Try Free and Start Using Realistic Verified CAS-004 Dumps Instantly [Q200-Q221

Try Free and Start Using Realistic Verified CAS-004 Dumps Instantly CAS-004 Actual Questions - Instant Download 440 Questions

CompTIA CASP+ certification exam is vendor-neutral, which means it is not tied to any specific software, hardware, or technology. This impartiality ensures that the skills and knowledge tested in the exam are transferable across different organizations and industry sectors. CompTIA Advanced Security Practitioner (CASP+) Exam certification exam is recognized globally, making it an excellent choice for IT security professionals who want to expand their career opportunities and work in different regions.

NEW QUESTION 200

An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:

– Be based on open-source Android for user familiarity and ease.

– Provide a single application for inventory management of physical

assets.

– Permit use of the camera be only the inventory application for the

purposes of scanning

– Disallow any and all configuration baseline modifications.

– restrict all access to any device resource other than those required

for use of the inventory management application

Which of the following approaches would best meet these security requirements?
* Set an application wrapping policy, wrap the application, distributes the inventory APK via the MAM tool, and test the application restrictions.
* Write a MAC sepolicy that defines domains with rules, label the inventory application, build the policy, and set to enforcing mode.
* Swap out Android Linux kernel version for >2,4,0, but the internet build Android, remove unnecessary functions via MDL, configure to block network access, and perform integration testing
* Build and install an Android middleware policy with requirements added, copy the file into/ user/init, and then built the inventory application.

NEW QUESTION 201

An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.

Which of the following historian server locations will allow the business to get the required reports in anOTand IT environment?
* In theOTenvironment, use a VPN from the IT environment into theOTenvironment.
* In theOTenvironment, allow IT traffic into theOTenvironment.
* In the IT environment, allow PLCs to send data from theOTenvironment to the IT environment.
* Use a screened subnet between theOTand IT environments.

A screened subnet is a network segment that separates two different environments, such asOT(operational technology) and IT (information technology), and provides security controls to limit and monitor the traffic between them. This would allow the business to get the required reports from the historian server without exposing theOTenvironment to unnecessary risks. Using a VPN, allowing IT traffic, or allowing PLCs to send data are less secure options that could compromise theOTenvironment. Verified Reference: https://www.comptia.org/blog/what-is-operational-technology
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 202

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 vulnerability
* A threat
* A breach
* A risk

A vulnerability refers to a weakness in your system while the risk is related to the potential for lost, damaged, or destroyed assets.

NEW QUESTION 203

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?
* Detection
* Remediation
* Preparation
* Recovery

NEW QUESTION 204

A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away.

Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?
* Scan the code with a static code analyzer, change privileged user passwords, and provide security training.
* Change privileged usernames, review the OS logs, and deploy hardware tokens.
* Implement MFA, review the application logs, and deploy a WAF.
* Deploy a VPN, configure an official open-source library repository, and perform a full application review for vulnerabilities.
Specifying a repository serves no purpose. You already know the library has a vulnerability. You need something which mitigates the unauthorized access, which MFA does, and a properly configured WAF would also provide protection.

NEW QUESTION 205

A security analyst is validating the MAC policy on a set of Android devices. The policy was written to ensure non-critical applications are unable to access certain resources. When reviewing dmesg, the analyst notes many entries such as:

Despite the deny message, this action was still permit following is the MOST likely fix for this issue?
* Add the objects of concern to the default context.
* Set the devices to enforcing
* Create separate domain and context files for irc.
* Rebuild the policy, reinstall, and test.

NEW QUESTION 206

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?
* NIDS
* NIPS
* WAF
* Reverse proxy

NEW QUESTION 207

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  30400  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?
* 65
* 77
* 83
* 87
These are percentages of total CPU time.

us: Time spent running non-kernel code. (user time, including nice time) sy: Time spent running kernel code. (system time) id: Time spent idle. Prior to Linux 2.5.41, this includes IO-wait time.

wa: Time spent waiting for IO. Prior to Linux 2.5.41, included in idle.

st: Time stolen from a virtual machine. Prior to Linux 2.6.11, unknown.

