CAS-003 Q&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.pass4itsure.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A facilities manager requests approval to deploy a new key management system that integrates with logical network access controls to provide conditional access. The security analyst who is assessing the risk has no experience with the category of products.

Which of the following is the FIRST step the analyst should take to begin the research?

A. Seek documented industry best practices.

B. Review the preferred vendor\\'s white papers.

C. Compare the product function to relevant RFCs

D. Execute a non-disclosure agreement with the vendor

Correct Answer: A

QUESTION 2

A security analyst is attempting to break into a client\\'s secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. After network enumeration, the analyst\\'s NEXT step is to perform:

A. a gray-box penetration test

B. a risk analysis

C. a vulnerability assessment

D. an external security audit

E. a red team exercise

Correct Answer: A

QUESTION 3

An enterprise with global sites processes and exchanges highly sensitive information that is protected under several countries\\' arms trafficking laws. There is new information that malicious nation-state-sponsored activities are targeting the use of encryption between the geographically disparate sites. The organization currently employs ECDSA and ECDH with P-384, SHA-384, and AES-256-GCM on VPNs between sites.

Which of the following techniques would MOST likely improve the resilience of the enterprise to attack on cryptographic implementation?

A. Add a second-layer VPN from a different vendor between sites.

B. Upgrade the cipher suite to use an authenticated AES mode of operation.

C. Use a stronger elliptic curve cryptography algorithm.

D. Implement an IDS with sensors inside (clear-text) and outside (cipher-text) of each tunnel between sites.

E. Ensure cryptography modules are kept up to date from vendor supplying them.

Correct Answer: C

QUESTION 4

A software company is releasing a new mobile application to a broad set of external customers. Because the software company is rapidly releasing new features, it has built in an over-the-air software update process that can automatically update the application at launch time. Which of the following security controls should be recommended by the company\\'s security architect to protect the integrity of the update process? (Choose two.)

A. Validate cryptographic signatures applied to software updates

B. Perform certificate pinning of the associated code signing key

C. Require HTTPS connections for downloads of software updates

D. Ensure there are multiple download mirrors for availability

E. Enforce a click-through process with user opt-in for new features

Correct Answer: AB

QUESTION 5

An analyst has noticed unusual activities in the SIEM to a .cn domain name. Which of the following should the analyst use to identify the content of the traffic?

A. Log review

B. Service discovery

C. Packet capture

D. DNS harvesting

Correct Answer: D

QUESTION 6

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 7

When of the following is the BEST reason to implement a separation of duties policy?

A. It minimizes the risk of Dos due to continuous monitoring.

B. It eliminates the need to enforce least privilege by logging all actions.

C. It increases the level of difficulty for a single employee to perpetrate fraud.

D. it removes barriers to collusion and collaboration between business units.

Correct Answer: A

QUESTION 8

A security consultant was hired to audit a company\\'s password are account policy. The company implements the following controls:

1.

Minimum password length: 16

2.

Maximum password age: 0

3.

Minimum password age: 0

4.

Password complexity: disabled

5.

Store passwords in plain text: disabled

6.

Failed attempts lockout: 3

7.

Lockout timeout: 1 hour

The password database uses salted hashes and PBKDF2. Which of the following is MOST likely to yield the greatest number of plain text passwords in the shortest amount of time?

A. Offline hybrid dictionary attack

B. Offline brute-force attack

C. Online hybrid dictionary password spraying attack

D. Rainbow table attack

E. Online brute-force attack

F. Pass-the-hash attack

Correct Answer: C

QUESTION 9

A developer needs to provide feedback on a peer\\'s work during the SDLC. While reviewing the code changes, the developers session ID tokens for a web application will be transmitted over an unsecure connection. Which of the following code snippets should the developer recommend implement to correct the vulnerability?

A.
```
Cookie cookie = new Cookie("primary");
cookie.secure(true);
```

B.
```
String input = request.getParameter ("input");
String character Pattern = "[./a-zA-Z0-9?"="&]";
If (! input. matches (character Pattern))
{
out.println ("Invalid Input");
}
```

C.
```
<webapp>
<session-config>
<session-timeout>15</session-timeout>
</session-config>
</webapp>
```

D.
```
<input type="text" maxlength="30" name="ecaSessionPW" size="40" readonly="true"
value='<%=ESAPI.encoder().encodeForHTML(request.getParameter("SessionPW"))%>'/>
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 10

A regional transportation and logistics company recently hired its first Chief Information Security Officer (CISO). The CISO\\'s first project after onboarding involved performing a vulnerability assessment against the company\\'s public facing network. The completed scan found a legacy collaboration platform application with a critically rated vulnerability. While discussing this issue with the line of business, the CISO learns the vulnerable application cannot be updated without the company incurring significant losses due to downtime or new software purchases.

Which of the following BEST addresses these concerns?

A. The company should plan future maintenance windows such legacy application can be updated as needed.

B. The CISO must accept the risk of the legacy application, as the cost of replacing the application greatly exceeds the risk to the company.

C. The company should implement a WAF in front of the vulnerable application to filter out any traffic attempting to exploit the vulnerability.

D. The company should build a parallel system and perform a cutover from the old application to the new application, with less downtime than an upgrade.

Correct Answer: C

QUESTION 11

A security administrator is confirming specific ports and IP addresses that are monitored by the IPS- IDS system as well as the firewall placement on the perimeter network between the company and a new business partner Which of the following business documents defines the parameters the security administrator must confirm?

A. BIA

B. ISA

C. NDA

D. MOU

Correct Answer: A

QUESTION 12

A company requires a task to be carried by more than one person concurrently. This is an example of:

A. separation of d duties.

B. dual control

C. least privilege

D. job rotation

Correct Answer: A

QUESTION 13

During a recent incident, sensitive data was disclosed and subsequently destroyed through a properly secured, cloud-based storage platform. An incident response technician is working with management to develop an after action report that conveys critical metrics regarding the incident.

Which of the following would be MOST important to senior leadership to determine the impact of the breach?

A. The likely per-record cost of the breach to the organization

B. The legal or regulatory exposure that exists due to the breach

C. The amount of downtime required to restore the data

D. The number of records compromised

Correct Answer: A

QUESTION 14

An attacker attempts to create a DoS event against the VoIP system of a company. The attacker uses a tool to flood the network with a large number of SIP INVITE traffic. Which of the following would be LEAST likely to thwart such an attack?

A. Install IDS/IPS systems on the network

B. Force all SIP communication to be encrypted

C. Create separate VLANs for voice and data traffic

D. Implement QoS parameters on the switches

Correct Answer: D

Quality of service (QoS) is a mechanism that is designed to give priority to different applications, users, or data to provide a specific level of performance. It is often used in networks to prioritize certain types of network traffic. It is not designed to block traffic, per se, but to give certain types of traffic a lower or higher priority than others. This is least likely to counter a denial of service (DoS) attack.

QUESTION 15

A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.

Which of the following exercise types should the analyst perform?

A. Summarize the most recently disclosed vulnerabilities.

B. Research industry best practices and latest RFCs.

C. Undertake an external vulnerability scan and penetration test.

D. Conduct a threat modeling exercise.

Correct Answer: D

Latest CAS-003 Dumps CAS-003 VCE Dumps CAS-003 Study Guide