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:

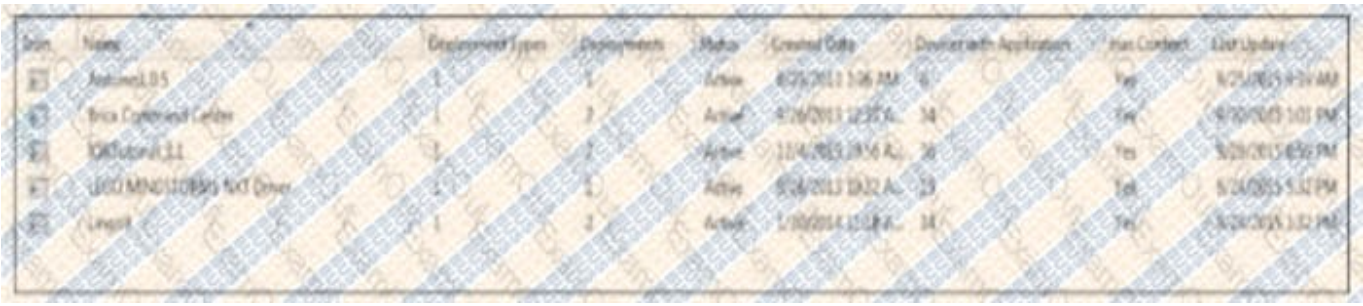
https://www.pass4itsure.com/gccc.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is the list displaying?



A. Allowed program in a software inventory application

B. Unauthorized programs detected in a software inventory

C. Missing patches from a patching server

D. Installed software on an end-user device

Correct Answer: A

QUESTION 2

How can the results of automated network configuration scans be used to improve the security of the network?

A. Reports can be sent to the CIO for performance benchmarks

B. Results can be provided to network engineers as actionable feedback

C. Scanners can correct network configurations issues

D. Results can be included in audit evidence failures

Correct Answer: B

QUESTION 3

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

QUESTION 4

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 5

What documentation should be gathered and reviewed for evaluating an Incident Response program?

A. Staff member interviews

B. NIST Cybersecurity Framework

C. Policy and Procedures

D. Results from security training assessments

Correct Answer: C

QUESTION 6

An organization has created a policy that allows software from an approved list of applications to be installed on workstations. Programs not on the list should not be installed. How can the organization best monitor compliance with the policy?

A. Performing regular port scans of workstations on the network

B. Auditing Active Directory and alerting when new accounts are created

C. Creating an IDS signature to alert based on unknown "User-Agent " strings

D. Comparing system snapshots and alerting when changes are made

Correct Answer: C

QUESTION 7

Why is it important to enable event log storage on a system immediately after it is installed?

A. To allow system to be restored to a known good state if it is compromised

B. To create the ability to separate abnormal behavior from normal behavior during an incident

C. To compare it performance with other systems already on the network

D. To identify root kits included on the system out of the box

Correct Answer: B

QUESTION 8

Which of the following actions would best mitigate against phishing attempts such as the example below?

A. Establishing email filters to block no-reply address emails

B. Making web filters to prevent accessing Google Docs

C. Having employee\\'s complete user awareness training

D. Recommending against the use of Google Docs

Correct Answer: C

QUESTION 9

Which of the following will decrease the likelihood of eavesdropping on a wireless network?

A. Broadcasting in the 5Ghz frequency

B. Using Wired Equivalent Protocol (WEP)

C. Using EAP/TLS authentication and WPA2 with AES encryption

D. Putting the wireless network on a separate VLAN

Correct Answer: C

QUESTION 10

Of the options shown below, what is the first step in protecting network devices?

A. Creating standard secure configurations for all devices

B. Scanning the devices for known vulnerabilities

C. Implementing IDS to detect attacks

D. Applying all known security patches

Correct Answer: A

QUESTION 11

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 12

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 13

An auditor is validating the policies and procedures for an organization with respect to a control for Data Recovery. The organization\\'s control states they will completely back up critical servers weekly, with incremental backups every four hours. Which action will best verify success of the policy?

A. Verify that the backup media cannot be read without the encryption key

B. Check the backup logs from the critical servers and verify there are no errors

C. Select a random file from a critical server and verify it is present in a backup set

D. Restore the critical server data from backup and see if data is missing

Correct Answer: D

QUESTION 14

Janice is auditing the perimeter of the network at Sugar Water InC. According to documentation, external SMTP traffic is only allowed to and from 10.10.10.25. Which of the following actions would demonstrate the rules are configured incorrectly?

