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.certbus.com/gccc.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What is the first step suggested before implementing any single CIS Control?

A. Develop an effectiveness test

B. Perform a gap analysis

C. Perform a vulnerability scan

D. Develop a roll-out schedule

Correct Answer: B

QUESTION 2

How does an organization\\'s hardware inventory support the control for secure configurations?

A. It provides a list of managed devices that should be secured

B. It provides a list of unauthorized devices on the network

C. It provides the MAC addresses for insecure network adapters

D. It identifies the life cycle of manufacturer support for hardware devices

Correct Answer: A

QUESTION 3

What type of Unified Modelling Language (UML) diagram is used to show dependencies between logical groupings in a system?

A. Package diagram

B. Deployment diagram

C. Class diagram

D. Use case diagram

Correct Answer: A

QUESTION 4

Implementing which of the following will decrease spoofed e-mail messages?

A. Finger Protocol

B. Sender Policy Framework

C. Network Address Translation

D. Internet Message Access Protocol

Correct Answer: B

QUESTION 5

Which of the following assigns a number indicating the severity of a discovered software vulnerability?

A. CPE

B. CVE

C. CCE

D. CVSS

Correct Answer: D

QUESTION 6

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 7

Which of the following best describes the CIS Controls?

A. Technical, administrative, and policy controls based on research provided by the SANS Institute

B. Technical controls designed to provide protection from the most damaging attacks based on current threat data

C. Technical controls designed to augment the NIST 800 series

D. Technical, administrative, and policy controls based on current regulations and security best practices

Correct Answer: B

QUESTION 8

Which of the following should be measured and analyzed regularly when implementing the Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers CIS Control?

A. How long does it take to identify new unauthorized listening ports on the network systems

B. How long does it take to remove unauthorized software from the organization\\'s systems

C. What percentage of the organization\\'s applications are using sandboxing products

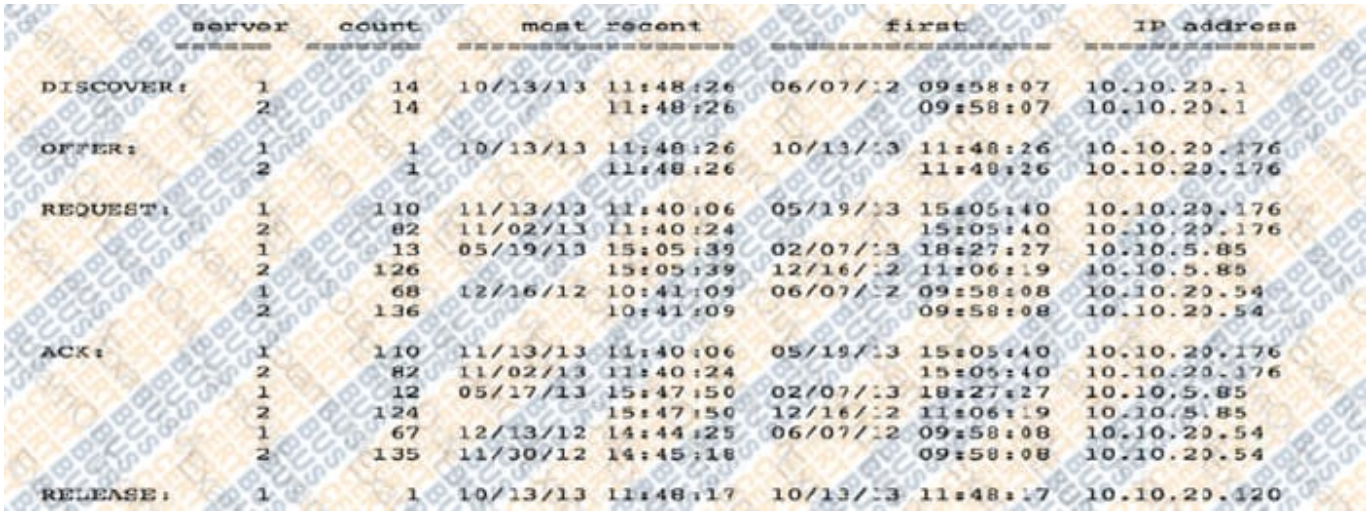
D. What percentage of assets will have their settings enforced and redeployed

E. What percentage of systems in the organization are using Network Level Authentication (NLA)

Correct Answer: D

QUESTION 9

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	05/19/13 15:05:39	02/07/13 18:27:27	10.10.5.85
	2	126	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

A. Enforcing port-based network access control to prevent unauthorized devices on the network.

B. Identifying new connections to maintain an up-to-date inventory of devices on the network.

C. Detecting malicious activity by compromised or unauthorized devices on the network.

D. Providing ping sweep results to identify live network hosts for vulnerability scanning.

Correct Answer: B

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

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?

A. Inventory of Authorized and Unauthorized Software

B. Continuous Vulnerability Management

C. Secure Configurations for Network Devices such as Firewalls, Routers and Switches

D. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Correct Answer: D

QUESTION 12

Acme Corporation performed an investigation of its centralized logging capabilities. It found that the central server is missing several types of logs from three servers in Acme\\'s inventory. Given these findings, what is the most appropriate next step?

A. Define processes to manually review logs for the problem servers

B. Restart or reinstall the logging service on each of the problem servers

C. Perform analysis to identify the source of the logging problems

D. Document the missing logs in the core evaluation report as a minor issue

Correct Answer: C

QUESTION 13

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 14

Which of the following is used to prevent spoofing of e-mail addresses?

A. Sender Policy Framework

B. DNS Security Extensions

C. Public-Key Cryptography

D. Simple Mail Transfer Protocol

Correct Answer: A

QUESTION 15

Which of the following baselines is considered necessary to implement the Boundary Defense CIS Control?

A. Multi-Factor Authentication Standard

B. Network Traffic/Service Baseline

C. Network Device Configuration Baselines

D. Network Information Flow

Correct Answer: D