

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 security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources.

Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

- A. Union filesystem overlay
- B. Cgroups
- C. Linux namespaces
- D. Device mapper

Answer: B

Explanation:

Reference: <https://www.ibm.com/support/pages/deep-dive-yarn-cgroups-hadoop-dev>

NEW QUESTION 3

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 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 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 6

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 7

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 8

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 9

An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.

Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

- A. NIST
- B. GDPR
- C. PCI DSS
- D. ISO

Answer: C

Explanation:

Reference: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

NEW QUESTION 10

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 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 13

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 15

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 16

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 21

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 25

During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee. Which of the following processes would BEST satisfy this requirement?

- A. Monitor camera footage corresponding to a valid access request.
- B. Require both security and management to open the door.
- C. Require department managers to review denied-access requests.
- D. Issue new entry badges on a weekly basis.

Answer: A

Explanation:

Reference: <https://www.getkisi.com/access-control>

NEW QUESTION 26

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 29

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 31

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 32

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 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 37

A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.

Which of the following would provide the BEST boot loader protection?

- A. TPM
- B. HSM
- C. PKI
- D. UEFI/BIOS

Answer: D

Explanation:

Reference: <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-898217D4-689D-4EB5-866C-888353FE241C.html>

NEW QUESTION 39

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 43

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 45

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$5}'`
- B. `sudo netstat -nlt -p | grep "ESTABLISHED"`
- C. `sudo netstat -plntu | grep -v "Foreign Address"`
- D. `sudo netstat -pnut -w | column -t -s '$\w'`
- E. `sudo netstat -pnut | grep -P ^tcp`

Answer: B

Explanation:

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

NEW QUESTION 49

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 50

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 51

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 52

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 54

An organization wants to perform a scan of all its systems against best practice security configurations.

Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

- A. ARF
- B. XCCDF
- C. CPE
- D. CVE
- E. CVSS
- F. OVAL

Answer: BF

Explanation:

Reference: <https://www.govinfo.gov/content/pkg/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6/pdf/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6.pdf> (p.12)

NEW QUESTION 56

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 61

The Chief information Officer (CIO) wants to establish a non-banding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership .

Which of the follow would MOST likely be used?

- A. MOU
- B. OLA
- C. NDA
- D. SLA

Answer: A

NEW QUESTION 63

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 68

A company is repeatedly being breached by hackers who valid credentials. The company's Chief information Security Officer (CISO) has installed multiple controls for authenticating users, including biometric and token-based factors. Each successive control has increased overhead and complexity but has failed to stop further breaches. An external consultant is evaluating the process currently in place to support the authentication controls .

Which of the following recommendation would MOST likely reduce the risk of unauthorized access?

- A. Implement strict three-factor authentication.
- B. Implement least privilege policies
- C. Switch to one-time or all user authorizations.
- D. Strengthen identify-proofing procedures

Answer: A

NEW QUESTION 71

.....

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