CAS-003Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

A consultant is hired to perform a passive vulnerability assessment of a company to determine what information might be collected about the company and its employees. The assessment will be considered successful if the consultant can discover the name of one of the IT administrators. Which of the following is MOST likely to produce the needed information?

A. Whois

B. DNS enumeration

C. Vulnerability scanner

D. Fingerprinting

Correct Answer: A

QUESTION 2

A company\\'s Chief Information Security Officer (CISO) is working with the product owners to perform a business impact assessment. The product owners provide feedback related to the critically of various business processes, personal, and technologies. Transitioning into risk assessment activities, which of the following types of information should the CISO require to determine the proper risk ranking? (Select TWO).

A. Trend analysis

B. Likelihood

C. TCO

D. Compensating controls

E. Magnitude

F. ROI

Correct Answer: AC

QUESTION 3

A government entity is developing requirements for an RFP to acquire a biometric authentication system When developing these requirements, which of the following considerations is MOST critical to the verification and validation of the SRTM?

A. Local and national laws and regulations

B. Secure software development requirements

C. Environmental constraint requirements

D. Testability of requirements

Correct Answer: A

QUESTION 4

A company is outsourcing to an MSSP that performs managed detection and response services. The MSSP requires a server to be placed inside the network as a log aggregator and allows remote access to MSSP analysts. Critical devices send logs to the log aggregator, where data is stored for 12 months locally before being archived to a multitenant cloud The data is then sent from the log aggregator to a public IP address in the MSSP\\'s datacenter for analysis. A security engineer is concerned about the secunty of the solution and notes the following

1.

The critical devices send cleartext logs to the aggregator.

2.

The log aggregator utilizes full disk encryption.

3.

The log aggregator sends to the analysis server via port 80.

4.

MSSP analysts utilize an SSL VPN with MFA to access the log aggregator remotely.

5.

The data is compressed and encrypted prior to being archived in the cloud.

Which of the following should be the secunty engineer\\'s GREATEST concern?

A. Hardware vulnerabilities introduced by the log aggregator server.

B. Network bridging from a remote access VPN.

C. Encryption of data in transit.

D. Multitenancy and data remnants in the cloud.

Correct Answer: C

QUESTION 5

Management is reviewing the results of a recent risk assessment of the organization\\'s policies and procedures. During the risk assessment it is determined that procedures associated with background checks have not been effectively implemented. In response to this risk, the organization elects to revise policies and procedures related to background checks and use a third-party to perform background checks on all new employees.

Which of the following risk management strategies has the organization employed?

A. Transfer

B. Mitigate

C. Accept

D. Avoid

E. Reject

Correct Answer: B

QUESTION 6

A security engineer is a new member to a configuration board at the request of management. The company has two new major IT projects starting this year and wants to plan security into the application deployment. The board is primarily concerned with the applications\\' compliance with federal assessment and authorization standards. The security engineer asks for a timeline to determine when a security assessment of both applications should occur and does not attend subsequent configuration board meetings. If the security engineer is only going to perform a security assessment, which of the following steps in system authorization has the security engineer omitted?

A. Establish the security control baseline

B. Build the application according to software development security standards

C. Review the results of user acceptance testing

D. Consult with the stakeholders to determine which standards can be omitted

Correct Answer: A

A security baseline is the minimum level of security that a system, network, or device must adhere to. It is the initial point of reference for security and the document against which assessments would be done.

