TCP 23456 on each workstation. The port is part of a software management function that is not needed on corporate workstations. Which actions would best protect the computers with the software package installed?

A. Document the port number and request approval from a change control group

B. Redirect traffic to and from the software management port to a non-default port

C. Block TCP 23456 at the network perimeter firewall

D. Determine which service controls the software management function and opens the port, and disable it

Correct Answer: D

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

Given the audit finding below, which CIS Control was being measured?

```
* 58% percent of system assets do not require multi-factor authentication for elevated account access
* 9% percent of system assets do not enforce encrypted channels for elevated account activity
```

A. Controlled Access Based on the Need to Know

B. Controlled Use of Administrative Privilege

C. Limitation and Control of Network Ports, Protocols and Services

D. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

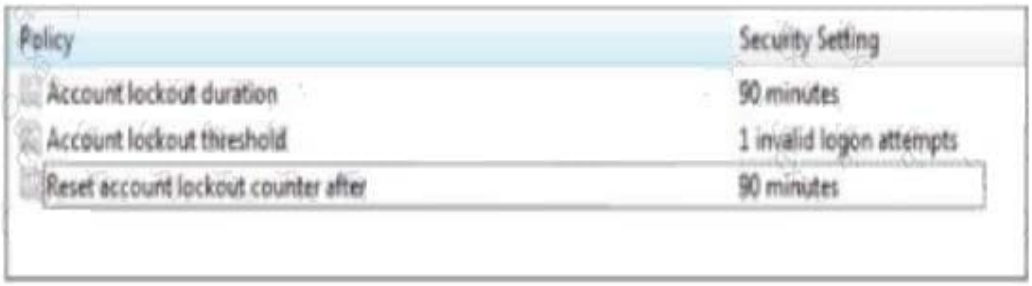
E. Inventory and Control of Hardware Assets

Correct Answer: B

QUESTION 4

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)



Policy	Security Setting
Account lockout duration	90 minutes
Account lockout threshold	1 invalid logon attempts
Reset account lockout counter after	90 minutes

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

B. Legitimate users could be unable to access resources.

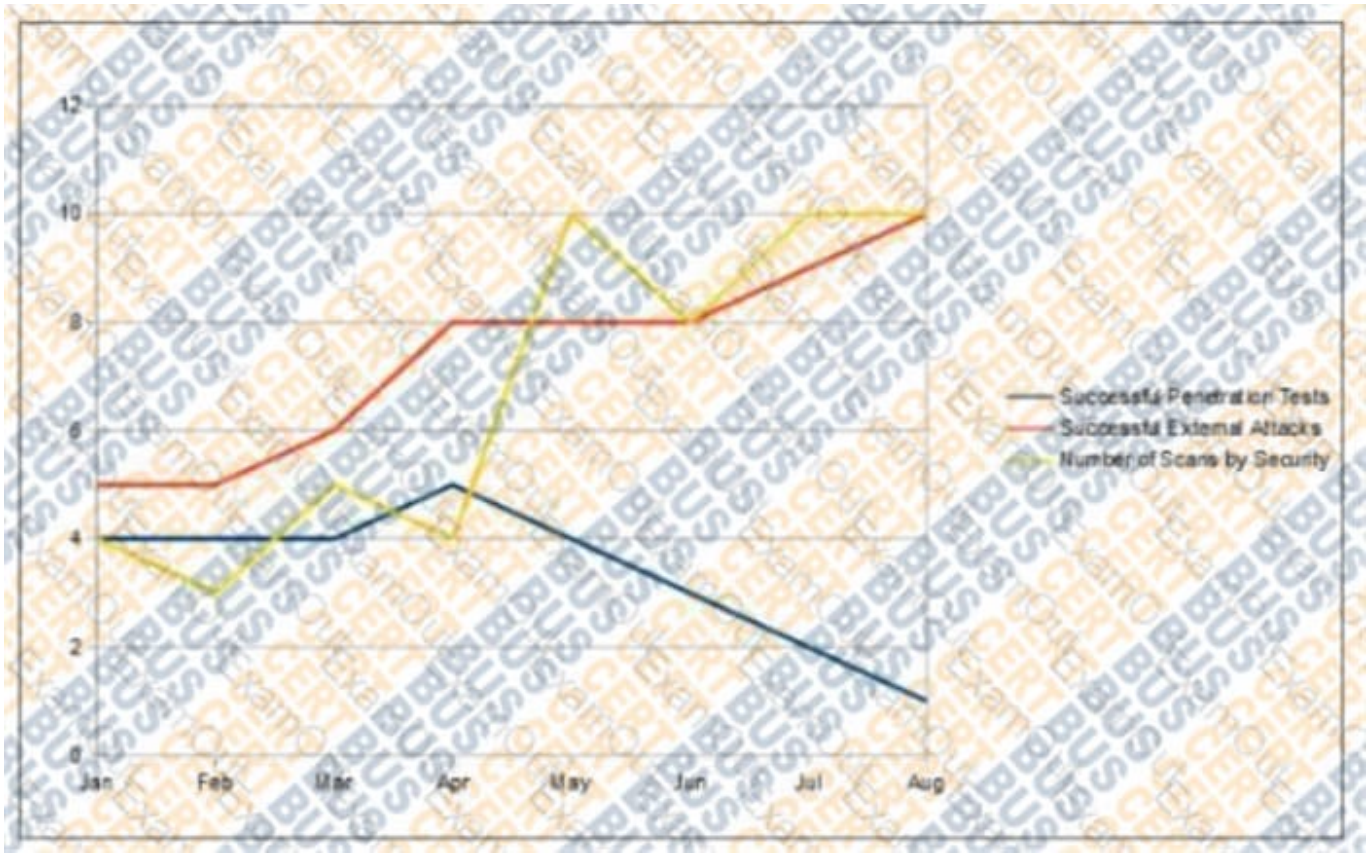
C. Password length and complexity will be automatically reduced.

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

Correct Answer: B

QUESTION 5

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