GCCC Q&As

GCCC - GIAC Critical Controls Certification (GCCC)

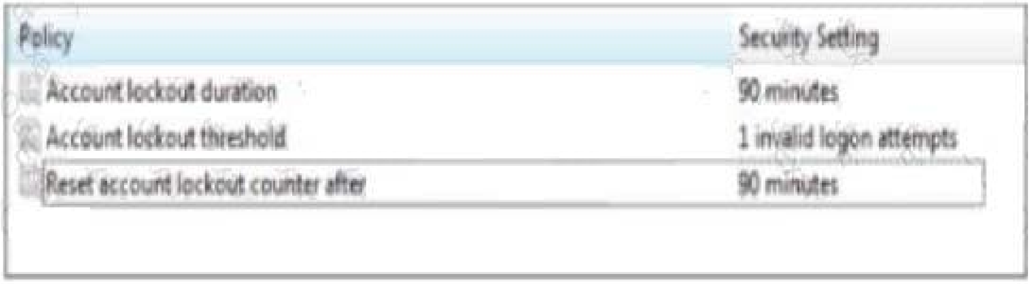
Pass GIAC GCCC Exam with 100% Guarantee

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

QUESTION 1

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 2

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 3

An organization has implemented a policy to continually detect and remove malware from its network. Which of the following is a detective control needed for this?

A. Host-based firewall sends alerts when packets are sent to a closed port

B. Network Intrusion Prevention sends alerts when RST packets are received

C. Network Intrusion Detection devices sends alerts when signatures are updated

D. Host-based anti-virus sends alerts to a central security console

Correct Answer: D

QUESTION 4

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

QUESTION 5

Allied services have recently purchased NAC devices to detect and prevent non-company owned devices from attaching to their internal wired and wireless network. Corporate devices will be automatically added to the approved device list by querying Active Directory for domain devices. Non-approved devices will be placed on a protected VLAN with no network access. The NAC also offers a web portal that can be integrated with Active Directory to allow for employee device registration which will not be utilized in this deployment. Which of the following recommendations would make NAC installation more secure?

A. Enforce company configuration standards for personal mobile devices

B. Configure Active Directory to push an updated inventory to the NAC daily

C. Disable the web portal device registration service

D. Change the wireless password following the NAC implementation

Correct Answer: C