# CompTIA

## Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

# About Exambible

*Your Partner of IT Exam*

# Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

# Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

**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/

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

**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**
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 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/

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 8**
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 9**

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 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

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 10**

An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.

Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.
B. Change the operating system.
C. Buy a new server and create an active-active cluster.
D. Upgrade the server with a new one.

**Answer:** A

**NEW QUESTION 12**

Device event logs sources from MDM software as follows:

```
Device        Date/Time      Location            Event       Description
ANDROID_1022  01JAN21 0255   39.9072N,77.0369W   PUSH        APPLICATION 1220 INSTALL QUEUED
ANDROID_1022  01JAN21 0301   39.9072N,77.0369W   INVENTORY   APPLICATION 1220 ADDED
ANDROID_1022  01JAN21 0701   39.0067N,77.4291W   CHECK-IN    NORMAL
ANDROID_1022  01JAN21 0701   25.2854N,51.5310E   CHECK-IN    NORMAL
ANDROID_1022  01JAN21 0900   39.0067N,77.4291W   CHECK-IN    NORMAL
ANDROID_1022  01JAN21 1030   39.0067N,77.4291W   STATUS      LOCAL STORAGE REPORTING 85% FULL
```

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 17**
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

What are the types of BIAs?

There are two types of BIAs:

1. Comprehensive BIA: A Comprehensive BIA is conducted for all critical applications or systems that must be restored within 24 hours following a disaster.

2. Basic BIA: A Basic BIA is an abbreviated version of the Comprehensive BIA and is conducted for less critical applications or systems

**NEW QUESTION 19**
A security analyst notices a number of SIEM events that show the following activity:

```
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop WinDefend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptiacasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell
https://content.comptia.com/content.exam.ps1
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell --> 40.90.23.154:443
```

Which of the following response actions should the analyst take FIRST?

A. Disable powershell.exe on all Microsoft Windows endpoints.
B. Restart Microsoft Windows Defender.
C. Configure the forward proxy to block 40.90.23.154.
D. Disable local administrator privileges on the endpoints.

**Answer:** A

**NEW QUESTION 20**
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 22**
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 25**
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/

When creating a CI/CD variable in the settings, GitLab gives the user more configuration options for the variable. Use these extra configuration options for stricter control over more sensitive variables:

1. **Environment scope**: If a variable only ever needs to be used in one specific environment, set it to only ever be available in that environment. For example, you can set a deploy token to only be available in the `production` environment.

2. **Protected variables**: Similar to the environment scope, you can set a variable to be available only when the pipeline runs on a protected branch, like your default branch.

3. **Masked**: Variables that contain secrets should always be masked. This lets you use the variable in job scripts without the risk of exposing the value of the variable. If someone tries to output it in a job log with a command like `echo $VARIABLE`, the job log will only show `echo [masked]`. There are limits to the types of values that can be masked.

**NEW QUESTION 28**
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 30**
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 34**
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 39**
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
DocumnetRoot /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 42**
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:

- VLAN 30        Guest networks                    192.168.20.0/25
- VLAN 20        Corporate user network            192.168.0.0/28
- VLAN 110       Corporate server network          192.168.0.16/29

The security engineer looks at the UTM firewall rules and finds the following:

| Rule active | Firewall ID | Source | Destination | Ports | Action | TLS decryption |
|---|---|---|---|---|---|---|
| Yes | 58 | VLAN 20 | 15.22.33.45 | 143 | Allow and log | Enabled |
| Yes | 33 | VLAN 30 | Any | 80, 443, | Allow and log | Disabled |
| Yes | 22 | VLAN 110 | VLAN 20 | Any | Allow and log | Disabled |
| No | 21 | VLAN 20 | 15.22.33.45 | 990 | Allow and log | Disabled |
| Yes | 20 | VLAN 20 | VLAN 110 | Any | Allow and log | Enabled |
| Yes | 19 | VLAN 20 | Any | 993, 587 | Allow and log | Enabled |

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 47**
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 51**
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 54**

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 55**
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.

```
procs ---------memory---------swap---io-- --system-- -----cpu------
r  b  swpd  free    buff   cache   si  so  bi      bo       in   cs   us  sy  id  wa  st
3  0  0     44712  110052  623096  0   0   304023  30004040 217  883  13  3   83  1   0
1  0  0     44408  110052  623096  0   0   300     200003   88   1446 31  4   65  0   0
0  0  0     44524  110052  623096  0   0   400020  20       84   872  11  2   87  0   0
0  2  0     44516  110052  623096  0   0   10      0        149  142  18  5   77  0   0
0  0  0     44524  110052  623096  0   0   0       0        60   431  14  1   85  0   0
```

