# 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**

A company has instituted a new policy in which all outbound traffic must go over TCP ports 80 and 443 for all its managed mobile devices. No other IP traffic is allowed to be initiated from a device. Which of the following should the organization consider implementing to ensure internet access continues without interruption?

A. CYOD

B. MDM

C. WPA3

D. DoH

Correct Answer: B

**QUESTION 2**

Which of the following BEST sets expectation between the security team and business units within an organization?

A. Risk assessment

B. Memorandum of understanding

C. Business impact analysis

D. Business partnership agreement

E. Services level agreement

Correct Answer: C

**QUESTION 3**

A company\\'s SOC has received threat intelligence about an active campaign utilizing a specific vulnerability. The company would like to determine whether it is vulnerable to this active campaign. Which of the following should the company use to make this determination?

A. Threat hunting

B. A system penetration test

C. Log analysis within the SIEM tool

D. The Cyber Kill Chain

Correct Answer: B

**QUESTION 4**

A help desk technician is troubleshooting an issue with an employee\\'s laptop that will not boot into its operating system. The employee reported the laptop had been stolen but then found it one day later. The employee has asked the technician for help recovering important data. The technician has identified the following:

1.

The laptop operating system was not configured with BitLocker.

2.

The hard drive has no hardware failures.

3.

Data is present and readable on the hard drive, although it appears to be illegible.

Which if the following is the MOST likely reason the technician is unable to retrieve legible data from the hard drive?

A. The employee\\'s password was changed, and the new password needs to be used.

B. The PKI certificate was revoked, and a new one must be installed.

C. The hard drive experienced crypto-shredding.

D. The technician is using the incorrect cipher to read the data.

Correct Answer: C

Crypto-shredding describes the concept that destroying a decryption key in essence destroys the data it was designed to protect. Especially important in cloud environments where methods available to confidently destroy data is limited. This technique depends upon assurance that the data was never available in decrypted format at any point in its life cycle, that the encryption method was sufficiently secure, and that the key is irrecoverably destroyed.

**QUESTION 5**

A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:

1.

Must have a minimum of 15 characters

2.

Must use one number

3.

Must use one capital letter

4.

Must not be one of the last 12 passwords used

Which of the following policies should be added to provide additional security?

A. Shared accounts

B. Password complexity

C. Account lockout

D. Password history

E. Time-based logins

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold

**QUESTION 6**

A forensic investigator would use the foremost command for:

A. cloning disks.

B. analyzing network-captured packets.

C. recovering lost files.

D. extracting features such as email addresses.

Correct Answer: C

Reference: https://www.networkworld.com/article/2333727/foremost--a-linux-computer-forensics-tool.html

**QUESTION 7**

A systems engineer is reviewing output from a web application vulnerability scan. The engineer has determined data is entenng the application from an untrusted source and is being used to construct a query dynamically. Which of the following code snippets would BEST protect the application against an SQL injection attack?

A. String input = request.getParameter ("SeqNo"); String characterPattern = "[0-9a0zA-Z] If (! input. Matches (characterPattern)) { out.println ("Invalid Input"); }

B. Cinput type= "text" maxlength= "30" name= "ecsChangePwdForm" size= "40" readonly= "true" value= \\'\\'/>

C. catch (Exception e) { if (log.isDebugEnabled()) log.debug (context, EVENTS.ADHOC, "Caught InvalidGSMException Exception —andquot;

+ e.toString() );

}

D.

Correct Answer: B

**QUESTION 8**

An employee decides to log into an authorized system The system does not prompt the employee for authentication prior to granting access to the console, and it cannot authenticate the network resources. Which of the following attack types can this lead to if it is not mitigated?

A. Memory leak

B. Race condition

C. Smurf

D. Deadlock

Correct Answer: C

Reference: https://www imperva com/learn/ddos/smurf-attack-ddos/

**QUESTION 9**

A software development company is building a new mobile application for its social media platform. The company wants to gain its users\\' trust by reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users\\' trust, the company has released the following internal guidelines:

1.

Mobile clients should verity the identity of all social media servers locally.

2.

Social media servers should improve TLS performance of their certificate status.

3.

Social media servers should inform the client to only use HTTPS.

Given the above requirements, which of the following should the company implement? (Choose two.)

A. Quick UDP internet connection

B. OCSP stapling

C. Private CA

D. DNSSEC

E. CRL

F. HSTS

G. Distributed object model

Correct Answer: BF

**QUESTION 10**

A network engineer is concerned about hosting web, SFTP. and email services in a single DMZ that is hosted in the same security zone This could potentially allow lateral movement within the environment. Which of the following should the engineer implement to mitigate the risk?

A. Put all the services on a single host to reduce the number of servers.

B. Create separate security zones for each service and use ACLs for segmentation.

C. Keep the web server in the DMZ and move the other server services to the internal network.

D. Deploy a switch and create VLANs for each service.

Correct Answer: B

**QUESTION 11**

A security consultant has been asked to recommend a secure network design that would:

1.

Permit an existing OPC server to communicate with a new Modbus server that is controlling electrical relays.

2.

Limit operational disruptions.

Due to the limitations within the Modbus protocol, which of the following configurations should the security engineer recommend as part of the solution?

A. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 135.

B. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 102.

C. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 5000.

D. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502.

Correct Answer: D

**QUESTION 12**

A significant weather event caused all systems to fail over to the disaster recovery site successfully. However, successful data replication has not occurred in the last six months, which has resulted in the service being unavailable. Which of the following would BEST prevent this scenario form happening again?

A. Performing routine tabletop exercises

B. Implementing scheduled, full interruption tests

C. Backing up system log reviews

D. Performing department disaster recovery walk-throughs

Correct Answer: B

**QUESTION 13**

The Chief Information Security Officer is concerned about the possibility of employees downloading malicious files from the internet and opening them on corporate workstations. Which of the following solutions would be BEST to reduce this risk?

A. Integrate the web proxy with threat intelligence feeds.

B. Scan all downloads using an antivirus engine on the web proxy.

C. Block known malware sites on the web proxy.

D. Execute the files in the sandbox on the web proxy.

Correct Answer: D

Sandboxing provides a proactive approach, evaluating files based on behavior and potentially catching malicious files that signature-based solutions might miss.

**QUESTION 14**

An organization is in frequent litigation and has a large number of legal holds. Which of the following types of functionality should the organization\\'s new email system provide?

A. DLP

B. Encryption

C. E-discovery

D. Privacy-level agreements

Correct Answer: C

**QUESTION 15**

An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting

the smart card to high temperatures, the secret key could be revealed. Which of the following side-channel attacks did the team use?

A. Differential power analysis

B. Differential fault analysis

C. Differential temperature analysis

D. Differential timing analysis

Correct Answer: B

"Differential fault analysis (DFA) is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults--unexpected environmental conditions--into cryptographic operations, to reveal their internal states."

Reference: https://www.hitachi-hightech.com/global/products/science/tech/ana/thermal/descriptions/dta.html