NEW QUESTION 208

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?
* SDLC
* OVAL
* IEEE
* OWASP
Explanation

OWASP is a resource used to identify attack vectors and their mitigations, OVAL is a vulnerability assessment standard OWASP (Open Web Application Security Project) is a source that the security architect could consult to address the security concern of XSS (cross-site scripting) attacks on a web application that uses a database back end. OWASP is a non-profit organization that provides resources and guidance for improving the security of web applications and services. OWASP publishes the OWASP Top 10 list of common web application vulnerabilities and risks, which includes XSS attacks, as well as recommendations and best practices for preventing or mitigating them. SDLC (software development life cycle) is not a source for addressing XSS attacks, but a framework for developing software in an organized and efficient manner.

OVAL (Open Vulnerability and Assessment Language) is not a source for addressing XSS attacks, but a standard for expressing system configuration information and vulnerabilities. IEEE (Institute of Electrical and Electronics Engineers) is not a source for addressing XSS attacks, but an organization that develops standards for various fields of engineering and technology. Verified

References:

https://www.comptia.org/blog/what-is-owasp

https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 209

A client is adding scope to a project. Which of the following processes should be used when requesting updates or corrections to the client’s systems?
* The implementation engineer requests direct approval from the systems engineer and the Chief Information Security Officer.
* The change control board must review and approve a submission.
* The information system security officer provides the systems engineer with the system updates.
* The security engineer asks the project manager to review the updates for the client’s system.

Explanation

The change control board (CCB) is a committee that consists of subject matter experts and managers who decide whether to implement proposed changes to a project. The change control board is part of the change management plan, which defines the roles and processes for managing change within a team or organization.

The change control board must review and approve a submission for any change request that affects the scope, schedule, budget, quality, or risks of the project. The change control board evaluates the impact and benefits of the change request and decides whether to accept, reject, or defer it.

A) The implementation engineer requesting direct approval from the systems engineer and the Chief Information Security Officer is not a correct process for requesting updates or corrections to the client’s systems, because it bypasses the change control board and the project manager. This could lead to unauthorized changes that could compromise the project’s objectives and deliverables.

C) The information system security officer providing the systems engineer with the system updates is not a correct process for requesting updates or corrections to the client’s systems, because it does not involve the change control board or the project manager. This could lead to unauthorized changes that could introduce security vulnerabilities or conflicts with other system components.

D) The security engineer asking the project manager to review the updates for the client’s system is not a correct process for requesting updates or corrections to the client’s systems, because it does not involve the change control board. The project manager is responsible for facilitating the change management process, but not for approving or rejecting change requests.

https://www.projectmanager.com/blog/change-control-board-roles-responsibilities-processes

NEW QUESTION 210

A security engineer needs to select the architecture for a cloud database that will protect an organization’s sensitive dat a. The engineer has a choice between a single-tenant or a multitenant database architecture offered by a cloud vendor. Which of the following best describes the security benefits of the single-tenant option? (Select two).
* Most cost-effective
* Ease of backup and restoration
* High degree of privacy
* Low resilience to side-channel attacks
* Full control and ability to customize

* Increased geographic diversity

Single-tenant architectures provide a dedicated environment for each client, which enhances data privacy since the resources are not shared with other tenants. This isolation minimizes the risk of data leakage or interference from other tenants, offering a high degree of privacy. Additionally, single-tenancy allows for full control over the database environment, including customization options tailored to specific security requirements or compliance needs, which is not always possible in a multi-tenant architecture.

NEW QUESTION 211

A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.

Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

* The company will have access to the latest version to continue development.
* The company will be able to force the third-party developer to continue support.
* The company will be able to manage the third-party developer’s development process.
* The company will be paid by the third-party developer to hire a new development team.

NEW QUESTION 212

A security manager wants to transition the organization to a zero trust architecture. To meet this requirement, the security manager has instructed administrators to remove trusted zones, role-based access, and one-time authentication. Which of the following will need to be implemented to achieve this objective? (Select THREE).

