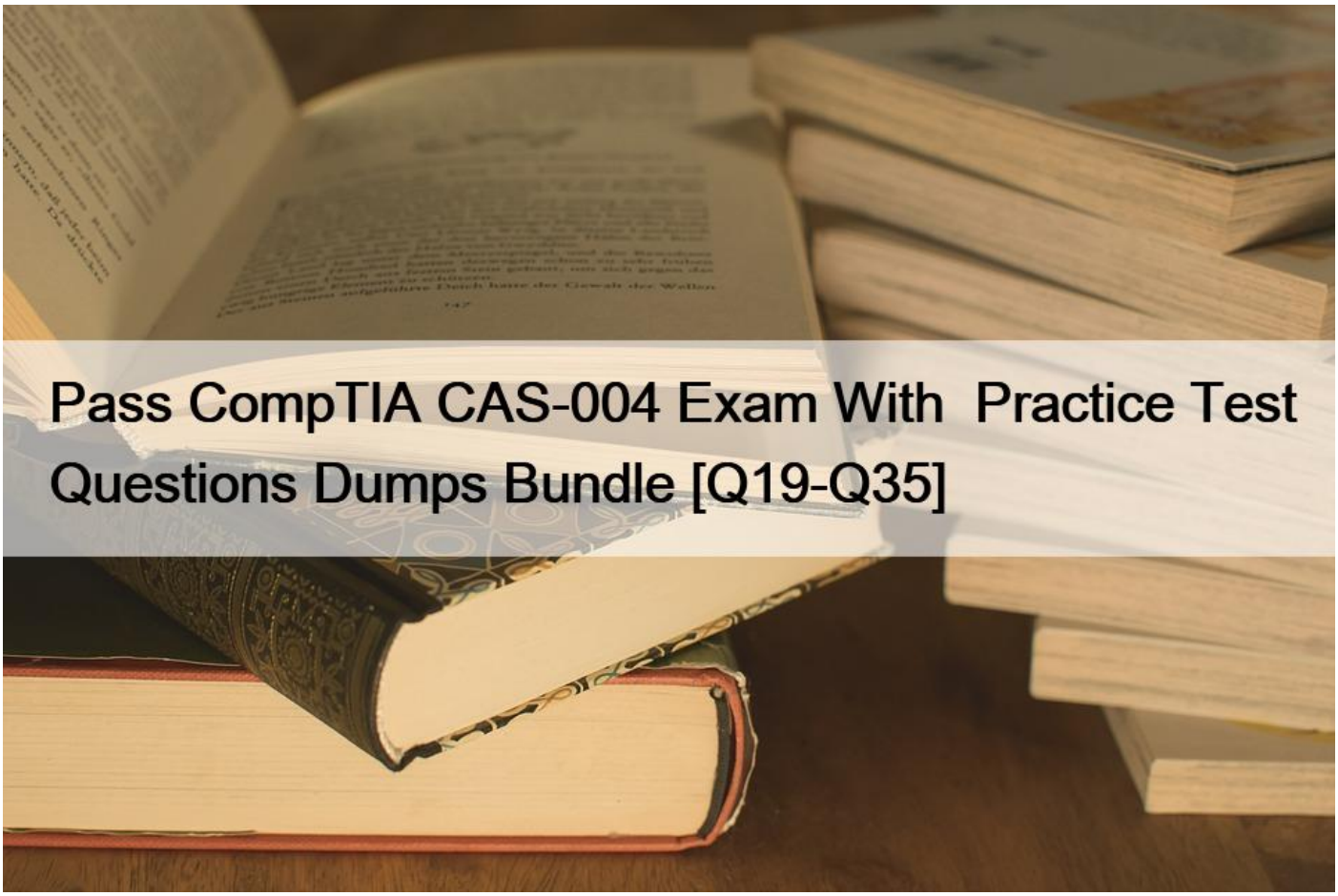
Pass CompTIA CAS-004 Exam With Practice Test Questions Dumps Bundle [Q19-Q35



Pass CompTIA CAS-004 Exam With Practice Test Questions Dumps Bundle
2022 Valid CAS-004 test answers & CompTIA Exam PDF

NO.19 A company is preparing to deploy a global service.