A. Receive spam from a known bad domain

B. Receive mail at Sugar Water Inc. account using Outlook as a mail client

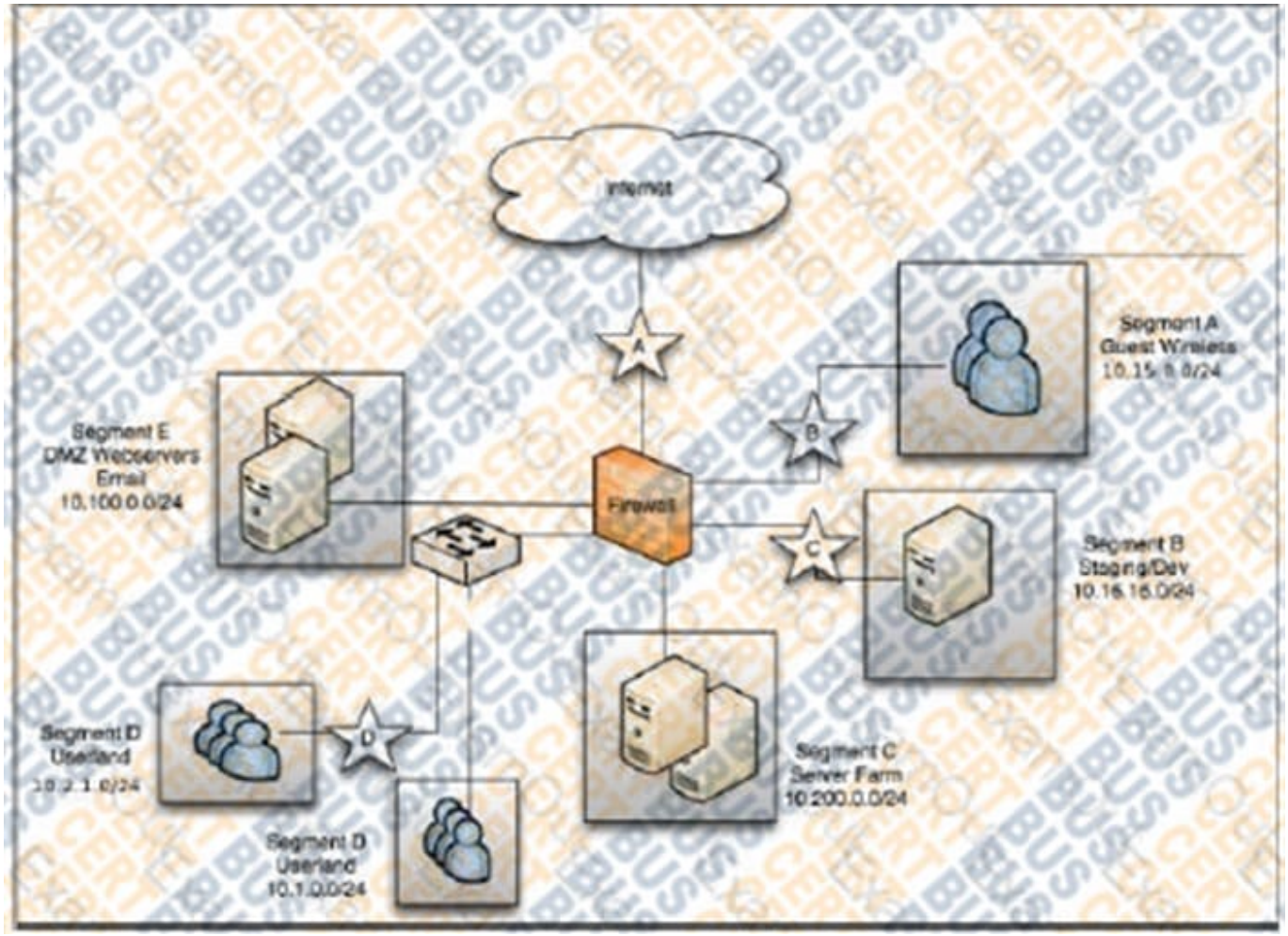
C. Successfully deliver mail from another host inside the network directly to an external contact

D. Successfully deliver mail from web client using another host inside the network to an external contact.

Correct Answer: C

QUESTION 15

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