

CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam



NEW QUESTION 1

A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from `/var/log/auth.log: graphic.ssh_auth_log`.

Which of the following actions would BEST address the potential risks by the activity in the logs?

- A. Alerting the misconfigured service account password
- B. Modifying the AllowUsers configuration directive
- C. Restricting external port 22 access
- D. Implementing host-key preferences

Answer: C

Explanation:

Reference: <https://www.rapid7.com/blog/post/2017/10/04/how-to-secure-ssh-server-using-port-knocking-on-ubuntu-linux/>

NEW QUESTION 2

A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements.

Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

- A. Designing data protection schemes to mitigate the risk of loss due to multitenancy
- B. Implementing redundant stores and services across diverse CSPs for high availability
- C. Emulating OS and hardware architectures to blur operations from CSP view
- D. Purchasing managed FIM services to alert on detected modifications to covered data

Answer: A

NEW QUESTION 3

A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. The solution must also have the lowest power requirement on the CA.

Which of the following is the BEST solution?

- A. Deploy an RA on each branch office.
- B. Use Delta CRLs at the branches.
- C. Configure clients to use OCSP.
- D. Send the new CRLs by using GPO.

Answer: C

Explanation:

Reference: <https://www.sciencedirect.com/topics/computer-science/revoke-certificate>

NEW QUESTION 4

An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access.

Which of the following describes the administrator's discovery?

- A. A vulnerability
- B. A threat
- C. A breach
- D. A risk

Answer: A

Explanation:

Reference: <https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained>

NEW QUESTION 5

In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:

- * 1. International users reported latency when images on the web page were initially loading.
- * 2. During times of report processing, users reported issues with inventory when attempting to place orders.
- * 3. Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.

Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

- A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.
- B. Increase the bandwidth for the server that delivers images, use a CDN, change the database to a non-relational database, and split the ten API servers across two load balancers.
- C. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.
- D. Serve static-content object storage across different regions, increase the instance size on the managed relational database, and distribute the ten API servers across multiple regions.

Answer: A

NEW QUESTION 6

A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.

Which of the following is the MOST likely cause?

- A. The user agent client is not compatible with the WAF.
- B. A certificate on the WAF is expired.
- C. HTTP traffic is not forwarding to HTTPS to decrypt.
- D. Old, vulnerable cipher suites are still being used.

Answer: B

Explanation:

Reference: <https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-http-requests-no-user-agent/>

NEW QUESTION 7

Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.

Which of the following would be the BEST option to implement?

- A. Distributed connection allocation
- B. Local caching
- C. Content delivery network
- D. SD-WAN vertical heterogeneity

Answer: C

NEW QUESTION 8

A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.

Which of the following should the engineer report as the ARO for successful breaches?

- A. 0.5
- B. 8
- C. 50
- D. 36,500

Answer: A

Explanation:

Reference: <https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/>

NEW QUESTION 9

During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.

Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

- A. Spawn a shell using sudo and an escape string such as `sudo vim -c '!sh'`.
- B. Perform ASIC password cracking on the host.
- C. Read the `/etc/passwd` file to extract the usernames.
- D. Initiate unquoted service path exploits.
- E. Use the UNION operator to extract the database schema.

Answer: C

Explanation:

Reference: <https://docs.rapid7.com/insightvm/elevating-permissions/>

NEW QUESTION 10

An organization is implementing a new identity and access management architecture with the following objectives: Supporting MFA against on-premises infrastructure

Improving the user experience by integrating with SaaS applications

Applying risk-based policies based on location Performing just-in-time provisioning Which of the following authentication protocols should the organization implement to support these requirements?

- A. Kerberos and TACACS
- B. SAML and RADIUS
- C. OAuth and OpenID
- D. OTP and 802.1X

Answer: A

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/migrate-application-authentication-toazure-active-directory>

NEW QUESTION 10

Device event logs sources from MDM software as follows:

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

- A. Malicious installation of an application; change the MDM configuration to remove application ID 1220.
- B. Resource leak; recover the device for analysis and clean up the local storage.
- C. Impossible travel; disable the device's account and access while investigating.
- D. Falsified status reporting; remotely wipe the device.

Answer: A

NEW QUESTION 15

An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items. Which of the following phases establishes the identification and prioritization of critical systems and functions?

- A. Review a recent gap analysis.
- B. Perform a cost-benefit analysis.
- C. Conduct a business impact analysis.
- D. Develop an exposure factor matrix.

