

## GIAC GCCC Real 2025 Braindumps Mock Exam Dumps [Q45-Q59]



### GIAC GCCC Real 2025 Braindumps Mock Exam Dumps GCCC Exam Questions | Real GCCC Practice Dumps QUESTION 45

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?

```
sshHydra
Target Passwords Tuning Specific Start
Output
Hydra v2.10.3 (c)2012 by van Hauser/THC & David Maciejak - For legal purposes
Hydra (http://www.thc.org/thc-hydra) starting at 2014-04-22 17:04:21
[WARNING] Restorefile (hydra.restore) from a previous session could prevent overwriting, you have 10 seconds to abort (press ctrl-c) or to continue (press any other key)
[DATA] 5 tasks, 1 server, 18 login tries (l0:p0:1), - 3 tasks failed
[22][ssh] host 192.168.50.15: login: dave, password: Spring2014
[22][ssh] host 192.168.50.15: login: jerry, password: Fall2013
[22][ssh] host 192.168.50.15: login: ted, password: Spring2014
1 of 3 target successes found, 3 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-04-22 17:04:47
sFinished

Start Stop Save Output Clear Output
hydra -e 22 -L /root/daemon.txt -R /root/daemon.txt -t 192.168.50.15 ssh
```

- \* Procedure for authorizing remote server access
- \* Procedure for modifying file permissions
- \* Procedure for adjusting network share permissions
- \* Procedure for setting and resetting user passwords

#### QUESTION 46

What is an organization's goal in deploying a policy to encrypt all mobile devices?

- \* Enabling best practices for the protection of their software licenses
- \* Providing their employees, a secure method of connecting to the corporate network
- \* Controlling unauthorized access to sensitive information
- \* Applying the principle of defense in depth to their mobile devices

#### QUESTION 47

Based on the data shown below.



Which wireless access point has the manufacturer default settings still in place?

- \* Starbucks
- \* Linksys
- \* Hhonors
- \* Interwebz

#### QUESTION 48

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

- \* A schedule for creating and storing backup

- \* A phone tree used to contact necessary personnel
- \* A script used to verify patches are installed on systems
- \* An IPS rule that prevents web access from international locations

#### QUESTION 49

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.



- \* The blue team is adequately protecting the network
- \* There are too many internal penetration tests being conducted
- \* The methods the red team is using are not effectively testing the network
- \* The red team is improving their capability to measure network security

#### QUESTION 50

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

- \* Mandatory Access Control (MAC)
- \* Data normalization
- \* Data classification
- \* Discretionary Access Control (DAC)

#### QUESTION 51

Which projects enumerates or maps security issues to CVE?

- \* CIS Controls
- \* SCAP
- \* ISO 2700
- \* NIST

### QUESTION 52

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

- \* The organization's proprietary data needs to be encrypted
- \* Employees need to be notified that proprietary data should be protected
- \* The organization's proprietary data needs to be identified
- \* Appropriate file content matching needs to be configured

### QUESTION 53

Which of the following archiving methods would maximize log integrity?

- \* DVD-R
- \* USB flash drive
- \* Magnetic Tape
- \* CD-RW

### QUESTION 54

Which CIS Control includes storing system images on a hardened server, scanning production systems for out-of-date software, and using file integrity assessment tools like tripwire?

- \* Inventory of Authorized and Unauthorized Software
- \* Continuous Vulnerability Management
- \* Secure Configurations for Network Devices such as Firewalls, Routers and Switches
- \* Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

### QUESTION 55

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?

- \* Verify that the backup media cannot be read without the encryption key
- \* Check the backup logs from the critical servers and verify there are no errors
- \* Select a random file from a critical server and verify it is present in a backup set
- \* Restore the critical server data from backup and see if data is missing

### QUESTION 56

Below is a screenshot from a deployed next-generation firewall. These configuration settings would be a defensive measure for which CIS Control?

## URI List Configuration

Allowed URI List:	<input type="text" value="None"/>
Forbidden URI List:	<input type="text" value="None"/>
URI List Searching Order:	<input type="text" value="Allowed URI List First"/>
Operation for Forbidden URI List:	<input type="text" value="Block"/>

## Category Configuration

#	Category	Operation
11.	Gambling	<input type="text" value="Block"/>
12.	Alcohol/Tobacco	<input type="text" value="Block"/>
13.	Chat/Instant Messaging (IM)	<input type="text" value="Allow"/>
14.	Arts/Entertainment	<input type="text" value="Block"/>
15.	Business and Economy	<input type="text" value="Allow"/>

- \* Controlled Access Based on the Need to Know
- \* Limitation and Control of Network Ports, Protocols and Services
- \* Email and Web Browser Protections
- \* Secure Configuration for Network Devices, such as Firewalls, Routers and Switches.

### QUESTION 57

An attacker is able to successfully access a web application as root using `&#8216; or 1 = 1 .` as the password. The successful access indicates a failure of what process?

- \* Input Validation
- \* Output Sanitization
- \* URL Encoding
- \* Account Management

### QUESTION 58

A global corporation has major data centers in Seattle, New York, London and Tokyo. Which of the following is the correct approach from an intrusion detection and event correlation perspective?

- \* Configure all data center systems to use local time
- \* Configure all data center systems to use GMT time
- \* Configure all systems to use their default time settings
- \* Synchronize between Seattle and New York, and use local time for London and Tokyo

### QUESTION 59

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

- \* Privilege Escalation
- \* Exploitation
- \* Initial Compromise
- \* Reconnaissance

**Verified GCCC Exam Dumps Q&As - Provide GCCC with Correct Answers:**  
<https://www.vceprep.com/GCCC-latest-vce-prep.html>