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
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 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
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 4
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 5

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 6
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 7
A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.
Which of the following should the engineer report as the ARO for successful breaches?

A. 0.5
B. 8
C. 50
D. 36,500

Answer: A

Explanation:
Reference: https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/
There are two types of risk analysis — quantitative and qualitative:

- **Quantitative risk analysis** is an objective approach that uses hard numbers to assess the likelihood and impact of risks. The process involves calculating metrics, such as annual loss expectancy, to help you determine whether a given risk mitigation effort is worth the investment. The assessment requires well-developed project models and high-quality data.
- **Qualitative risk analysis** is a quicker way to gauge the likelihood of potential risks and their impact so you can prioritize them for further assessment. While quantitative risk analysis is objective, qualitative risk analysis is a subjective approach that ranks risks in broader terms, such as a scale of 1–5 or simply low, medium and

Both forms of risk analysis are valuable tools in risk management. In this article, we will focus on quantitative risk analysis and explain how to calculate annual loss expectancy (ALE).

NEW QUESTION 8
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 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
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
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

Manage cost

Your organization may have multiple Identity Access Management (IAM) solutions in place. Migrating to one Azure AD infrastructure is an opportunity to reduce dependencies on IAM licenses (on-premises or in the cloud) and infrastructure costs. In cases where you may have already paid for Azure AD via Microsoft 365 licenses, there is no reason to pay the added cost of another IAM solution.

With Azure AD, you can reduce infrastructure costs by:

- Providing secure remote access to on-premises apps using Azure AD Application Proxy
- Decoupling apps from the on-prem credential approach in your tenant by setting up Azure AD as the trusted universal identity provider

NEW QUESTION 11
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 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 15
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
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 23
Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

A. Key sharing
B. Key distribution
C. Key recovery
D. Key escrow

Answer: B

Explanation:
Reference: https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=48322§ion=1.3

NEW QUESTION 24
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 26
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 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 35
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 37
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 41
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 44
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 47
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 48
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 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 53
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 54
A security engineer was auditing an organization's current software development practice and discovered that multiple opensource libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.
Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

A. Perform additional SAST/DAST on the open-source libraries.
B. Implement the SDLC security guidelines.
C. Track the library versions and monitor the CVE website for related vulnerabilities.
D. Perform unit testing of the open-source libraries.

Answer: B

Explanation:
Reference: https://www.whitesourcesoftware.com/resources/blog/application-security-best-practices/

NEW QUESTION 57
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 60
An organization is designing a network architecture that must meet the following requirements: Users will only be able to access predefined services.
Each user will have a unique allow list defined for access.
The system will construct one-to-one subject/object access paths dynamically.
Which of the following architectural designs should the organization use to meet these requirements?

A. Peer-to-peer secure communications enabled by mobile applications
B. Proxied application data connections enabled by API gateways
C. Microsegmentation enabled by software-defined networking
D. VLANs enabled by network infrastructure devices

