CAS-004Q&As

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers

QUESTION 1

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?

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.

Correct Answer: D

Reference: https://eclipsesource.com/blogs/2016/07/06/keyed-hash-message-authentication-code-in-rest-apis/

QUESTION 2

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.

Correct Answer: C

Reference: https://docs.rapid7.com/insightvm/elevating-permissions/

QUESTION 3

A penetration tester is on an active engagement and has access to a remote system. The penetration tester wants to bypass the DLP, which is blocking emails that are encrypted or contain sensitive company information. Which of the following cryptographic techniques should the penetration tester use?

A. GNU Privacy Guard

B. UUencoding

C. DNSCrypt

D. Steganography

Correct Answer: D

QUESTION 4

A security compliance requirement states that specific environments that handle sensitive data must be protected by need-to-know restrictions and can only connect to authorized endpoints. The requirement also states that a DLP solution within the environment must be used to control the data from leaving the environment.

Which of the following should be implemented for privileged users so they can support the environment from their workstations while remaining compliant?

A. NAC to control authorized endpoints

B. FIM on the servers storing the data

C. A jump box in the screened subnet

D. A general VPN solution to the primary network

Correct Answer: D

QUESTION 5

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

Correct Answer: A

Reference: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

QUESTION 6

A security engineer is hardening a company\\'s multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:

1.

22

2.

25

3.

110

4.

137

5.

138

6.

139

7.

445

Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company\\'s distribution process.

Which of the following would be the BEST solution to harden the system?

A. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.

B. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.

C. Close ports 22 and 139. Bind ports 137, 138, and 445 to only the internal interface.

D. Close ports 22, 137, and 138. Bind ports 110 and 445 to only the internal interface.

Correct Answer: A

QUESTION 7

A small company is implementing a new technology that promises greater performance but does not abide by accepted RFCs.

Which of the following should the company do to ensure the risks associated with implementing the standard-violating technology are addressed?

A. Document the technology\\'s differences in a system security plan.

B. Require the vendor to provide justification for the product\\'s deviation.

C. Increase the frequency of vulnerability scanning of all systems using the technology.

D. Block the use of non-standard ports or protocols to and from the system.

Correct Answer: A

Reference: https://www.sciencedirect.com/toDics/computer-science/svstem-securitv-plan

QUESTION 8

A corporation with a BYOD policy is very concerned about issues that may arise from data ownership. The corporation is investigating a new MDM solution and has gathered the following requirements as part of the requirements-gathering phase.

1.

Each device must be issued a secure token of trust from the corporate PKI.

2.

All corporate application and local data must be able to deleted from a central console.

3.

Cloud storage and backup applications must be restricted from the device.

4.

Devices must be on the latest OS version within three weeks of an OS release.

Which of the following should be feature in the new MDM solution to meet these requirement? (Select TWO.)

A. Application-based containerization

B. Enforced full-device encryption

C. Mandatory acceptance of SCEP system

D. Side-loaded application prevention

E. Biometric requirement to unlock device

F. Over-the-air restriction

Correct Answer: A

QUESTION 9

A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:

1.

Be efficient at protecting the production environment

2.

Not require any change to the application

3.

Act at the presentation layer

Which of the following techniques should be used?

A. Masking

B. Tokenization

C. Algorithmic

D. Random substitution

Correct Answer: A

QUESTION 11

Technicians have determined that the current server hardware is outdated, so they have decided to throw it out. Prior to disposal, which of the following is the BEST method to use to ensure no data remnants can be recovered?

A. Drive wiping

B. Degaussing

C. Purging

D. Physical destruction

Correct Answer: B

Reference: https://securis.com/data-destruction/degaussing-as-a-service/

QUESTION 12

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.

Correct Answer: C

QUESTION 14

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.

Correct Answer: BD

QUESTION 15

A security manager wants to standardize security settings, firmware, and software across a heterogeneous environment. Which of the following can be used in combination to meet these goals? (Choose three).

A. Attestation services

B. TPM

C. HIPS software

D. OOB management software

E. Group Policy

F. EDR software

G. MDM software

Correct Answer: BEF