CAS-003$^{Q\&As}$

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

QUESTION 1

Following the merger of two large companies the newly combined security team is overwhelmed by the volume of logs flowing from the IT systems The company\\'s data retention schedule complicates the issue by requiring detailed logs to be collected and available for months Which of the following designs BEST meets the company\\'s security and retention requirement?

A. Forward logs to both a SIEM and a cheaper longer-term storage and then delete logs from the SIEM after 14 days

B. Reduce the log volume by disabling logging of routine maintenance activities or failed authentication attempts

C. Send logs to a SIEM that correlates security data and store only the alerts and relevant data arising from that system.

D. Maintain both companies\\' logging and SIEM solutions separately but merge the resulting alerts and reports.

Correct Answer: C

QUESTION 2

Due to a recent acquisition, the security team must find a way to secure several legacy applications. During a review of the applications, the following issues are documented:

1.

The applications are considered mission-critical.

2.

The applications are written in code languages not currently supported by the development staff.

3.

Security updates and patches will not be made available for the applications.

4.

Username and passwords do not meet corporate standards.

5.

The data contained within the applications includes both PII and PHI.

6.

The applications communicate using TLS 1.0.

7.

Only internal users access the applications.

Which of the following should be utilized to reduce the risk associated with these applications and their current architecture?

A. Update the company policies to reflect the current state of the applications so they are not out of compliance.

B. Create a group policy to enforce password complexity and username requirements.

C. Use network segmentation to isolate the applications and control access.

D. Move the applications to virtual servers that meet the password and account standards.

Correct Answer: D

QUESTION 3

A medical device company is implementing a new COTS antivirus solution in its manufacturing plant. All validated machines and instruments must be retested for interoperability with the new software. Which of the following would BEST ensure the software and instruments are working as designed?

A. System design documentation

B. User acceptance testing

C. Peer review

D. Static code analysis testing

E. Change control documentation

Correct Answer: A

QUESTION 4

An organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?

A. BGP route hijacking attacks

B. Bogon IP network traffic

C. IP spoofing attacks

D. Man-in-the-middle attacks

E. Amplified DDoS attacks

Correct Answer: C

The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall. This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range.

IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. Here\\'s how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.

When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker.

If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.

QUESTION 5

A forensic analyst receives a hard drive containing malware quarantined by the antivirus application. After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

A. The malware file\\'s modify, access, change time properties.

B. The timeline analysis of the file system.

C. The time stamp of the malware in the swap file.

D. The date/time stamp of the malware detection in the antivirus logs.

Correct Answer: B

Timelines can be used in digital forensics to identify when activity occurred on a computer. Timelines are mainly used for data reduction or identifying specific state changes that have occurred on a computer.

QUESTION 6

A company recently implemented a variety of security services to detect various types of traffic that pose a threat to the company. The following services were enabled within the network:

1.

Scan of specific subsets for vulnerabilities

2.

Categorizing and logging of website traffic

3.

Enabling specific ACLs based on application traffic

4.

Sending suspicious files to a third-party site for validation A report was sent to the security team that identified multiple incidents of users sharing large amounts of data from an on-premise server to a public site. A small percentage of that data also contained malware and spyware Which of the following services MOST likely identified the behavior and sent the report?

A. Content filter

B. User behavioral analytics

C. Application sandbox

D. Web application firewall

E. Endpoint protection

F. Cloud security broker

Correct Answer: B

QUESTION 7

A company enlists a trusted agent to implement a way to authenticate email senders positively Which of the following is the BEST method for the company to prove Vie authenticity of the message?

A. issue PIN-enabled hardware tokens

B. Create a CA win all users

C. Configure the server to encrypt all messages in transit

D. include a hash in the body of the message

Correct Answer: A

QUESTION 8

A government contracting company issues smartphones to employees to enable access to corporate resources. Several employees will need to travel to a foreign country for business purposes and will require access to their phones. However, the company recently received intelligence that its intellectual property is highly desired by the same country\\'s government. Which of the following MDM configurations would BEST reduce the risk of compromise while on foreign soil?

A. Disable firmware OTA updates.

B. Disable location services.

C. Disable push notification services.

D. Disable wipe

Correct Answer: B

QUESTION 9

A security engineer is designing a system in which offshore, outsourced staff can push code from the development environment to the production environment securely. The security engineer is concerned with data loss, while the business does not want to slow down its development process. Which of the following solutions BEST balances security requirements with business need?