* Least privilege
* VPN
* Policy automation
* PKI
* Firewall
* Continuous validation
* Continuous integration
* laas

Least privilege, policy automation, and continuous validation are some of the key elements that need to be implemented to achieve the objective of transitioning to a zero trust architecture. Zero trust architecture is a security model that assumes no implicit trust for any entity or resource, regardless of their location or ownership. Zero trust architecture requires verifying every request and transaction before granting access or allowing data transfer. Zero trust architecture also requires minimizing the attack surface and reducing the risk of lateral movement by attackers.

A) Least privilege is a principle that states that every entity or resource should only have the minimum level of access or permissions necessary to perform its function. Least privilege can help enforce granular and dynamic policies that limit the exposure and impact of potential breaches. Least privilege can also help prevent privilege escalation and abuse by malicious insiders or compromised accounts.

C) Policy automation is a process that enables the creation, enforcement, and management of security policies using automated tools and workflows. Policy automation can help simplify and streamline the implementation of zero trust architecture by reducing human errors, inconsistencies, and delays. Policy automation can also help adapt to changing conditions and requirements by updating and applying policies in real time.

F) Continuous validation is a process that involves verifying the identity, context, and risk level of every request and transaction throughout its lifecycle. Continuous validation can help ensure that only authorized and legitimate requests and transactions are allowed to access or transfer data. Continuous validation can also help detect and respond to anomalies or threats by revoking access

or terminating sessions if the risk level changes.

B) VPN is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. VPN stands for Virtual Private Network, which is a technology that creates a secure tunnel between a device and a network over the internet. VPN can provide confidentiality, integrity, and authentication for network communications, but it does not provide zero trust security by itself. VPN still relies on network-based perimeters and does not verify every request or transaction at a granular level.

D) PKI is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. PKI stands for Public Key Infrastructure, which is a system that manages the creation, distribution, and verification of certificates. Certificates are digital documents that contain public keys and identity information of their owners. Certificates can be used to prove the identity and authenticity of the certificate holders, as well as to encrypt and sign data. PKI can provide encryption and authentication for data communications, but it does not provide zero trust security by itself. PKI still relies on trusted authorities and does not verify every request or transaction at a granular level.

E) Firewall is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. Firewall is a device or software that monitors and controls incoming and outgoing network traffic based on predefined rules. Firewall can provide protection against unauthorized or malicious network access, but it does not provide zero trust security by itself. Firewall still relies on network-based perimeters and does not verify every request or transaction at a granular level.

G) Continuous integration is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. Continuous integration is a software development practice that involves merging code changes from multiple developers into a shared repository frequently and automatically. Continuous integration can help improve the quality, reliability, and performance of software products, but it does not provide zero trust security by itself. Continuous integration still relies on code-based quality assurance and does not verify every request or transaction at a granular level.

H) IaaS is not an element that needs to be implemented to achieve the objective of transitioning to a zero trust architecture. IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources over the internet. IaaS can provide scalability, flexibility, and cost-efficiency for IT infrastructure, but it does not provide zero trust security by itself. IaaS still relies on cloud-based security controls and does not verify every request or transaction at a granular level.

NEW QUESTION 213

Which of the following BEST sets expectation between the security team and business units within an organization?
* Risk assessment
* Memorandum of understanding
* Business impact analysis
* Business partnership agreement
* Services level agreement

Explanation

A service level agreement (SLA) is the best option to set expectations between the security team and business units within an organization. An SLA is a document that defines the scope, quality, roles, responsibilities, and metrics of a service provided by one party to another. An SLA can help align the security team’s objectives and activities with the business units’ needs and expectations, as well as establish accountability and communication channels. Verified References:

https://www.comptia.org/training/books/casp-cas-004-study-guide ,

https://searchitchannel.techtarget.com/definition/service-level-agreement

NEW QUESTION 214

An executive has decided to move a company’s customer-facing application to the cloud after experiencing a lengthy power outage at a locally managed service provider’s data center. The executive would like a solution that can be implemented as soon as possible. Which of the following will BEST prevent similar issues when the service is running in the cloud? (Choose two.)
* Placing the application instances in different availability zones
* Restoring the snapshot and starting the new application instance from a different zone
* Enabling autoscaling based on application instance usage
* Having several application instances running in different VPCs
* Using the combination of block storage and multiple CDNs in each application instance
* Setting up application instances in multiple regions

