Free Questions for CAS-004 by vceexamstest

Shared by Oneil on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization performed a risk assessment and discovered that less than 50% of its employees have been completing security awareness training. Which of the following should the Chief Information Security Officer highlight as an area of Increased vulnerability in a report to the management team?

Options:

A- Social engineering

B- Third-party compromise

C- APT targeting

D- Pivoting

Answer:

A

Explanation:

The Chief Information Security Officer (CISO) should highlight social engineering as an area of increased vulnerability due to the lack of completion of security awareness training by employees. Social engineering attacks exploit human behavior, and employees who are not adequately trained are more likely to fall victim to phishing, pretexting, and other types of social engineering tactics. Increasing awareness and training helps employees recognize and respond appropriately to these threats.

CompTIA CASP+ CAS-004 Exam Objectives: Section 4.3: Understand how to conduct risk management activities.

CompTIA CASP+ Study Guide, Chapter 9: Risk Management and Incident Response.

Question 2

Question Type: **MultipleChoice**

An IDS was unable to detect malicious network traffic during a recent security incident, even though all traffic was being sent using HTTPS. As a result, a website used by employees was compromised. Which of the following detection mechanisms would allow the IDS to detect an attack like this one in the future?

Options:

A- Deobfuscation

B- Protocol decoding

C- Inspection proxy

D- Digital rights management

Answer:

C

Explanation:

An inspection proxy, also known as an SSL/TLS inspection proxy, can decrypt HTTPS traffic, allowing the IDS to analyze the content for malicious activity. This method ensures that encrypted traffic can be inspected without compromising the security of the data in transit. The inspection proxy will re-encrypt the data before sending it on to its destination, maintaining the confidentiality of the communication while enabling security tools to perform their functions.

CompTIA CASP+ CAS-004 Exam Objectives: Section 3.3: Integrate network and security components and implement security controls.

CompTIA CASP+ Study Guide, Chapter 7: Analyzing Security Incidents.

Question 3

Question Type: MultipleChoice

The security analyst discovers a new device on the company's dedicated loT subnet during the most recent vulnerability scan. The scan results show numerous open ports and insecure protocols in addition to default usernames and passwords. A camera needs to transmit video to the security server in the loT subnet. Which of the following should the security analyst recommend to securely operate the camera?

Options:

A- Harden the camera configuration.

B- Send camera logs to the SIEM.

C- Encrypt the camera's video stream.

D- Place the camera on an isolated segment

Answer:

A

Explanation:

To securely operate the camera, the security analyst should recommend hardening the camera configuration. This involves several steps:

Changing Default Credentials: Default usernames and passwords are a common vulnerability. They should be replaced with strong, unique passwords.

Disabling Unnecessary Services and Ports: The numerous open ports and insecure protocols should be reviewed, and any unnecessary services should be disabled to reduce the attack surface.

Firmware Updates: Ensuring the camera's firmware is up to date will mitigate known vulnerabilities.

Enable Encryption: If possible, enable encryption for both data in transit and at rest to protect the video stream and other communications from interception.

This approach addresses the identified vulnerabilities directly and ensures that the device is more secure. Simply sending logs to the SIEM or isolating the camera might not fully mitigate the risks associated with default settings and open ports.

CompTIA CASP+ CAS-004 Exam Objectives: Section 2.4: Implement security activities across the technology life cycle.

CompTIA CASP+ Study Guide, Chapter 5: Implementing Host Security.

Question 4

Question Type: **MultipleChoice**

Which of the following should an organization implement to prevent unauthorized API key sharing?

Options:

A- OTP

B- Encryption

C- API gateway

D- HSM

Answer:

C

Explanation:

An API gateway is a management tool that sits between a client and a collection of backend services. It acts as a reverse proxy to accept all application programming interface (API) calls, aggregate the various services required to fulfill them, and return the appropriate result. API gateways can enforce policies such as rate limiting and authentication to prevent unauthorized access, making it an effective solution to prevent unauthorized API key sharing. By managing APIs at the gateway level, organizations can ensure that API keys are used as intended and are not shared or misused, addressing the need for secure management of API keys.

Question 5

Question Type: MultipleChoice

A technician accidentally deleted the secret key that was corresponding to the public key pinned to a busy online magazine. To remedy the situation, the technician obtained a new certificate with a different key. However, paying subscribers were locked out of the website until the key-pinning policy expired. Which of the following alternatives should the technician adopt to prevent a similar issue in the future?

Options:

A- Registration authority

B- Certificate revocation list

C- Client authentication

D- Certificate authority authorization

Answer:

D

Explanation:

Certificate Authority Authorization (CAA) is not listed directly in the provided options, but it is a relevant mechanism in the context of managing certificates and preventing issues similar to the one described. However, based on the available choices, the Online Certificate Status Protocol (OCSP) comes closest to providing a viable solution. OCSP allows for real-time validation of a certificate's revocation status, which could mitigate the issue of users being locked out due to key pinning policies. It is a more modern and efficient

alternative to Certificate Revocation Lists (CRLs), offering faster and more reliable certificate status checks. By implementing OCSP, the technician could ensure that clients receive timely updates on the revocation status of certificates, potentially avoiding the downtime caused by the key-pinning policy awaiting expiration.

