

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/>

Obviously the specification for the hash calculation must be precise when different implementations on the server and the client are expected. Here's an example:

```
com.eclipsesource.auth.hash.sha256 = AccessKeyId + ":" + Signature

Signature = Base64( HMAC-SHA256( YourSecretAccessKeyID, UTF-8-Encoding-Of( .StringToSign ) ) );

StringToSign = HTTP-Verb + "\n" +
  Content-Type + "\n" +
  CanonicalizedResource + "\n" +
  CanonicalizedApplicationHeaders +
  CanonicalizedFormParameters

CanonicalizedResource =
CanonicalizedApplicationHeaders = [ CanonicalizedApplicationHeader + "\n" ]
CanonicalizedApplicationHeader = HeaderName + ":" + HeaderValue + "\n"
CanonicalizedFormParameters = [ CanonicalizedFormParameter + "\n" ]
CanonicalizedFormParameter = ParameterName + ":" + ParameterValue
```

NEW QUESTION 2

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/>

The essential element of traditional disaster recovery is a secondary data center, which can store all redundant copies of critical data, and to which you can fail over production workloads. A traditional on-premises DR site generally includes the following:

- A dedicated facility for housing the IT infrastructure, including maintenance employees and computing equipment.
- Sufficient server capacity to ensure a high level of operational performance and allow the data center to scale up or scale out depending on your business needs.
- Internet connectivity with sufficient bandwidth to enable remote access to the secondary data center.
- Network infrastructure, including firewalls, routers, and switches, to ensure a reliable connection between the primary and secondary data centers, as well as provide data availability.

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

A threat hunting team receives a report about possible APT activity in the network. Which of the following threat management frameworks should the team implement?

- A. NIST SP 800-53
- B. MITRE ATT&CK
- C. The Cyber Kill Chain
- D. The Diamond Model of Intrusion Analysis

Answer: A

Explanation:

Reference: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>

NEW QUESTION 5

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/>

First, create the regex pattern set:

1. Open the [AWS WAF console](#).
2. In the navigation pane, under **AWS WAF**, choose **Regex pattern sets**.
3. For **Region**, select the Region where you created your web access control list (web ACL).
Note: Select **Global** if your web ACL is set up for Amazon CloudFront.
4. Choose **Create regex pattern sets**.
5. For **Regex pattern set name**, enter **testpattern**.
6. For **Regular expressions**, enter **.+**
7. Choose **Create regex pattern set**.

NEW QUESTION 6

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 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>

1. Use the latest Android kernel.
2. Adopt the principle of least privilege.
3. Address only your own additions to Android. The default policy works with the Android Open Source Project codebase automatically.
4. Compartmentalize software components into modules that conduct singular tasks.
5. Create SELinux policies that isolate those tasks from unrelated functions.
6. Put those policies in *.te files (the extension for SELinux policy source files) within the `/device/manufacturer/device-name/sepolicy` directory and use `BOARD_SEPOLICY` variables to include them in your build.
7. Make new domains permissive initially. This is done by using a permissive declaration in the domain's *.te file.
8. Analyze results and refine your domain definitions.
9. Remove the permissive declaration when no further denials appear in userdebug builds.

NEW QUESTION 8

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 9

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 10

A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks.

Which of the following would be the BEST solution against this type of attack?

- A. Cookies
- B. Wildcard certificates
- C. HSTS
- D. Certificate pinning

Answer: C

Explanation:

Reference: <https://cloud.google.com/security/encryption-in-transit>

ALTS has a secure handshake protocol similar to mutual TLS. Two services wishing to communicate using ALTS employ this handshake protocol to authenticate and negotiate communication parameters before sending any sensitive information. The protocol is a two-step process:

- **Step 1: Handshake** The client initiates an elliptic curve-Diffie Hellman (ECDH) handshake with the server using Curve25519. The client and server each have certified ECDH public parameters as part of their certificate, which is used during a Diffie Hellman key exchange. The handshake results in a common traffic key that is available on the client and the server. The peer identities from the certificates are surfaced to the application layer to use in authorization decisions.
- **Step 2: Record encryption** Using the common traffic key from Step 1, data is transmitted from the client to the server securely. Encryption in ALTS is implemented using BoringSSL and other encryption libraries. Encryption is most commonly AES-128-GCM while integrity is provided by AES-GCM's GMAC.

