

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

<https://www.2passeasy.com/dumps/CAS-004/>



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 undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.

Which of the following would be BEST to proceed with the transformation?

- A. An on-premises solution as a backup
- B. A load balancer with a round-robin configuration
- C. A multicloud provider solution
- D. An active-active solution within the same tenant

Answer: D

NEW QUESTION 3

A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test. Computational resources ran out at 70% of restoration of critical services.

Which of the following should be modified to prevent the issue from reoccurring?

- A. Recovery point objective
- B. Recovery time objective
- C. Mission-essential functions
- D. Recovery service level

Answer: B

Explanation:

Reference: <https://www.nakivo.com/blog/disaster-recovery-in-cloud-computing/>

NEW QUESTION 4

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 5

A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away. Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

- A. Scan the code with a static code analyzer, change privileged user passwords, and provide security training.
- B. Change privileged usernames, review the OS logs, and deploy hardware tokens.
- C. Implement MFA, review the application logs, and deploy a WAF.
- D. Deploy a VPN, configure an official open-source library repository, and perform a full application review for vulnerabilities.

Answer: D

Explanation:

Reference: <https://www.microfocus.com/en-us/what-is/sast>

NEW QUESTION 6

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 7

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 8

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 9

A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation.

Which of the following is the BEST solution to meet these objectives?

- A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.
- B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
- C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
- D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Answer: A

Explanation:

Reference: <https://www.cyberark.com/what-is/privileged-access-management/>

NEW QUESTION 10

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 10

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 15

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 20

A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed. Which of the following will allow the inspection of the data without multiple certificate deployments?

- A. Include all available cipher suites.
- B. Create a wildcard certificate.
- C. Use a third-party CA.
- D. Implement certificate pinning.

Answer: D

NEW QUESTION 22

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 25

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 30

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 35

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 39

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 43

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 45

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 49

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 50

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 52

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/ch05lvl1sec38/differentiatingbetween-nids-and-nips>

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 58

A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation: `graphic.linux_randomization.prg`
Which of the following technologies would mitigate the manipulation of memory segments?

- A. NX bit
- B. ASLR
- C. DEP
- D. HSM

Answer: B

Explanation:

Reference: <http://webpages.eng.wayne.edu/~fy8421/19sp-csc5290/labs/lab2-instruction.pdf> (3)

NEW QUESTION 63

An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:

ERR_SSL_VERSION_OR_CIPHER_MISMATCH

Which of the following is MOST likely the root cause?

- A. The client application is testing PFS.
- B. The client application is configured to use ECDHE.
- C. The client application is configured to use RC4.
- D. The client application is configured to use AES-256 in GCM.

Answer: C

Explanation:

Reference: https://kinsta.com/knowledgebase/err_ssl_version_or_cipher_mismatch/

NEW QUESTION 68

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 73

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 78

A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.

Which of the following techniques would be BEST suited for this requirement?

- A. Deploy SOAR utilities and runbooks.
- B. Replace the associated hardware.
- C. Provide the contractors with direct access to satellite telemetry data.
- D. Reduce link latency on the affected ground and satellite segments.

Answer: A

NEW QUESTION 82

A company plans to build an entirely remote workforce that utilizes a cloud-based infrastructure. The Chief Information Security Officer asks the security engineer to design connectivity to meet the following requirements:

Only users with corporate-owned devices can directly access servers hosted by the cloud provider. The company can control what SaaS applications each individual user can access. User browser activity can be monitored.

Which of the following solutions would BEST meet these requirements?

- A. IAM gateway, MDM, and reverse proxy
- B. VPN, CASB, and secure web gateway
- C. SSL tunnel, DLP, and host-based firewall
- D. API gateway, UEM, and forward proxy

Answer: B

NEW QUESTION 86

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 91

DRAG DROP

An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS

Review the following scenarios and instructions. Match each relevant finding to the affected host.

After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding. Each finding may be used more than once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button. Select and Place:

A.

A.

Answer: A

NEW QUESTION 92

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 94

After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary

ISP that is not normally used.

Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

- A. Disable BGP and implement a single static route for each internal network.
- B. Implement a BGP route reflector.
- C. Implement an inbound BGP prefix list.
- D. Disable BGP and implement OSPF.

Answer: B

NEW QUESTION 98

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 103

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 104

Over the last 90 days, many storage services has been exposed in the cloud services environments, and the security team does not have the ability to see is creating these instance. Shadow IT is creating data services and instances faster than the small security team can keep up with them. The Chief information security Officer (CIASO) has asked the security officer (CISO) has asked the security lead architect to architect to recommend solutions to this problem. Which of the following BEST addresses the problem best address the problem with the least amount of administrative effort?

- A. Compile a list of firewall requests and compare than against interesting cloud services.
- B. Implement a CASB solution and track cloud service use cases for greater visibility.
- C. Implement a user-behavior system to associate user events and cloud service creation events.
- D. Capture all log and feed then to a SIEM and then for cloud service events

Answer: C

NEW QUESTION 107

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 111

A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

Which of the following should the security analyst perform?

- A. Contact the security department at the business partner and alert them to the email event.
- B. Block the IP address for the business partner at the perimeter firewall.
- C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.
- D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

Answer: A

NEW QUESTION 116

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAS-004 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAS-004 Product From:

<https://www.2passeasy.com/dumps/CAS-004/>

Money Back Guarantee

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