CAS-005$^{Q\&As}$

CompTIA SecurityX Exam

Pass CompTIA CAS-005 Exam with 100% Guarantee

QUESTION 1

A company is having issues with its vulnerability management program New devices/IPs are added and dropped regularly, making the vulnerability report inconsistent

Which of the following actions should the company lake to most likely improve the vulnerability management process\\'

A. Request a weekly report with all new assets deployed and decommissioned

B. Extend the DHCP lease lime to allow the devices to remain with the same address for a longer period.

C. Implement a shadow IT detection process to avoid rogue devices on the network

D. Perform regular discovery scanning throughout the 11 landscape using the vulnerability management tool

Correct Answer: D

To improve the vulnerability management process in an environment where new devices/IPs are added and dropped regularly, the company should perform regular discovery scanning throughout the IT landscape using the vulnerability

management tool.

Here\\'s why:

Accurate Asset Inventory: Regular discovery scans help maintain an up-to-date inventory of all assets, ensuring that the vulnerability management process includes all relevant devices and IPs. Consistency in Reporting: By continuously

discovering and scanning new and existing assets, the company can generate consistent and comprehensive vulnerability reports that reflect the current state of the network. Proactive Management:

Regular scans enable the organization to proactively identify and address vulnerabilities on new and existing assets, reducing the window of exposure to potential threats.

QUESTION 2

A security analyst is reviewing suspicious emails that were forwarded by users. Which of the following is the best method for the analyst to use when reviewing attachments that came with these emails?

A. Reverse engineering

B. Protocol analysis

C. Sandboxing

D. Fuzz testing

E. Steganography

Correct Answer: C

The most effective method for a security analyst to review suspicious email attachments is to use sandboxing. This approach allows the attachments to be executed in a safe, isolated environment, making it possible to observe any malicious activities without risking the integrity of the actual systems. Sandboxing offers a comprehensive and efficient way to analyze potentially harmful content in email attachments.

QUESTION 3

An application engineer is using the Swagger framework to leverage REST APIs to authenticate endpoints. The engineer is receiving HTTP 403 responses. Which of the following should the engineer do to correct this issue? (Choose two.)

A. Obtain a security token.

B. Obtain a public key.

C. Leverage Kerberos for authentication

D. Leverage OAuth for authentication.

E. Leverage LDAP for authentication.

F. Obtain a hash value.

Correct Answer: AD

Obtain a security token: HTTP 403 responses typically indicate that the request is authenticated but the user does not have the necessary permissions to access the endpoint. Obtaining a security token is a common method for authenticating

requests. This token is usually required by the API to verify that the requestor has the proper access rights.

Leverage OAuth for authentication: OAuth is a widely used authentication framework that allows an application to obtain limited access to user accounts on an HTTP service. It is commonly used for token- based authentication, and

leveraging OAuth would help in obtaining the necessary tokens and permissions to access the API endpoints.

QUESTION 4

A security technician is trying to connect a remote site to the central office over a site-to-site VPN. The technician has verified the source and destination IP addresses are correct, but the technician is unable to get the remote site to connect. The following error message keeps repeating:

An error has occurred during Phase 1 handshake. Deleting keys and retrying...

Which of the following is most likely the reason the connection is failing?

A. The IKE hashing algorithm uses different key lengths on each VPN device.

B. The IPSec settings allow more than one cipher suite on both devices.

C. The Diffie-Hellman group on both sides matches but is a legacy group.

D. The remote VPN is attempting to connect with a protocol other than SSL/TLS.

Correct Answer: C

The error message "An error has occurred during Phase 1 handshake. Deleting keys and retrying..." suggests that there is an issue with the initial negotiation or key exchange process. Legacy Diffie-Hellman groups are a common cause of such issues because modern VPN devices might reject or fail to negotiate with older, less secure groups.

QUESTION 5

Which of the following security features do email signatures provide?

A. Non-repudiation

B. Body encryption

C. Code signing

D. Sender authentication

E. Chain of custody

Correct Answer: AD