100% PASS RATE Cyber Security GCCC Certified Exam DUMP with 95 Questions [Q42-Q61

100% PASS RATE Cyber Security GCCC Certified Exam DUMP with 95 Questions
Updates For the Latest GCCC Free Exam Study Guide!

NEW QUESTION 42

Which CIS Control includes storing system images on a hardened server, scanning production systems for out-of-date software, and using file integrity assessment tools like tripwire?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

NEW QUESTION 43

An auditor is focusing on potential vulnerabilities. Which of the following should cause an alert?
* Workstation on which a domain admin has never logged in
* Windows host with an uptime of 382 days
* Server that has zero browser plug-ins
* Fully patched guest machine that is not in the asset inventory

NEW QUESTION 44

Which of the following is a reliable way to test backed up data?
* Verify the file size of the backup
* Confirm the backup service is running at the proper time
* Compare data hashes of backed up data to original systems
* Restore the data to a system

NEW QUESTION 45

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 host ran malicious software that exploited a vulnerability for which there was no patch
* The security console alerted when a host anti-virus ran whitelisted software
* The intrusion prevention system failed to update to the newest signature list
* A newly discovered vulnerability was not detected by the intrusion detection system

NEW QUESTION 46

What type of Unified Modelling Language (UML) diagram is used to show dependencies between logical groupings in a system?
* Package diagram
* Deployment diagram
* Class diagram
* Use case diagram

NEW QUESTION 47

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?
* Document the port number and request approval from a change control group
* Redirect traffic to and from the software management port to a non-default port
* Block TCP 23456 at the network perimeter firewall
* Determine which service controls the software management function and opens the port, and disable it

NEW QUESTION 48

Which type of scan is best able to determine if user workstations are missing any important patches?
* A network vulnerability scan using aggressive scanning
* A source code scan
* A port scan using banner grabbing
* A web application/database scan
* A vulnerability scan using valid credentials

NEW QUESTION 49

What is the relationship between a service and its associated port?
* A service closes a port after a period of inactivity
* A service relies on the port to select the protocol
* A service sets limits on the volume of traffic sent through the port
* A service opens the port and listens for network traffic

NEW QUESTION 50

Acme Corporation is doing a core evaluation of its centralized logging capabilities. Which of the following scenarios indicates a failure in more than one CIS Control?
* The loghost is missing logs from 3 servers in the inventory
* The loghost is receiving logs from hosts with different timezone values
* The loghost time is out-of-sync with an external host
* The loghost is receiving out-of-sync logs from undocumented servers

NEW QUESTION 51

Which of the following is used to prevent spoofing of e-mail addresses?
* Sender Policy Framework
* DNS Security Extensions
* Public-Key Cryptography
* Simple Mail Transfer Protocol

NEW QUESTION 52

A security incident investigation identified the following modified version of a legitimate system file on a compromised client:

C:WindowsSystem32winxml.dll Addition Jan. 16, 2014 4:53:11 PM

The infection vector was determined to be a vulnerable browser plug-in installed by the user. Which of the organization&#8217;s CIS Controls failed?
* Application Software Security
* Inventory and Control of Software Assets
* Maintenance, Monitoring, and Analysis of Audit Logs
* Inventory and Control of Hardware Assets

NEW QUESTION 53

What is a zero-day attack?
* An attack that has a known attack signature but no available patch
* An attack that utilizes a vulnerability unknown to the software developer
* An attack that deploys at the end of a countdown sequence
* An attack that is launched the day the patch is released

