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

QUESTION 1

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

QUESTION 2

Which of the following is necessary to automate a control for Inventory and Control of Hardware Assets?

A. A method of device scanning

B. A centralized time server

C. An up-to-date hardening guide

D. An inventory of unauthorized assets

Correct Answer: A

QUESTION 3

Review the below results of an audit on a server. Based on these results, which document would you recommend be reviewed for training or updates?

A. Procedure for authorizing remote server access

B. Procedure for modifying file permissions

C. Procedure for adjusting network share permissions

D. Procedure for setting and resetting user passwords

Correct Answer: D

QUESTION 4

A breach was discovered after several customers reported fraudulent charges on their accounts. The attacker had exported customer logins and cracked passwords that were hashed but not salted. Customers were made to reset their passwords.

Shortly after the systems were cleaned and restored to service, it was discovered that a compromised system administrator\\'s account was being used to give the attacker continued access to the network. Which CIS Control failed in the continued access to the network?

A. Maintenance, Monitoring, and Analysis of Audit Logs

B. Controlled Use of Administrative Privilege

C. Incident Response and Management

D. Account Monitoring and Control

Correct Answer: C

QUESTION 5

An organization is implementing a control for the Limitation and Control of Network Ports, Protocols, and Services CIS Control. Which action should they take when they discover that an application running on a web server is no longer needed?

A. Uninstall the application providing the service

B. Turn the service off in the host configuration files

C. Block the protocol for the unneeded service at the firewall

D. Create an access list on the router to filter traffic to the host

Correct Answer: A

QUESTION 6

An organization has failed a test for compliance with a policy of continual detection and removal of malicious software on its network. Which of the following errors is the root cause?

A. A host ran malicious software that exploited a vulnerability for which there was no patch

B. The security console alerted when a host anti-virus ran whitelisted software

C. The intrusion prevention system failed to update to the newest signature list

D. A newly discovered vulnerability was not detected by the intrusion detection system

Correct Answer: C

QUESTION 7

What is the business goal of the Inventory and Control of Software Assets Control?

A. Only authorized software should be installed on the agency \\'s c omput er s ys t ems

B. All software conforms to licensing requirements for the business

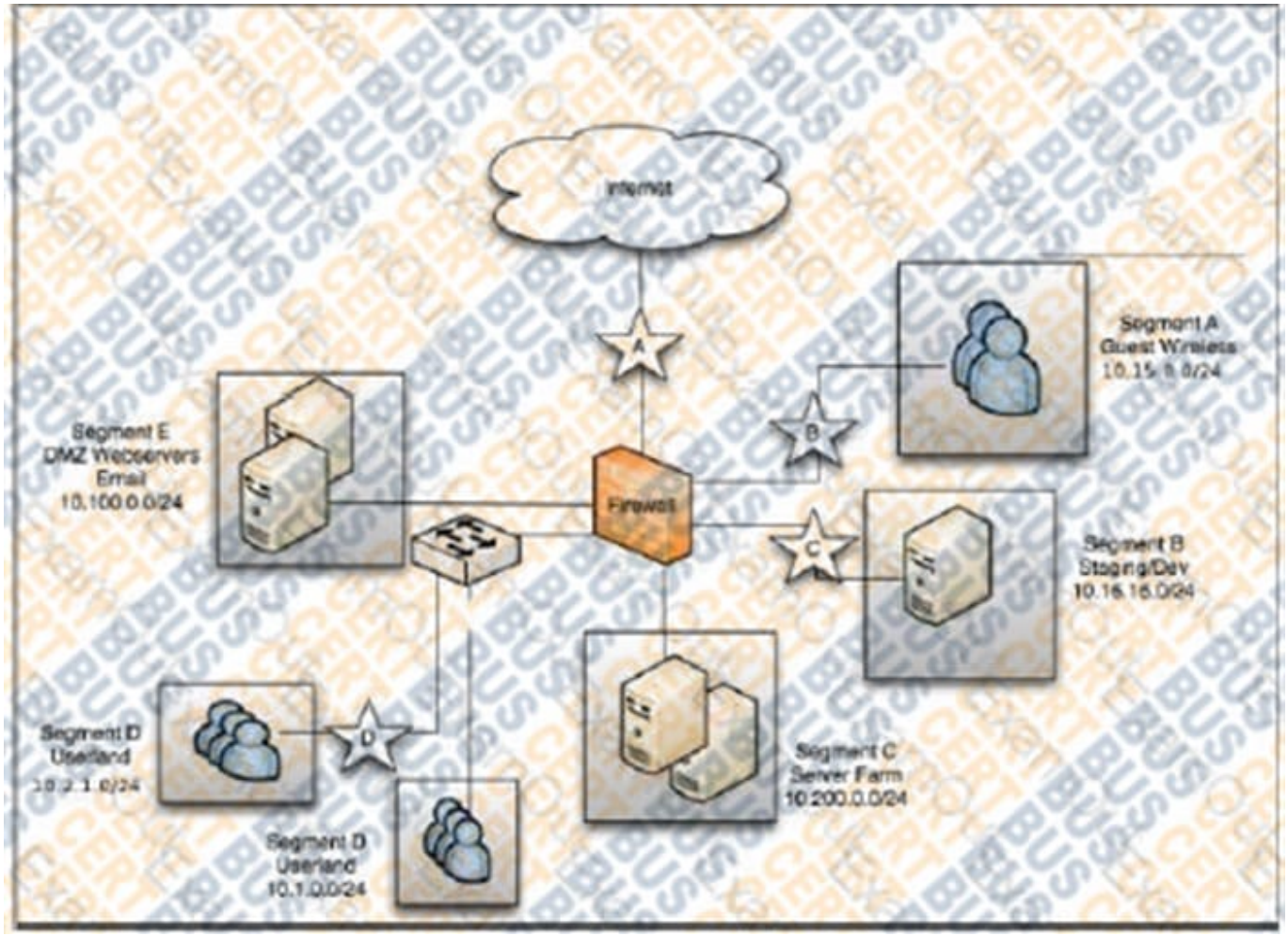
C. Accurate software versions are captured to enable patching

