CAS-004 Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

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

https://www.leads4pass.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

When implementing serverless computing, an organization must still account for:

A. the underlying computing network infrastructure.

B. hardware compatibility.

C. the security of its data.

D. patching the service.

Correct Answer: C

QUESTION 2

A commercial OSINT provider utilizes and reviews data from various sources of publicly available information. The provider is transitioning the subscription service to a model that limit\\'s the scope of available data based on subscription tier. Which of the following approaches would best ensure subscribers are only granted access to data associated with their tier? (Choose two.)

A. Storing collected data on separate physical media per tier

B. Controlling access to data based on the role of users

C. Employing attribute-based access control

D. Implementing a behavior-based IDS positioned at the storage network gateway

E. Establishing a classification and labeling scheme

F. Implementing a mandatory access control scheme

Correct Answer: BE

QUESTION 3

A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack. Which of the following is the NEXT step of the incident response plan?

A. Remediation

B. Containment

C. Response

D. Recovery

Correct Answer: B

Reference: https://www.sciencedirect.com/topics/computer-science/containment-strategy

QUESTION 4

After a server was compromised an incident responder looks at log files to determine the attack vector that was used The incident responder reviews the web server log files from the time before an unexpected SSH session began:

Date	URL
April 18 04:16	https://myapp.mycompany.com/shopping-cart.php=?orderproducts
April 18 04:18	https://myapp.mycompany.com/something.php=?../../../../etc/shadow
April 18 04:21	https://myapp.mycompany.com/put_file=?admin:password
April 18 04:22	https://myapp.mycompany.com/something.php=?whoami
April 18 04:23	https://myapp.mycompany.com/shopping-cart.php=?processorder

Which of the following is the most likely vulnerability that was exploited based on the log files?

A. Directory traversal revealed the hashed SSH password, which was used to access the server.

B. A SQL injection was used during the ordering process to compromise the database server

C. The root password was easily guessed and used as a parameter lo open a reverse shell

D. An outdated third-party PHP plug-in was vulnerable to a known remote code execution

Correct Answer: A

The logs indicate a directory traversal attempt (/../..//.etc/shadow), which is a type of attack that exploits insufficient security validation/sanitization of user-supplied input file names, so that characters representing "traverse to parent directory" are passed through to the file APIs. The /etc/shadow file on Unix systems contains password hashes. If an attacker successfully exploited this vulnerability, they could potentially access the hashed SSH password. This information could then be used to gain unauthorized access to the server if the hash was cracked.

QUESTION 5

Company A acquired Company . During an audit, a security engineer found Company B\\'s environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B\\'s infrastructure could be integrated into Company A\\'s security program.

Which of the following risk-handling techniques was used?

A. Accept

B. Avoid

C. Transfer

D. Mitigate

Correct Answer: D

Reference: https://www.pivotpointsecurity.com/blog/risk-tolerance-in-business/

QUESTION 6

A company is in the process of refreshing its entire infrastructure The company has a business-critical process running on an old 2008 Windows server If this server fails, the company would lose millions of dollars in revenue. Which of the following actions should the company should take?

A. Accept the risk as the cost of doing business

B. Create an organizational risk register for project prioritization

C. Calculate the ALE and conduct a cost-benefit analysis

D. Purchase insurance to offset the cost if a failure occurred

Correct Answer: C

Calculating the Annual Loss Expectancy (ALE) and conducting a cost-benefit analysis is a critical part of risk management. The ALE will help the company understand the potential losses associated with the server failure per year, which can then be weighed against the cost of mitigating the risk (e.g., replacing the server or implementing redundancies). This analysis will inform the decision on the best course of action to manage the risk associated with the aging server.

QUESTION 7

A company\\'s internet connection is commonly saturated during business hours, affecting internet availability. The company requires all Internet traffic to be business related After analyzing the traffic over a period of a few hours, the security administrator observes the following:

Protocol	Usage	%
TCP/SSL	324Gb	85%
TCP/HTTP	37Gb	10%
UDP/DNS	10Gb	3%
Other	8Gb	2%

The majority of the IP addresses associated with the TCP/SSL traffic resolve to CDNs

Which of the following should the administrator recommend for the CDN traffic to meet the corporate security requirements?

A. Block outbound SSL traffic to prevent data exfiltration.

B. Confirm the use of the CDN by monitoring NetFlow data.

C. Further investigate the traffic using a sanctioned MITM proxy.

D. Implement an IPS to drop packets associated with the CDN.

Correct Answer: A

QUESTION 8

Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs.

Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

A. Implement rate limiting on the API.

B. Implement geoblocking on the WAF.

C. Implement OAuth 2.0 on the API.

D. Implement input validation on the API.

Correct Answer: A

QUESTION 9

The Chief information Officer (CIO) wants to implement enterprise mobility throughout the organization. The goal is to allow employees access to company resources. However the CIO wants the ability to enforce configuration settings, manage data, and manage both company-owned and personal devices. Which of the following should the CIO implement to achieve this goal?

A. BYOO

B. CYOD

C. COPE

D. MDM

Correct Answer: D

QUESTION 10

A company based in the United States holds insurance details of EU citizens. Which of the following must be adhered to when processing EU citizens\\' personal, private, and confidential data?

A. The principle of lawful, fair, and transparent processing

B. The right to be forgotten principle of personal data erasure requests

C. The non-repudiation and deniability principle

D. The principle of encryption, obfuscation, and data masking

Correct Answer: A

QUESTION 11

A security manager wants to implement a policy that will management with the ability to monitor employees\\' activities with minimum impact to productivity. Which of the following policies Is BEST suited for this scenario?

A. Separation of duties

B. Mandatory vacations

C. Least privilege

D. Incident response

Correct Answer: A

QUESTION 12

A penetration tester is trying to gain access to a building after hours as part of a physical assessment of an office complex. The tester notes that each employee touches a badge near a small black box outside the side door, and the door unlocks. The tester uses a software-defined radio tool to determine a 125kHz signal is used during this process. Which of the following technical solutions would be BEST to help the penetration tester gain access to the building?

A. Generate a 125kHz tone.

B. Compromise the ICS/SCADA system.

C. Utilize an RFID duplicator.

D. Obtain a lock pick set.

Correct Answer: A

QUESTION 13

A security engineer is reviewing a record of events after a recent data breach incident that Involved the following:

1.

A hacker conducted reconnaissance and developed a footprint of the company s Internet- facing web application assets.

2.

A vulnerability in a third-party horary was exploited by the hacker, resulting in the compromise of a local account.

3.

The hacker took advantage of the account\\'s excessive privileges to access a data store and exfilltrate the data without detection.

Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

A. Dynamic analysis

B. Secure web gateway

C. Software composition analysis

D. User behavior analysis

E. Web application firewall

Correct Answer: C

QUESTION 14

An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of impact.

Which of the following should the organization perform NEXT?

A. Assess the residual risk.

B. Update the organization\\'s threat model.

C. Move to the next risk in the register.

D. Recalculate the magnitude of impact.

Correct Answer: A

QUESTION 15

An organization collects personal data from its global customers. The organization determines how that data is going to be used, why it is going to be used, and how it is manipulated for business processes. Which of the following will the organization need in order to comply with GDPR? (Choose two.)

A. Data processor

B. Data custodian

C. Data owner

D. Data steward

E. Data controller

F. Data manager

Correct Answer: AE