A. Set up a VDI environment that prevents copying and pasting to the local workstations of outsourced staff members

B. Install a client-side VPN on the staff laptops and limit access to the development network

C. Create an IPSec VPN tunnel from the development network to the office of the outsourced staff

D. Use online collaboration tools to initiate workstation-sharing sessions with local staff who have access to the development network

Correct Answer: D

QUESTION 10

An organization enables BYOD but wants to allow users to access the corporate email, calendar, and contacts from their devices. The data associated with the user\\'s accounts is sensitive, and therefore, the organization wants to comply with the following requirements:

Active full-device encryption Enabled remote-device wipe Blocking unsigned applications Containerization of email, calendar, and contacts

Which of the following technical controls would BEST protect the data from attack or loss and meet the above requirements?

A. Require frequent password changes and disable NFC.

B. Enforce device encryption and activate MAM.

C. Install a mobile antivirus application.

D. Configure and monitor devices with an MDM.

Correct Answer: B

QUESTION 11

The IT Security Analyst for a small organization is working on a customer\\'s system and identifies a possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.

B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.

C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.

D. Refer the issue to management for handling according to the incident response process.

Correct Answer: D

The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer\\'s system. Therefore, this IT Security Analyst does not know what the customer\\'s incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.

QUESTION 12

A recent penetration test identified that a web server has a major vulnerability. The web server hosts a critical shipping application for the company and requires 99.99% availability. Attempts to fix the vulnerability would likely break the application. The shipping application is due to be replaced in the next three months. Which of the following would BEST secure the web server until the replacement web server is ready?

A. Patch management

B. Antivirus

C. Application firewall

D. Spam filters

E. HIDS

Correct Answer: E

QUESTION 13

A company is purchasing an application that will be used to manage all IT assets as well as provide an incident and problem management solution for IT activity The company narrows the search to two products. Application A and Application B; which meet all of its requirements. Application A is the most cost-effective product, but it is also the riskiest so the company purchases Application B. Which of the following types of strategies did the company use when determining risk appetite?

A. Mitigation

B. Acceptance

C. Avoidance

D. Transfer

Correct Answer: B

QUESTION 14

An engineer maintains a corporate-owned mobility infrastructure, and the organization requires that all web browsing using corporate-owned resources be monitored. Which of the following would allow the organization to meet its requirement? (Choose two.)

A. Exempt mobile devices from the requirement, as this will lead to privacy violations

B. Configure the devices to use an always-on IPSec VPN

C. Configure all management traffic to be tunneled into the enterprise via TLS

D. Implement a VDI solution and deploy supporting client apps to devices

E. Restrict application permissions to establish only HTTPS connections outside of the enterprise boundary

Correct Answer: BE

QUESTION 15

A security architect has been assigned to a new digital transformation program. The objectives are to provide better capabilities to customers and reduce costs. The program has highlighted the following requirements:

Long-lived sessions are required, as users do not log in very often.

The solution has multiple SPs, which include mobile and web applications.

A centralized IdP is utilized for all customer digital channels.

The applications provide different functionality types such as forums and customer portals.

The user experience needs to be the same across both mobile and web-based applications.

Which of the following would BEST improve security while meeting these requirements?

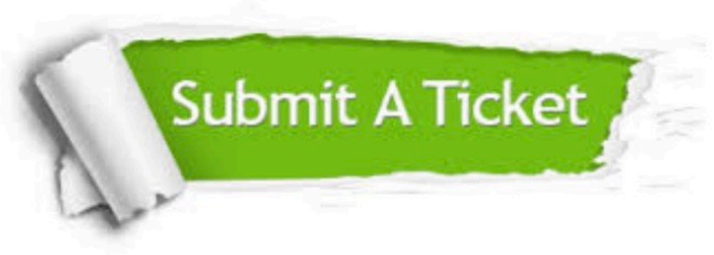
A. Social login to IdP, securely store the session cookies, and implement one-time passwords sent to the mobile device

B. Create-based authentication to IdP, securely store access tokens, and implement secure push notifications.

C. Username and password authentication to IdP, securely store refresh tokens, and implement context-aware authentication.

D. Username and password authentication to SP, securely store Java web tokens, and implement SMS OTPs.

Correct Answer: A


Submit A Ticket

100%