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 57**
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 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 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:
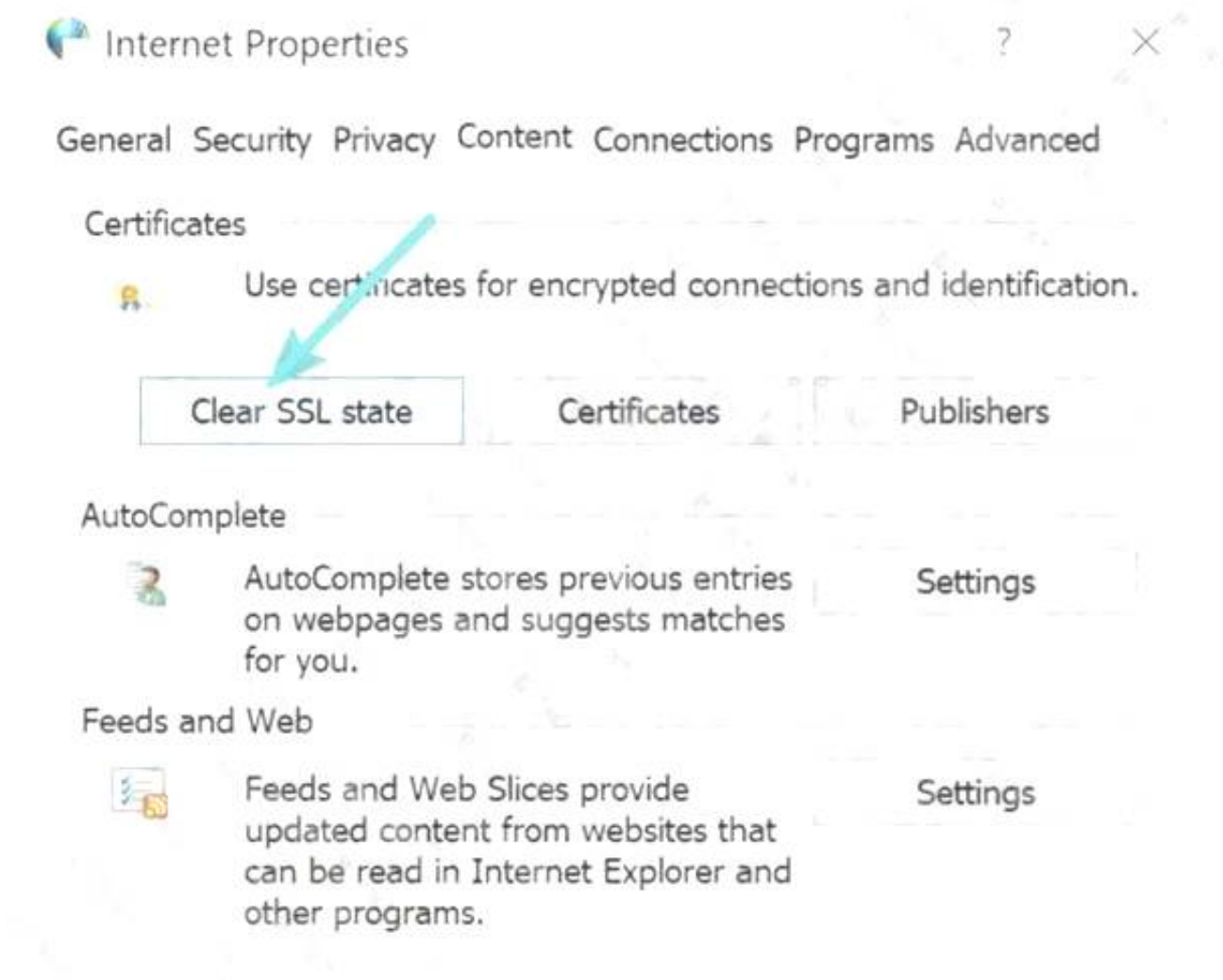ERR_SSL_VERSION_OR_CIPHER_MISMATCH
Which of the following is MOST likely the root cause?

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/

Internet Properties                                    ?        ✕

General  Security  Privacy  Content  Connections  Programs  Advanced

Certificates

        Use certificates for encrypted connections and identification.

        Clear SSL state          Certificates          Publishers

AutoComplete

        AutoComplete stores previous entries          Settings
        on webpages and suggests matches
        for you.

