DUMPSARENA

GIAC Critical Controls Certification (GCCC)

GIAC GCCC

Version Demo

Total Demo Questions: 10

Total Premium Questions: 93

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

A. Mandatory Access Control (MAC)

B. Data normalization

C. Data classification

D. Discretionary Access Control (DAC)

ANSWER: C

QUESTION NO: 2

Which of the options below will do the most to reduce an organization's attack surface on the internet?

A. Deploy an access control list on the perimeter router and limit inbound ICMP messages to echo requests only

B. Deploy antivirus software on internet-facing hosts, and ensure that the signatures are updated regularly

C. Ensure that rotation of duties is used with employees in order to compartmentalize the most important tasks

D. Ensure only necessary services are running on Internet-facing hosts, and that they are hardened according to best practices

ANSWER: D

QUESTION NO: 3

A need has been identified to organize and control access to different classifications of

information stored on a fileserver. Which of the following approaches will meet this need?

A. Organize files according to the user that created them and allow the user to determine permissions

B. Divide the documents into confidential, internal, and public folders, and ser permissions on each folder

C. Set user roles by job or position, and create permission by role for each file

D. Divide the documents by department and set permissions on each departmental folder

ANSWER: B

QUESTION NO: 4

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

A. CPE

B. CVE

C. CCE

D. CVSS

ANSWER: D

QUESTION NO: 5

An organization has implemented a policy to continually detect and remove malware from its network. Which of the following is a detective control needed for this?

A. Host-based firewall sends alerts when packets are sent to a closed port

B. Network Intrusion Prevention sends alerts when RST packets are received

C. Network Intrusion Detection devices sends alerts when signatures are updated

D. Host-based anti-virus sends alerts to a central security console

ANSWER: D

QUESTION NO: 6

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

ANSWER: A

QUESTION NO: 7

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

ANSWER: C

QUESTION NO: 8

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

ANSWER: A

QUESTION NO: 9

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

ANSWER: A

QUESTION NO: 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

ANSWER: D