QUESTION 7

A security auditor needs to review the manner in which an entertainment streaming device operates The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output:

```
# nmap -F -T4 192.168.8.11
Starting Nmap 7.60
Nmap scan report for 192.168.8.11
Host is up (0.702s latency).
Not shown: 99 filtered ports
PORT          STATE     SERVICE
80/tcp        open      http
MAC Address:  04:18:18:EB:10:13   (CompTIA)
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

The best option for the auditor to use NEXT is:

A. a SCAP assessment

B. reverse engineering

C. fuzzing

D. network interception

Correct Answer: B

QUESTION 8

A software development company lost customers recently because of a large number of software issues. These issues were related to integrity and availability defects, including buffer overflows, pointer deferences, and others. Which of the following should the company implement to improve code quality? (Select two).

A. Development environment access controls

B. Continuous integration

C. Code comments and documentation

D. Static analysis tools

E. Application containerization

F. Code obfuscation

Correct Answer: AE

QUESTION 9

A Chief Information Security Officer (CISO) implemented MFA for all accounts in parallel with the BYOD policy. After the implementation, employees report the increased authentication method is causing increased time to tasks. This applies both to accessing the email client on the workstation and the online collaboration portal. Which of the following should be the CISO implement to address the employees\\' concerns?

A. Create an exception for the company\\'s IPs.

B. Implement always-on VPN.

C. Configure the use of employee PKI authentication for email.

D. Allow the use of SSO.

Correct Answer: D

QUESTION 10

A new security policy states all wireless and wired authentication must include the use of certificates when connecting to internal resources within the enterprise LAN by all employees.

Which of the following should be configured to comply with the new security policy? (Choose two.)

A. SSO

B. New pre-shared key

C. 802.1X

D. OAuth

E. Push-based authentication

F. PKI

Correct Answer: CF

QUESTION 11

A security administrator wants to implement controls to harden company-owned mobile devices. Company policy specifies the following requirements:

1.

Mandatory access control must be enforced by the OS.

2.

Devices must only use the mobile carrier data transport.

Which of the following controls should the security administrator implement? (Select three).

A. Enable DLP

B. Enable SEAndroid

C. Enable EDR

D. Enable secure boot

E. Enable remote wipe

F. Disable Bluetooth

G. Disable 802.11

H. Disable geotagging

Correct Answer: BFG

QUESTION 12

A medical facility wants to purchase mobile devices for doctors and nurses. To ensure accountability, each individual will be assigned a separate mobile device. Additionally, to protect patients\\' health information, management has identified

the following requirements:

Data must be encrypted at rest.

The device must be disabled if it leaves the facility.

The device must be disabled when tampered with.

Which of the following technologies would BEST support these requirements? (Select two.)

A. eFuse

B. NFC

C. GPS

D. Biometric

E. USB 4.1

F. MicroSD

Correct Answer: CD

QUESTION 13

A security incident responder discovers an attacker has gained access to a network and has overwritten key system files with backdoor software. The server was reimaged and patched offline.

Which of the following tools should be implemented to detect similar attacks?

A. Vulnerability scanner

B. TPM

C. Host-based firewall

D. File integrity monitor

E. NIPS

Correct Answer: D

QUESTION 14

An organization is deploying IoT locks, sensors, and cameras, which operate over 802.11, to replace legacy building access control systems. These devices are capable of triggering physical access changes, including locking and unlocking doors and gates. Unfortunately, the devices have known vulnerabilities for which the vendor has yet to provide firmware updates.

Which of the following would BEST mitigate this risk?

A. Direct wire the IoT devices into physical switches and place them on an exclusive VLAN.

B. Require sensors to sign all transmitted unlock control messages digitally.

C. Associate the devices with an isolated wireless network configured for WPA2 and EAP-TLS.

D. Implement an out-of-band monitoring solution to detect message injections and attempts.

Correct Answer: C

QUESTION 15

While traveling to another state, the Chief Financial (CFO) forgot to submit payroll for the company. The CFO quickly gained to the corporate through the high-speed wireless network provided by the hotel and completed the desk. Upon returning from the business trip, the CFO was told no one received their weekly pay due to a malware on attack on the system. Which of the following is the MOST likely of the security breach?

A. The security manager did not enforce automate VPN connection.

B. The company\\'s server did not have endpoint security enabled.

C. The hotel and did require a wireless password to authenticate.

D. The laptop did not have the host-based firewall properly configured.

Correct Answer: A