Question 6

Question Type: MultipleChoice

A security engineer needs to implement a cost-effective authentication scheme for a new web-based application that requires:

* Rapid authentication

* Flexible authorization

* Ease of deployment

* Low cost but high functionality

Which of the following approaches best meets these objectives?

Options:

A- Kerberos

B- EAP

C- SAML

D- OAuth

E- TACACS+

Answer:

D

Explanation:

OAuth, which stands for Open Authorization, is a standard for authorization that enables secure token-based access. It allows users to grant a web application access to their information on another web application without giving them the credentials for their account. OAuth is particularly useful for rapid authentication, flexible authorization, ease of deployment, and offers high functionality at a low cost, making it an ideal choice for new web-based applications. This approach is well-suited for situations where web applications need to interact with each other on behalf of the user, without sharing user's password, such as integrating a geolocation application with Facebook. OAuth uses tokens issued by an authorization server, providing restricted access to a user's data, which aligns with the objectives of rapid authentication, flexible authorization, ease of deployment, and cost-effectiveness.

Question 7

Question Type: MultipleChoice

An employee's device was missing for 96 hours before being reported. The employee called the help desk to ask for another device Which of the following phases of the incident response cycle needs improvement?

Options:

A- Containment

B- Preparation

C- Resolution

D- Investigation

Answer:

B

Explanation:

The incident response cycle's preparation phase includes establishing policies and procedures for reporting lost or stolen devices promptly. If an employee's device was missing for 96 hours before being reported, this indicates a lack of awareness or clear procedures on the employee's part, pointing to inadequacies in the preparation phase of the incident response.

Question 8

Question Type: MultipleChoice

When implementing serverless computing an organization must still account for:

Options:

A- the underlying computing network infrastructure

B- hardware compatibility

C- the security of its data

D- patching the service

Answer:

C

Explanation:

While serverless computing abstracts the infrastructure layer from developers, organizations must still ensure the security of their data in the serverless environment. This includes protecting the data from unauthorized access and ensuring data privacy and integrity. Serverless architectures can be complex, and understanding the security model and shared responsibility is essential for safeguarding

applications and services.

Question 9

Question Type: MultipleChoice

An organization is designing a MAC scheme (or critical servers running GNU/Linux. The security engineer is investigating SELinux but is confused about how to read labeling contexts. The engineer executes the command stat ./secretfile and receives the following output:

```
...
Context: sys:secret:sec_t:s0
...
```

Which of the following describes the correct order of labels shown in the output above?

Options:

A- Role, type MLS level, and user identity

B- Role, user identity, object, and MLS level

C- Object MLS level, role, and type

D- User identity, role, type, and MLS level

E- Object, user identity, role, and MLS level

Answer:

D

Explanation:

SELinux contexts are typically made up of several components, including the user identity, role, type (also known as domain or type), and MLS (Multi-Level Security) level. The context format is user:role:type:level. In the given output sys:secret:sec_t:s0, 'sys' represents the user identity, 'secret' is the role, 'sec_t' is the type, and 's0' is the MLS level. Understanding SELinux contexts is critical for managing Mandatory Access Control (MAC) in GNU/Linux systems to protect against unauthorized access.

Question 10

Question Type: **MultipleChoice**

The Chief Executive Officer of an online retailer notices a sudden drop in sales A security analyst at the retailer detects a redirection of unsecure web traffic to a competitor's site Which of the following would best prevent this type of attack?

Options:

A- Enabling HSTS

B- Configuring certificate pinning

C- Enforcing DNSSEC

D- Deploying certificate stapling

Answer:

A

Explanation:

HTTP Strict Transport Security (HSTS) is a web security policy mechanism that helps to protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol. Enabling HSTS would prevent attackers from redirecting users from a secure site to an unsecure or malicious one.

Question 11

Question Type: MultipleChoice

A company has retained the services of a consultant to perform a security assessment. As part of the assessment the consultant recommends engaging with others in the industry to collaborate in regards to emerging attacks Which of the following would best enable this activity?

Options:

A- ISAC

B- OSINT

C- CVSS

D- Threat modeling

Answer:

A

Explanation:

Information Sharing and Analysis Centers (ISACs) are member-driven organizations, facilitated by the government, that gather and share information on cybersecurity threats, vulnerabilities, and incidents among their members. Engaging with an ISAC would enable the company to collaborate with others in the industry regarding emerging attacks and security threats.

Question 12

Question Type: MultipleChoice

An organization has an operational requirement with a specific equipment vendor The organization is located in the United States, but the vendor is located in another region Which of the following risks would be most concerning to the organization in the event of equipment failure?

Options:

A- Support may not be available during all business hours

B- The organization requires authorized vendor specialists.

C- Each region has different regulatory frameworks to follow

D- Shipping delays could cost the organization money

Answer:

A

Explanation:

The primary risk for an organization working with vendors in different time zones is that support might not be available during the organization's regular business hours. This can lead to delays in receiving necessary support or assistance when equipment issues arise, which could be critical if there's an equipment failure.