Answer: C

NEW QUESTION 61
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:
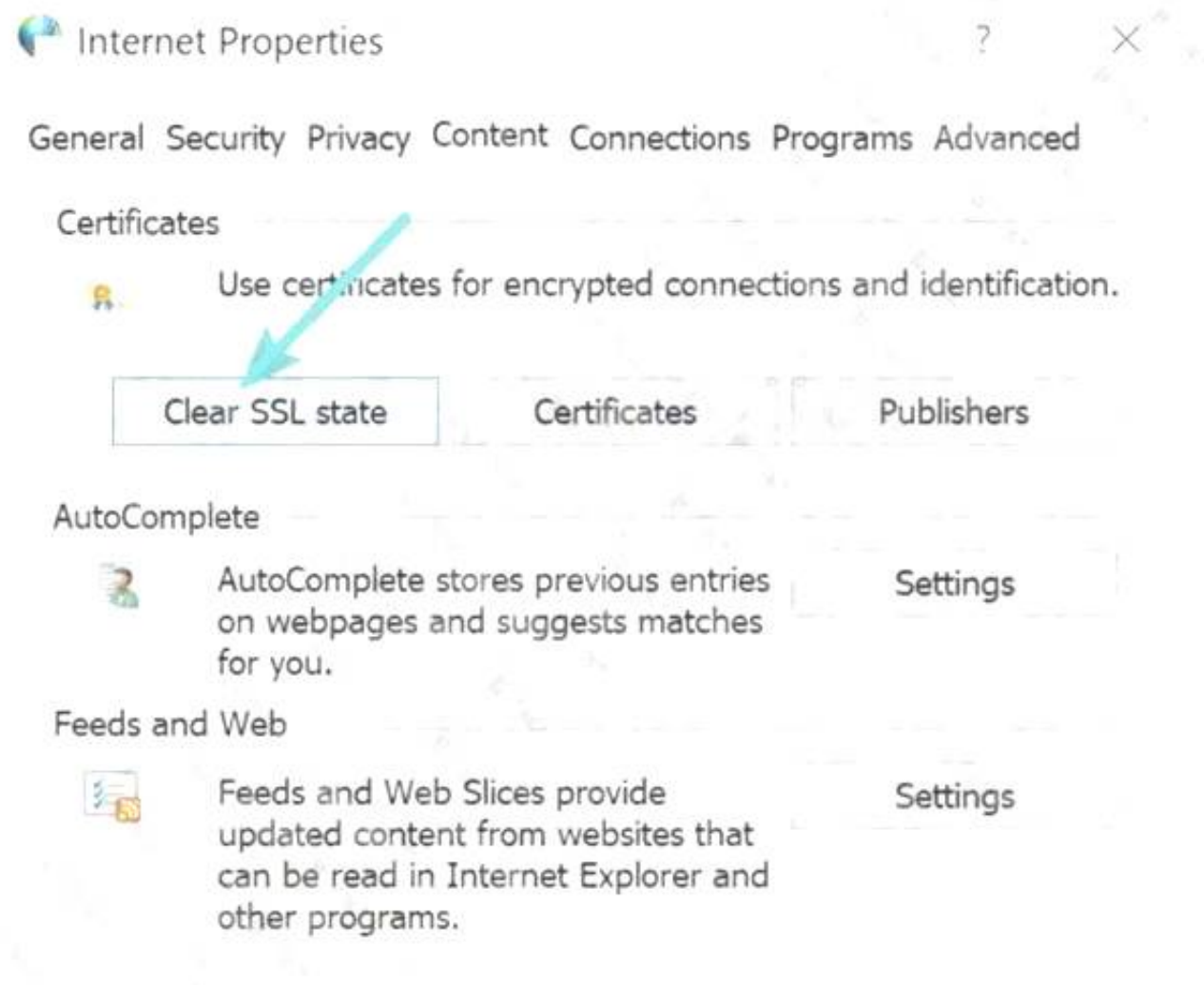ERR_SSL_VERSION_OR_CIPHER_MISMATCH
Which of the following is MOST likely the root cause?

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 66
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 67
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 72
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 76
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.