Answer: C

Explanation:

Reference: <https://itsm.ucsf.edu/business-impact-analysis-bia-0>

NEW QUESTION 20

A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:

Unauthorized insertions into application development environments

Authorized insiders making unauthorized changes to environment configurations Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

- A. Perform static code analysis of committed code and generate summary reports.
- B. Implement an XML gateway and monitor for policy violations.
- C. Monitor dependency management tools and report on susceptible third-party libraries.
- D. Install an IDS on the development subnet and passively monitor for vulnerable services.
- E. Model user behavior and monitor for deviations from normal.
- F. Continuously monitor code commits to repositories and generate summary logs.

Answer: CD

NEW QUESTION 22

A security analyst notices a number of SIEM events that show the following activity:

Which of the following response actions should the analyst take FIRST?

- A. Disable powershell.exe on all Microsoft Windows endpoints.
- B. Restart Microsoft Windows Defender.
- C. Configure the forward proxy to block 40.90.23.154.
- D. Disable local administrator privileges on the endpoints.

Answer: A

NEW QUESTION 27

Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the RPO for a disaster recovery event for this data classification is 24 hours.

Based on RPO requirements, which of the following recommendations should the management team make?

- A. Leave the current backup schedule intact and pay the ransom to decrypt the data.
- B. Leave the current backup schedule intact and make the human resources fileshare read-only.
- C. Increase the frequency of backups and create SIEM alerts for IOCs.
- D. Decrease the frequency of backups and pay the ransom to decrypt the data.

Answer: C

NEW QUESTION 31

A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.

Which of the following would be BEST suited to meet these requirements?

- A. ARF
- B. ISACs
- C. Node.js
- D. OVAL

Answer: D

NEW QUESTION 34

A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements: The credentials used to publish production software to the container registry should be stored in a secure location.

Access should be restricted to the pipeline service account, without the ability for the third-party developer to read the credentials directly. Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

- A. TPM
- B. Local secure password file
- C. MFA
- D. Key vault

Answer: A

Explanation:

Reference: <https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-fundamentals>

NEW QUESTION 38

A customer reports being unable to connect to a website at www.test.com to consume services. The customer notices the web application has the following published cipher suite:

Which of the following is the MOST likely cause of the customer's inability to connect?

- A. Weak ciphers are being used.
- B. The public key should be using ECDSA.
- C. The default should be on port 80.
- D. The server name should be test.com.

Answer: B

Explanation:

Reference: <https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa-ecdsa-are-there-easy-answers-forwhich-to-choose-when>

NEW QUESTION 42

A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

Which of the following would BEST mitigate this vulnerability?

- A. CAPTCHA
- B. Input validation
- C. Data encoding
- D. Network intrusion prevention

Answer: B

Explanation:

Reference: <https://hdivsecurity.com/owasp-xml-external-entities-xxe>

NEW QUESTION 43

A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:

The security engineer looks at the UTM firewall rules and finds the following:

Which of the following should the security engineer do to ensure IMAPS functions properly on the corporate user network?

- A. Contact the email service provider and ask if the company IP is blocked.
- B. Confirm the email server certificate is installed on the corporate computers.
- C. Make sure the UTM certificate is imported on the corporate computers.
- D. Create an IMAPS firewall rule to ensure email is allowed.

Answer: C

NEW QUESTION 44

All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:
Leaked to the media via printing of the documents
Sent to a personal email address
Accessed and viewed by systems administrators
Uploaded to a file storage site
Which of the following would mitigate the department's concerns?

- A. Data loss detection, reverse proxy, EDR, and PGP
- B. VDI, proxy, CASB, and DRM
- C. Watermarking, forward proxy, DLP, and MFA
- D. Proxy, secure VPN, endpoint encryption, and AV

Answer: B

NEW QUESTION 45

A security analyst is reviewing the following output:

Which of the following would BEST mitigate this type of attack?

- A. Installing a network firewall
- B. Placing a WAF inline
- C. Implementing an IDS
- D. Deploying a honeypot

Answer: A

NEW QUESTION 50

Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

- A. Importing the availability of messages
- B. Ensuring non-repudiation of messages
- C. Enforcing protocol conformance for messages
- D. Assuring the integrity of messages

Answer: D

NEW QUESTION 53

An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.

Which of the following historian server locations will allow the business to get the required reports in an ?? and IT environment?