NEW QUESTION 215

A forensics investigator is analyzing an executable file extracted from storage media that was submitted (or evidence The investigator must use a tool that can identify whether the executable has indicators, which may point to the creator of the file Which of the following should the investigator use while preserving evidence integrity?
* idd
* bcrypt
* SHA-3
* ssdeep
* dcfldd

ssdeep is a tool that computes and matches Context Triggered Piecewise Hashing (CTPH), also known as fuzzy hashing. It can be used to identify similar files or slight variations of the same file, which may point to the creator of the file if certain patterns or markers are consistently present. This method allows for integrity checking without altering the evidence, which is critical in forensic investigation.

NEW QUESTION 216

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?
* Protecting
* Permissive
* Enforcing
* Mandatory

NEW QUESTION 217

A company makes consumer health devices and needs to maintain strict confidentiality of unreleased product designs.

Recently unauthorized photos of products still in development have been for sale on the dark web.

The Chief Information Security Officer (CISO) suspects an insider threat, but the team that uses the secret outdoor testing area has been vetted many times and nothing suspicious has been found.

Which of the following is the MOST likely cause of the unauthorized photos?
* The location of the testing facility was discovered by analyzing fitness device information the test engineers posted on a website

* One of the test engineers is working for a competitor and covertly installed a RAT on the marketing department’s servers
* The company failed to implement least privilege on network devices, and a hacktivist published stolen public relations photos
* Pre-release marketing materials for a single device were accidentally left in a public location

NEW QUESTION 218

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?
* Distributed connection allocation
* Local caching
* Content delivery network
* SD-WAN vertical heterogeneity

A CDN is a network of servers that are distributed across the Internet and are designed to deliver content to users more efficiently. CDNs work by storing copies of content on servers that are located closer to the users who are requesting it, which can help to reduce latency and improve performance.

NEW QUESTION 219

A security engineer was auditing an organization’s current software development practice and discovered that multiple open-source 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?
* Perform additional SAST/DAST on the open-source libraries.
* Implement the SDLC security guidelines.
* Track the library versions and monitor the CVE website for related vulnerabilities.
* Perform unit testing of the open-source libraries.

It is important to keep track of the versions of open-source libraries that are being used, and to monitor the CVE website for any vulnerabilities that have been identified in those libraries. This can help the organization stay aware of potential security issues and take appropriate action to address them.

Performing unit testing of the open-source libraries is not necessary, as unit testing is typically focused on testing individual units of code within the software, not on external libraries that are being used.

NEW QUESTION 220

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?
* Spawn a shell using sudo and an escape string such as sudo vim -c ‘!sh’.
* Perform ASIC password cracking on the host.
* Read the /etc/passwd file to extract the usernames.
* Initiate unquoted service path exploits.
* Use the UNION operator to extract the database schema.

Reference:

Spawning a shell using sudo and an escape string is a valid Linux post-exploitation method that can exploit a misconfigured sudoers file and allow a standard user to execute commands as root. ASIC password cracking is used to break hashed passwords, not to elevate privileges. Reading the /etc/passwd file may reveal usernames, but not passwords or privileges. Unquoted service path exploits are applicable to Windows systems, not Linux. Using the UNION operator is a SQL injection technique, not a Linux post-exploitation method. Verified Reference: https://www.comptia.org/blog/what-is-post-exploitation https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 221

A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication.

Which of the following technologies would BEST meet this need?
* Faraday cage
* WPA2 PSK
* WPA3 SAE
* WEP 128 bit

WPA3 SAE prevents brute-force attacks.

“WPA3 Personal (WPA-3 SAE) Mode is a static passphrase-based method. It provides better security than what WPA2 previously provided, even when a non-complex password is used, thanks to Simultaneous Authentication of Equals (SAE), the personal authentication process of WPA3.”