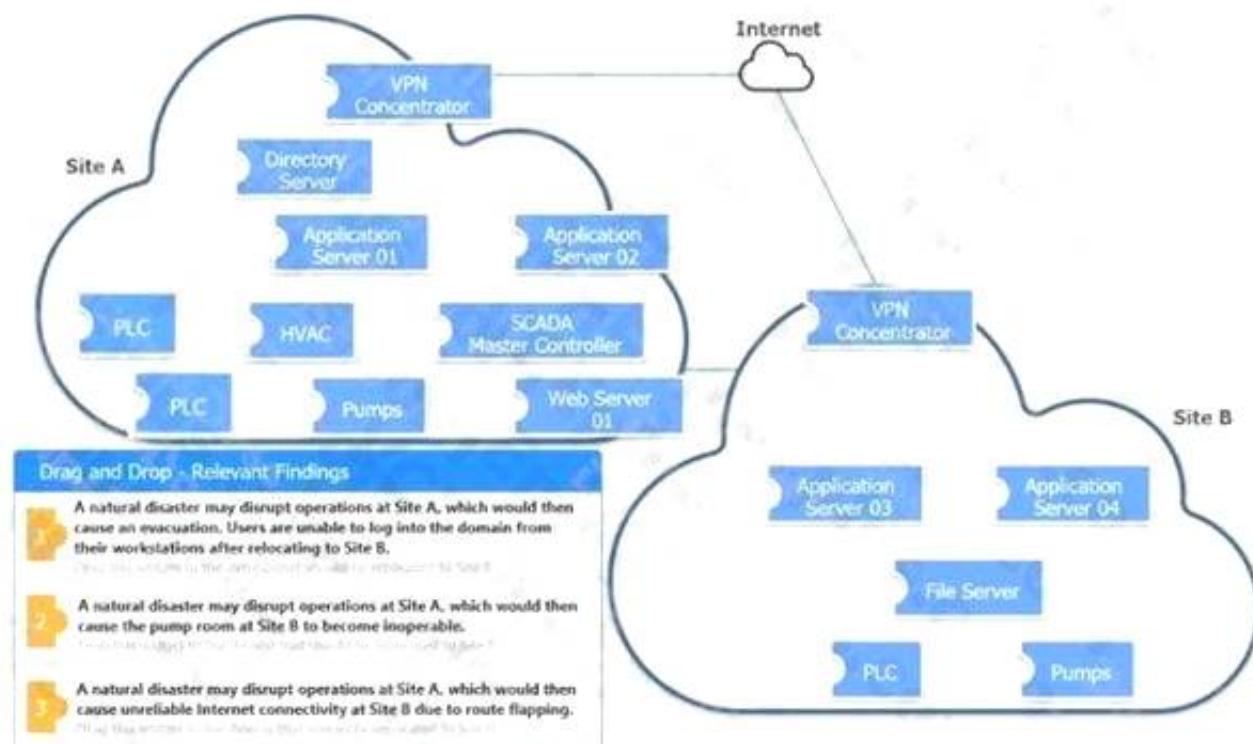**Answer:** C

NEW QUESTION 81
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 82
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 84
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

How does steganography work?

Steganography works by hiding information in a way that doesn't arouse suspicion. One of the most popular techniques is 'least significant bit (LSB) steganography. In this type of steganography, the information hider embeds the secret information in the least significant bits of a media file.

For instance, in an image file each pixel is comprised of three bytes of data corresponding to the colors red, green, and blue (some image formats allocate an additional fourth byte to transparency, or 'alpha').

LSB steganography changes the last bit of each of those bytes to hide one bit of data. So, to hide one megabyte of data using this method, you'll need an eight-megabyte image file.

Since modifying the last bit of the pixel value doesn't result in a visually perceptible change to the picture, a person viewing the original and the steganographically modified images won't be able to tell the difference.

NEW QUESTION 89
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:

* Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege
* SSL Medium Strength Cipher Suites Supported
* Vulnerability in DNS Resolution Could Allow Remote Code Execution
* SMB Host SIDs allows Local User Enumeration

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 91
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 96
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. Pass solution in a multinency cloud
C. SaaS solution in a community cloud
D. Private SaaS solution in a single tenancy cloud.

Answer: D

NEW QUESTION 100
An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue.
However, when the application is released to the public, report come In that a previously vulnerability has returned .
Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

A. Peer review
B. Regression testing
C. User acceptance
D. Dynamic analysis

Answer: A

NEW QUESTION 103
A developer implement the following code snippet.

```
catch (Exception e)
{
    if(log.isDebugEnabled())
    {
        log.debug("Caught InvalidSSNException Exception --"
        + e.toString());
    }
}
```

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 108
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.

```
Test email sent from bp_app01 to external client_app01_mailing_list.
```

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 112
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 115
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 116
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 118
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 120
......

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/