- A. In the ?? environment, use a VPN from the IT environment into the ?? environment.
- B. In the ?? environment, allow IT traffic into the ?? environment.
- C. In the IT environment, allow PLCs to send data from the ?? environment to the IT environment.
- D. Use a screened subnet between the ?? and IT environments.

Answer: A

NEW QUESTION 55

An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:

Unstructured data being exfiltrated after an employee leaves the organization

Data being exfiltrated as a result of compromised credentials

Sensitive information in emails being exfiltrated

Which of the following solutions should the security team implement to mitigate the risk of data loss?

- A. Mobile device management, remote wipe, and data loss detection
- B. Conditional access, DoH, and full disk encryption
- C. Mobile application management, MFA, and DRM
- D. Certificates, DLP, and geofencing

Answer: A

NEW QUESTION 60

An organization is designing a network architecture that must meet the following requirements: Users will only be able to access predefined services.

Each user will have a unique allow list defined for access.

The system will construct one-to-one subject/object access paths dynamically.

Which of the following architectural designs should the organization use to meet these requirements?

- A. Peer-to-peer secure communications enabled by mobile applications
- B. Proxied application data connections enabled by API gateways
- C. Microsegmentation enabled by software-defined networking
- D. VLANs enabled by network infrastructure devices

Answer: C

NEW QUESTION 61

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.

Answer: C

NEW QUESTION 64

A company has hired a security architect to address several service outages on the endpoints due to new malware. The Chief Executive Officer's laptop was impacted while working from home. The goal is to prevent further endpoint disruption.

The edge network is protected by a web proxy.

Which of the following solutions should the security architect recommend?

- A. Replace the current antivirus with an EDR solution.
- B. Remove the web proxy and install a UTM appliance.
- C. Implement a deny list feature on the endpoints.
- D. Add a firewall module on the current antivirus solution.

Answer: C

NEW QUESTION 67

An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.

Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

- A. Migrating operations assumes the acceptance of all risk.
- B. Cloud providers are unable to avoid risk.
- C. Specific risks cannot be transferred to the cloud provider.
- D. Risks to data in the cloud cannot be mitigated.

Answer: C

Explanation:

Reference: <https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf>

NEW QUESTION 72

A business stores personal client data of individuals residing in the EU in order to process requests for mortgage loan approvals. Which of the following does the business's IT manager need to consider?

- A. The availability of personal data
- B. The right to personal data erasure
- C. The company's annual revenue
- D. The language of the web application

Answer: B

Explanation:

Reference: <https://gdpr.eu/right-to-beforgotten/#:~:text=Also%20known%20as%20the%20right,to%20delete%20their%20personal%20data.&text=The%20General%20Data%20Protection%20Regulation,collected%2C%20processed%2C%20and%20erased>

NEW QUESTION 76

A small business requires a low-cost approach to theft detection for the audio recordings it produces and sells. Which of the following techniques will MOST likely meet the business's needs?

- A. Performing deep-packet inspection of all digital audio files
- B. Adding identifying filesystem metadata to the digital audio files
- C. Implementing steganography
- D. Purchasing and installing a DRM suite

Answer: C

Explanation:

Reference: <https://portswigger.net/daily-swig/what-is-steganography-a-complete-guide-to-the-ancient-art-of-concealingmessages>

NEW QUESTION 81

A developer implement the following code snippet.

Which of the following vulnerabilities does the code snippet resolve?

- A. SQL inject
- B. Buffer overflow
- C. Missing session limit
- D. Information leakage

Answer: D

NEW QUESTION 85

Ann, a CIRT member, is conducting incident response activities on a network that consists of several hundred virtual servers and thousands of endpoints and users. The network generates more than 10,000 log messages per second. The enterprise belong to a large, web-based cryptocurrency startup, Ann has distilled the relevant information into an easily digestible report for executive management. However, she still needs to collect evidence of the intrusion that caused the incident .

Which of the following should Ann use to gather the required information?

- A. Traffic interceptor log analysis
- B. Log reduction and visualization tools
- C. Proof of work analysis
- D. Ledger analysis software

Answer: B

NEW QUESTION 90

A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option . Which of the following is the BEST solution for this company?

- A. Community cloud service model
- B. Multitenancy SaaS
- C. Single-tenancy SaaS
- D. On-premises cloud service model

Answer: A

NEW QUESTION 95

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CAS-004 Practice Exam Features:

- * CAS-004 Questions and Answers Updated Frequently
- * CAS-004 Practice Questions Verified by Expert Senior Certified Staff
- * CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CAS-004 Practice Test Here](#)