Feeds and Web

        Feeds and Web Slices provide          Settings
        updated content from websites that
        can be read in Internet Explorer and
        other programs.

**NEW QUESTION 66**
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 68**
An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.
Which of the following processes can be used to identify potential prevention recommendations?

A. Detection
B. Remediation
C. Preparation
D. Recovery
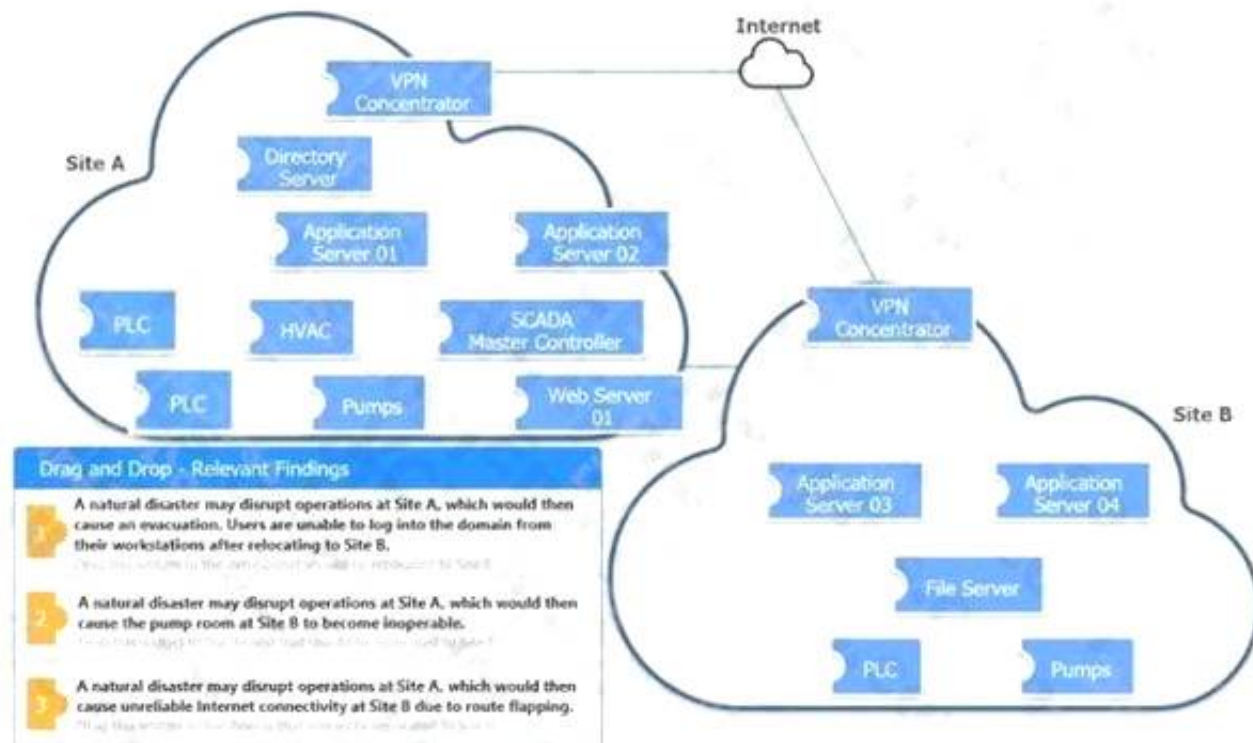
**Answer:** A

**NEW QUESTION 69**
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 70

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 71

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 75

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 76

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 78**
The Chief information Officer (CIO) asks the system administrator to improve email security at the company based on the following requirements:
* Transaction being requested by unauthorized individuals.
* Complete discretion regarding client names, account numbers, and investment information.
* Malicious attackers using email to malware and ransomeware.
* Exfiltration of sensitive company information.
The cloud-based email solution will provide anti-malware reputation-based scanning, signature-based scanning, and sandboxing .
Which of the following is the BEST option to resolve the boar's concerns for this email migration?

A. Data loss prevention
B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

**Answer:** A

**NEW QUESTION 80**
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 85**
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 90**
......

# Relate Links

**100% Pass Your CAS-004 Exam with Exambible Prep Materials**

https://www.exambible.com/CAS-004-exam/

# Contact us

**We are proud of our high-quality customer service, which serves you around the clock 24/7.**

**Viste -** https://www.exambible.com/

# Relate Links

**100% Pass Your CAS-004 Exam with Exambible Prep Materials**

https://www.exambible.com/CAS-004-exam/