NEW QUESTION 10

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 13

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:

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Signature hash algorithm:
sha256
Public key:
RSA (2048 Bits)
.htaccess config:
<VirtualHost> *:80>
ServerName www.test.com
Redirect / https://www.test.com
</VirtualHost>
<VirtualHost _default_:443>
ServerName www.test.com
DocumentRoot /usr/local/apache2/htdocs
SSLEngine On
...
</VirtualHost>
```

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 14

A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year. Which of the following will MOST likely secure the data on the lost device?

- A. Require a VPN to be active to access company data.
- B. Set up different profiles based on the person's risk.
- C. Remotely wipe the device.
- D. Require MFA to access company applications.

Answer: D

NEW QUESTION 18

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:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_RC4_128_SHA
RSA_WITH_AES_128_CCM
```

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 23

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>

This task describes how to use the vSphere Client to enable and disable secure boot for a virtual machine. You can also write scripts to manage virtual machine settings. For example, you can automate changing the firmware from BIOS to EFI for virtual machines with the following PowerCLI code:

```
$vm = Get-VM TestVM  
  
$spec = New-Object VMware.Vim.VirtualMachineConfigSpec  
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]:efi  
$vm.ExtensionData.ReconfigVM($spec)
```

NEW QUESTION 24

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 29

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 31

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 35

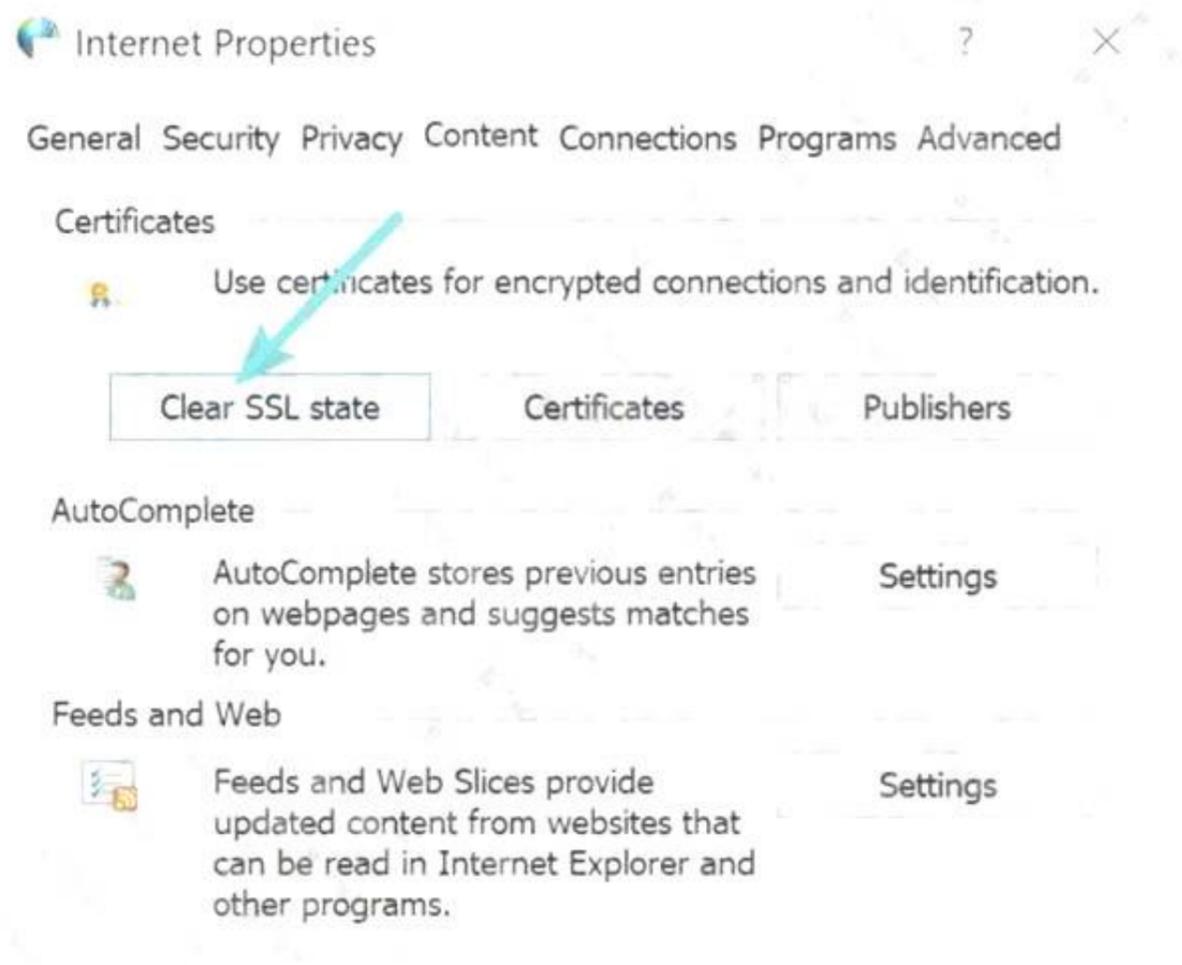
An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:

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 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 41

A company that all mobile devices be encrypted, commensurate with the full disk encryption scheme of assets, such as workstation, servers, and laptops.

Which of the following will MOST likely be a limiting factor when selecting mobile device managers for the company?

- A. Increased network latency
- B. Unavailable of key escrow
- C. Inability to selected AES-256 encryption
- D. Removal of user authentication requirements

Answer: A

NEW QUESTION 43

.....

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