

CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam



NEW QUESTION 1

Which of the following are risks associated with vendor lock-in? (Choose two.)

- A. The client can seamlessly move data.
- B. The vendor can change product offerings.
- C. The client receives a sufficient level of service.
- D. The client experiences decreased quality of service.
- E. The client can leverage a multicloud approach.
- F. The client experiences increased interoperability.

Answer: BD

Explanation:

Reference: <https://www.cloudflare.com/learning/cloud/what-is-vendor-lockin/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%20the%20data>

NEW QUESTION 2

An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key.

Which of the following would BEST secure the REST API connection to the database while preventing the use of a hardcoded string in the request string?

- A. Implement a VPN for all APIs.
- B. Sign the key with DSA.
- C. Deploy MFA for the service accounts.
- D. Utilize HMAC for the keys.

Answer: D

Explanation:

Reference: <https://eclipsesource.com/blogs/2016/07/06/keyed-hash-message-authentication-code-in-rest-apis/>

NEW QUESTION 3

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 4

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 5

A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks.

Which of the following sources could the architect consult to address this security concern?

- A. SDLC
- B. OVAL
- C. IEEE
- D. OWASP

Answer: B

Explanation:

Reference: <https://dzone.com/articles/what-is-oval-a-community-driven-vulnerability-mana>

NEW QUESTION 6

A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.

Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

- A. The company will have access to the latest version to continue development.
- B. The company will be able to force the third-party developer to continue support.
- C. The company will be able to manage the third-party developer's development process.
- D. The company will be paid by the third-party developer to hire a new development team.

Answer: B

NEW QUESTION 7

A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.

After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

- A. Protecting
- B. Permissive
- C. Enforcing
- D. Mandatory

Answer: B

Explanation:

Reference: <https://source.android.com/security/selinux/customize>

NEW QUESTION 8

A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud.

IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.

Which of the following encryption methods should the cloud security engineer select during the implementation phase?

- A. Instance-based
- B. Storage-based
- C. Proxy-based
- D. Array controller-based

Answer: A

NEW QUESTION 9

A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped.

The files were transferred via TLSprotected HTTP sessions from systems that do not send traffic to those sites.

The technician will define this threat as:

- A. a decrypting RSA using obsolete and weakened encryption attack.
- B. a zero-day attack.
- C. an advanced persistent threat.
- D. an on-path attack.

Answer: A

Explanation:

Reference: <https://www.internetsociety.org/deploy360/tls/basics/>

NEW QUESTION 10

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 10

A security engineer thinks the development team has been hard-coding sensitive environment variables in its code. Which of the following would BEST secure the company's CI/CD pipeline?

- A. Utilizing a trusted secrets manager
- B. Performing DAST on a weekly basis
- C. Introducing the use of container orchestration
- D. Deploying instance tagging

Answer: A

Explanation:

Reference: <https://about.gitlab.com/blog/2021/04/09/demystifying-ci-cd-variables/>

NEW QUESTION 13

A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location.

Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

- A. Execute never
- B. No-execute
- C. Total memory encryption
- D. Virtual memory encryption

Answer: A

Explanation:

Reference: <https://developer.arm.com/documentation/102433/0100/Stack-smashing-and-execution-permissions>

NEW QUESTION 14

A company wants to protect its intellectual property from theft. The company has already applied ACLs and DACs. Which of the following should the company use to prevent data theft?

- A. Watermarking
- B. DRM
- C. NDA
- D. Access logging

Answer: D

NEW QUESTION 18

A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage. Which of the following is a security concern that will MOST likely need to be addressed during migration?

- A. Latency
- B. Data exposure
- C. Data loss
- D. Data dispersion

Answer: A

NEW QUESTION 21

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 24

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 26

A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:

Which of the following ciphers should the security analyst remove to support the business requirements?

- A. TLS_AES_128_CCM_8_SHA256
- B. TLS_DHE_DSS_WITH_RC4_128_SHA
- C. TLS_CHACHA20_POLY1305_SHA256
- D. TLS_AES_128_GCM_SHA256

Answer: C

NEW QUESTION 28

A security analyst is performing a vulnerability assessment on behalf of a client. The analyst must define what constitutes a risk to the organization. Which of the following should be the analyst's FIRST action?

- A. Create a full inventory of information and data assets.
- B. Ascertain the impact of an attack on the availability of crucial resources.
- C. Determine which security compliance standards should be followed.
- D. Perform a full system penetration test to determine the vulnerabilities.

Answer: C

NEW QUESTION 32

An organization's hunt team thinks a persistent threats exists and already has a foothold in the enterprise network.

Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

- A. Deploy a SOAR tool.
- B. Modify user password history and length requirements.
- C. Apply new isolation and segmentation schemes.
- D. Implement decoy files on adjacent hosts.

Answer: C

Explanation:

Reference: <https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/>

NEW QUESTION 33

A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/ output (I/O) on the disk drive.

Based on the output above, from which of the following process IDs can the analyst begin an investigation?

- A. 65
- B. 77
- C. 83
- D. 87

Answer: D

NEW QUESTION 35

A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line. Which of the following commands would be the BEST to run to view only active Internet connections?

- A. `sudo netstat -antu | grep "LISTEN" | awk '{print$5}'`
- B. `sudo netstat -nlt -p | grep "ESTABLISHED"`
- C. `sudo netstat -plntu | grep -v "Foreign Address"`
- D. `sudo netstat -pntu -w | column -t -s '$\w'`
- E. `sudo netstat -pntu | grep -P ^tcp`

Answer: B

Explanation:

Reference: <https://www.codegrepper.com/code-examples/shell/netstat+find+port>

NEW QUESTION 40

A security engineer was auditing an organization's current software development practice and discovered that multiple opensource libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.

Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

- A. Perform additional SAST/DAST on the open-source libraries.
- B. Implement the SDLC security guidelines.
- C. Track the library versions and monitor the CVE website for related vulnerabilities.
- D. Perform unit testing of the open-source libraries.

Answer: B

Explanation:

Reference: <https://www.whitesourcesoftware.com/resources/blog/application-security-best-practices/>

NEW QUESTION 44

A company is preparing to deploy a global service.

Which of the following must the company do to ensure GDPR compliance? (Choose two.)

- A. Inform users regarding what data is stored.
- B. Provide opt-in/out for marketing messages.

- C. Provide data deletion capabilities.
- D. Provide optional data encryption.
- E. Grant data access to third parties.
- F. Provide alternative authentication techniques.

Answer: AB

Explanation:

Reference: <https://gdpr.eu/compliance-checklist-us-companies/>

NEW QUESTION 45

A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic. Which of the following would satisfy the requirement?

- A. NIDS
- B. NIPS
- C. WAF
- D. Reverse proxy

Answer: B

Explanation:

Reference: <https://subscription.packtpub.com/book/networking-and-servers/9781782174905/5/ch05lv1sec38/differentiatingbetween-nids-and-nips>

NEW QUESTION 49

While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware. Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

- A. Pay the ransom within 48 hours.
- B. Isolate the servers to prevent the spread.
- C. Notify law enforcement.
- D. Request that the affected servers be restored immediately.

Answer: C

NEW QUESTION 52

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 56

Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

- A. Lattice-based cryptography
- B. Quantum computing
- C. Asymmetric cryptography
- D. Homomorphic encryption

Answer: C

Explanation:

Reference: <https://searchsecurity.techtarget.com/definition/cryptanalysis>

NEW QUESTION 61

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 65

A company publishes several APIs for customers and is required to use keys to segregate customer data sets. Which of the following would be BEST to use to store customer keys?

- A. A trusted platform module
- B. A hardware security module
- C. A localized key store
- D. A public key infrastructure

Answer: C

Explanation:

Reference: <https://developer.android.com/studio/publish/app-signing>

NEW QUESTION 68

A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources.

The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.

Which of the following should the security team recommend FIRST?

- A. Investigating a potential threat identified in logs related to the identity management system
- B. Updating the identity management system to use discretionary access control
- C. Beginning research on two-factor authentication to later introduce into the identity management system
- D. Working with procurement and creating a requirements document to select a new IAM system/vendor

Answer: A

NEW QUESTION 72

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 73

A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.

Which of the following actions would BEST resolve the issue? (Choose two.)

- A. Conduct input sanitization.

- B. Deploy a SIEM.
- C. Use containers.
- D. Patch the OS
- E. Deploy a WAF.
- F. Deploy a reverse proxy
- G. Deploy an IDS.

Answer: BD

NEW QUESTION 78

A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:

- * 1. The network supports core applications that have 99.99% uptime.
- * 2. Configuration updates to the SD-WAN routers can only be initiated from the management service.
- * 3. Documents downloaded from websites must be scanned for malware.

Which of the following solutions should the network architect implement to meet the requirements?

- A. Reverse proxy, stateful firewalls, and VPNs at the local sites
- B. IDSs, WAFs, and forward proxy IDS
- C. DoS protection at the hub site, mutual certificate authentication, and cloud proxy
- D. IPSs at the hub, Layer 4 firewalls, and DLP

Answer: B

NEW QUESTION 81

A security engineer needs to recommend a solution that will meet the following requirements: Identify sensitive data in the provider's network
Maintain compliance with company and regulatory guidelines

Detect and respond to insider threats, privileged user threats, and compromised accounts Enforce datacentric security, such as encryption, tokenization, and access control Which of the following solutions should the security engineer recommend to address these requirements?

- A. WAF
- B. CASB
- C. SWG
- D. DLP

Answer: A

NEW QUESTION 83

An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:

Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

- A. Password cracker
- B. Port scanner
- C. Account enumerator
- D. Exploitation framework

Answer: A

NEW QUESTION 88

A health company has reached the physical and computing capabilities in its datacenter, but the computing demand continues to increase. The infrastructure is fully virtualized and runs custom and commercial healthcare application that process sensitive health and payment information .

Which of the following should the company implement to ensure it can meet the computing demand while complying with healthcare standard for virtualization and cloud computing?

- A. Hybrid IaaS solution in a single-tenancy cloud
- B. PaaS solution in a multi-tenancy cloud
- C. SaaS solution in a community cloud
- D. Private SaaS solution in a single tenancy cloud.

Answer: D

NEW QUESTION 90

An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, reports come in that a previously vulnerability has returned .

Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

- A. Peer review
- B. Regression testing
- C. User acceptance
- D. Dynamic analysis

Answer: A

NEW QUESTION 92

Company A is establishing a contractual with Company B. The terms of the agreement are formalized in a document covering the payment terms, limitation of liability, and intellectual property rights .

Which of the following documents will MOST likely contain these elements?

- A. Company A-B SLA v2.docx
- B. Company A OLA v1b.docx
- C. Company A MSA v3.docx
- D. Company A MOU v1.docx
- E. Company A-B NDA v03.docx

Answer: A

NEW QUESTION 94

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 97

A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employees recently received an email that approved to be claim form, but it installed malicious software on the employee's laptop when was opened.

- A. Impalement application whitelisting and add only the email client to the whitelist for laptop in the claims processing department.
- B. Required all laptops to connect to the VPN before accessing email.
- C. Implement cloud-based content filtering with sandboxing capabilities.
- D. Install a mail gateway to scan incoming messages and strip attachments before they reach the mailbox.

Answer: C

NEW QUESTION 99

.....

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](#)