

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

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



NEW QUESTION 1

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 2

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 3

A company's SOC has received threat intelligence about an active campaign utilizing a specific vulnerability. The company would like to determine whether it is vulnerable to this active campaign.

Which of the following should the company use to make this determination?

- A. Threat hunting
- B. A system penetration test
- C. Log analysis within the SIEM tool
- D. The Cyber Kill Chain

Answer: B

NEW QUESTION 4

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 5

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 6

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 7

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 8

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 9

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 10

A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users. Which of the following would be BEST for the developer to perform? (Choose two.)

- A. Utilize code signing by a trusted third party.
- B. Implement certificate-based authentication.
- C. Verify MD5 hashes.
- D. Compress the program with a password.
- E. Encrypt with 3DES.
- F. Make the DACL read-only.

Answer: AB

NEW QUESTION 10

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 13

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 18

A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.

Which of the following should the security engineer do to BEST manage the threats proactively?

- A. Join an information-sharing community that is relevant to the company.
- B. Leverage the MITRE ATT&CK framework to map the TTR.
- C. Use OSINT techniques to evaluate and analyze the threats.
- D. Update security awareness training to address new threats, such as best practices for data security.

Answer: D

NEW QUESTION 23

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 27

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 28

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 33

Which of the following is a benefit of using steganalysis techniques in forensic response?

- A. Breaking a symmetric cipher used in secure voice communications
- B. Determining the frequency of unique attacks against DRM-protected media
- C. Maintaining chain of custody for acquired evidence
- D. Identifying least significant bit encoding of data in a .wav file

Answer: D

Explanation:

Reference: https://www.garykessler.net/library/fsc_stego.html

NEW QUESTION 38

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 39

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 40

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 41

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 42

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 47

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 50

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 53

.....

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