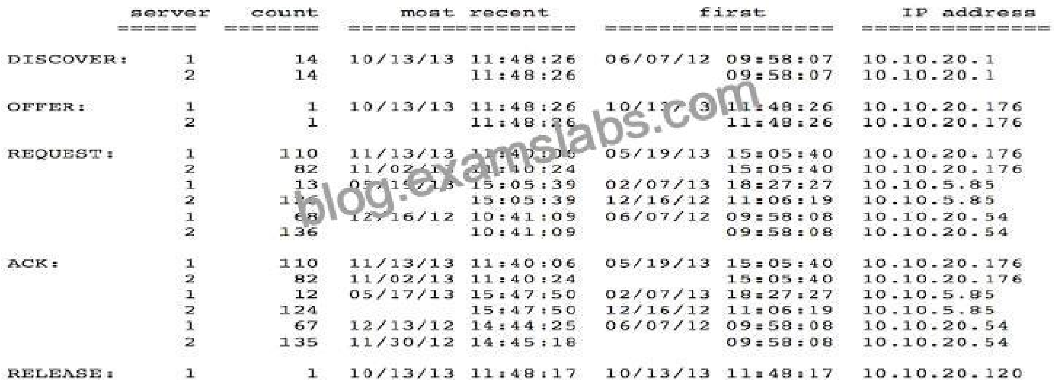
NEW QUESTION 54

John is implementing a commercial backup solution for his organization. Which of the following steps should be on the configuration checklist?

* Enable encryption if it &#8216;s not enabled by default
* Disable software-level encryption to increase speed of transfer
* Develop a unique encryption scheme

NEW QUESTION 55

DHCP logging output in the screenshot would be used for which of the following?



```
             server    count        most recent             first               IP address
             ======   =======   =================   =================   =============

DISCOVER:       1         14    10/13/13 11:48:26   06/07/12 09:58:07   10.10.20.1
                2         14             11:48:26            09:58:07   10.10.20.1

OFFER:          1          1    10/13/13 11:48:26   10/13/13 11:48:26   10.10.20.176
                2          1             11:48:26            11:48:26   10.10.20.176

REQUEST:        1        110    11/13/13 11:40:06   05/19/13 15:05:40   10.10.20.176
                2         82    11/02/13 11:40:24            15:05:40   10.10.20.176
                1         13    05/17/13 15:05:39   02/07/13 18:27:27   10.10.5.85
                2        125             15:05:39   12/16/12 11:06:19   10.10.5.85
                1         68    12/16/12 10:41:09   06/07/12 09:58:08   10.10.20.54
                2        136             10:41:09            09:58:08   10.10.20.54

ACK:            1        110    11/13/13 11:40:06   05/19/13 15:05:40   10.10.20.176
                2         82    11/02/13 11:40:24            15:05:40   10.10.20.176
                1         12    05/17/13 15:47:50   02/07/13 18:27:27   10.10.5.85
                2        124             15:47:50   12/16/12 11:06:19   10.10.5.85
                1         67    12/13/12 14:44:25   06/07/12 09:58:08   10.10.20.54
                2        135    11/30/12 14:45:18            09:58:08   10.10.20.54

RELEASE:        1          1    10/13/13 11:48:17   10/13/13 11:48:17   10.10.20.120
```

blog.examslabs.com

* Enforcing port-based network access control to prevent unauthorized devices on the network.
* Identifying new connections to maintain an up-to-date inventory of devices on the network.
* Detecting malicious activity by compromised or unauthorized devices on the network.
* Providing ping sweep results to identify live network hosts for vulnerability scanning.

NEW QUESTION 56

What could a security team use the command line tool Nmap for when implementing the Inventory and Control of Hardware Assets Control?
* Control which devices can connect to the network
* Passively identify new devices
* Inventory offline databases
* Actively identify new servers

NEW QUESTION 57

What tool creates visual network topology output and results that can be analyzed by Ndiff to determine if a service or network asset has changed?
* Ngrep
* CIS-CAT
* Netscreen
* Zenmap

NEW QUESTION 58

According to attack lifecycle models, what is the attacker&#8217;s first step in compromising an organization?
* Privilege Escalation
* Exploitation
* Initial Compromise

* Reconnaissance

NEW QUESTION 59

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?
* Users are required to change their password at the next login after three months
* Accounts must have passwords of at least 8 characters, with one number or symbol
* Accounts without login activity for 15 days are automatically locked

NEW QUESTION 60

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?
* Uninstall the application providing the service
* Turn the service off in the host configuration files
* Block the protocol for the unneeded service at the firewall
* Create an access list on the router to filter traffic to the host

NEW QUESTION 61

An organization wants to test its procedure for data recovery. Which of the following will be most effective?
* Verifying a file can be recovered from backup media
* Verifying that backup process is running when it should
* Verifying that network backups can&#8217;t be read in transit
* Verifying there are no errors in the backup server logs

Best GCCC Exam Preparation Material with New Dumps Questions
https://www.examslabs.com/GIAC/Cyber-Security/best-GCCC-exam-dumps.html]