D. Accurate software versions and counts are documented for licensing updates

Correct Answer: A

QUESTION 8

An organization has installed a firewall for Boundary Defense. It allows only outbound traffic from internal workstations for web and SSH, allows connections from the internet to the DMZ, and allows guest wireless access to the internet only. How can an auditor validate these rules?



A. Check for packets going from the Internet to the Web server

B. Try to send email from a wireless guest account

C. Check for packages going from the web server to the user workstations

D. Try to access the internal network from the wireless router

Correct Answer: D

QUESTION 9

An analyst investigated unused organizational accounts. The investigation found that:

-10% of accounts still have their initial login password, indicating they were never used

-10% of accounts have not been used in over six months

Which change in policy would mitigate the security risk associated with both findings?

A. Users are required to change their password at the next login after three months

B. Accounts must have passwords of at least 8 characters, with one number or symbol

C. Accounts without login activity for 15 days are automatically locked

Correct Answer: C

QUESTION 10

What could a security team use the command line tool Nmap for when implementing the Inventory and Control of Hardware Assets Control?

A. Control which devices can connect to the network

B. Passively identify new devices

C. Inventory offline databases

D. Actively identify new servers

Correct Answer: D

QUESTION 11

To effectively implement the Data Protection CIS Control, which task needs to be implemented first?

A. The organization\\'s proprietary data needs to be encrypted

B. Employees need to be notified that proprietary data should be protected

C. The organization\\'s proprietary data needs to be identified

D. Appropriate file content matching needs to be configured

Correct Answer: C

QUESTION 12

Which of the following items would be used reactively for incident response?

A. A schedule for creating and storing backup

B. A phone tree used to contact necessary personnel

C. A script used to verify patches are installed on systems

D. An IPS rule that prevents web access from international locations

Correct Answer: B

QUESTION 13

According to attack lifecycle models, what is the attacker\\'s first step in compromising an organization?

A. Privilege Escalation

B. Exploitation

C. Initial Compromise

D. Reconnaissance

Correct Answer: D

QUESTION 14

John a network administrator at Northeast High School. Faculty have been complaining that although they can detect and authenticate to the faculty wireless network, they are unable to connect. While troubleshooting, John discovers that the wireless network server is out of DHCP addresses due to a large number of unauthorized student devices connecting to the network. Which course of action would be an effective temporary stopgap to secure the network until a permanent solution can be found?

A. Limit access to allowed MAC addresses

B. Increase the size of the DHCP pool

C. Change the password immediately

D. Shorten the DHCP lease time

Correct Answer: C

QUESTION 15

What is the relationship between a service and its associated port?

A. A service closes a port after a period of inactivity

B. A service relies on the port to select the protocol

C. A service sets limits on the volume of traffic sent through the port

D. A service opens the port and listens for network traffic

Correct Answer: D