Which of the following must the company do to ensure GDPR compliance? (Choose two.)
* Inform users regarding what data is stored.
* Provide opt-in/out for marketing messages.
* Provide data deletion capabilities.
* Provide optional data encryption.
* Grant data access to third parties.
* Provide alternative authentication techniques.

The main rights for individuals under the GDPR are to:

allow subject access

have inaccuracies corrected

have information erased

prevent direct marketing

prevent automated decision-making and profiling

allow data portability (as per the paragraph above)

source: https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/

NO.20 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 hard-coded string in the request string?
* Implement a VPN for all APIs.
* Sign the key with DSA.
* Deploy MFA for the service accounts.
* Utilize HMAC for the keys.

NO.21 A security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources.

Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?
* Union filesystem overlay
* Cgroups
* Linux namespaces
* Device mapper

NO.22 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.

NO.23 A company provides guest WiFi access to the internet and physically separates the guest network from the company’s internal WIFI. Due to a recent incident in which an attacker gained access to the compay’s intend WIFI, the company plans to configure WPA2 Enterprise in an EAP- TLS configuration. Which of the following must be installed on authorized hosts for this new configuration to work properly?
* Active Directory OPOs
* PKI certificates
* Host-based firewall
* NAC persistent agent

NO.24 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

NO.25 Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure. Which of the must occur to ensure the integrity of the image?
* The image must be password protected against changes.
* A hash value of the image must be computed.
* The disk containing the image must be placed in a seated container.
* A duplicate copy of the image must be maintained

NO.26 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?
* Data loss detection, reverse proxy, EDR, and PGP
* VDI, proxy, CASB, and DRM
* Watermarking, forward proxy, DLP, and MFA
* Proxy, secure VPN, endpoint encryption, and AV

NO.27 A company is preparing to deploy a global service.

Which of the following must the company do to ensure GDPR compliance? (Choose two.)
* Inform users regarding what data is stored.
* Provide opt-in/out for marketing messages.
* Provide data deletion capabilities.
* Provide optional data encryption.
* Grant data access to third parties.
* Provide alternative authentication techniques.

NO.28 An organization developed a social media application that is used by customers in multiple remote geographic locations around the world. The organization’s headquarters and only datacenter are located in New York City. The Chief Information Security Officer wants to ensure the following requirements are met for the social media application:

Low latency for all mobile users to improve the users’ experience

SSL offloading to improve web server performance

Protection against DoS and DDoS attacks

High availability

Which of the following should the organization implement to BEST ensure all requirements are met?
* A cache server farm in its datacenter
* A load-balanced group of reverse proxy servers with SSL acceleration
* A CDN with the origin set to its datacenter
* Dual gigabit-speed Internet connections with managed DDoS prevention

NO.29 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?
* Investigating a potential threat identified in logs related to the identity management system
* Updating the identity management system to use discretionary access control
* Beginning research on two-factor authentication to later introduce into the identity management system
* Working with procurement and creating a requirements document to select a new IAM system/vendor

NO.30 Company A acquired Company B.

During an audit, a security engineer found Company B’s environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B’s infrastructure could be integrated into Company A’s security program.

Which of the following risk-handling techniques was used?
* Accept
* Avoid
* Transfer
* Mitigate

NO.31 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.

NO.32 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

NO.33 A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.

Which of the following techniques would BEST support this?
* Configuring systemd services to run automatically at startup
* Creating a backdoor
* Exploiting an arbitrary code execution exploit
* Moving laterally to a more authoritative server/service

NO.34 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?
* The client application is testing PFS.
* The client application is configured to use ECDHE.
* The client application is configured to use RC4.
* The client application is configured to use AES-256 in GCM.

NO.35 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