Free Questions for GCCC by vceexamstest

Shared by Morin on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- Enabling best practices for the protection of their software licenses

B- Providing their employees, a secure method of connecting to the corporate network

C- Controlling unauthorized access to sensitive information

D- Applying the principle of defense in depth to their mobile devices

Answer:

C

Question 2

Question Type: MultipleChoice

A breach was discovered after several customers reported fraudulent charges on their accounts. The attacker had exported customer logins and cracked passwords that were hashed but not salted. Customers were made to reset their passwords.

Shortly after the systems were cleaned and restored to service, it was discovered that a compromised system administrator's account was being used to give the attacker continued access to the network. Which CIS Control failed in the continued access to the network?

Options:

A- Maintenance, Monitoring, and Analysis of Audit Logs

B- Controlled Use of Administrative Privilege

C- Incident Response and Management

D- Account Monitoring and Control

Answer:

C

Question 3

Question Type: MultipleChoice

What is a zero-day attack?

Options:

A- An attack that has a known attack signature but no available patch

B- An attack that utilizes a vulnerability unknown to the software developer

C- An attack that deploys at the end of a countdown sequence

D- An attack that is launched the day the patch is released

Answer:

B

Question 4

Question Type: **MultipleChoice**

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

Options:

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

Answer:

A

Question 5

Question Type: MultipleChoice

Which type of scan is best able to determine if user workstations are missing any important patches?

Options:

A- A network vulnerability scan using aggressive scanning

B- A source code scan

C- A port scan using banner grabbing

D- A web application/database scan

E- A vulnerability scan using valid credentials

Answer:

E

Question 6

Question Type: **MultipleChoice**

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

NAGIOS GUEST

What is the most likely source of this event?

Options:

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

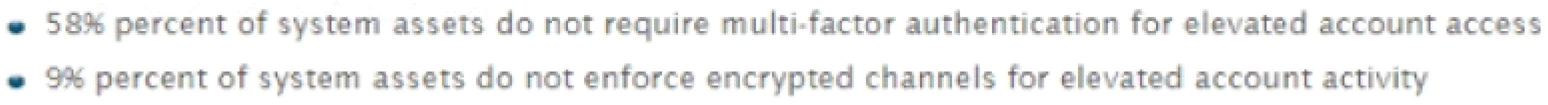
Answer:

C

Question 7

Question Type: MultipleChoice

Given the audit finding below, which CIS Control was being measured?



- 58% percent of system assets do not require multi-factor authentication for elevated account access
- 9% percent of system assets do not enforce encrypted channels for elevated account activity

Options:

A- Controlled Access Based on the Need to Know

B- Controlled Use of Administrative Privilege

C- Limitation and Control of Network Ports, Protocols and Services

D- Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

E- Inventory and Control of Hardware Assets

Answer:

B

Question 8

Question Type: **MultipleChoice**

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

Options:

A- The organization's proprietary data needs to be encrypted

B- Employees need to be notified that proprietary data should be protected

C- The organization's proprietary data needs to be identified

D- Appropriate file content matching needs to be configured

Answer:

C

Question 9

Question Type: **MultipleChoice**

Which of the following best describes the CIS Controls?

Options:

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

Answer:

B

Question 10

Question Type: **MultipleChoice**

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

Options:

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