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

CompTIA SecurityX Exam

QUESTION 1

Which of the following is the main reason quantum computing advancements are leading companies and countries to deploy new encryption algorithms?

A. Encryption systems based on large prime numbers will be vulnerable to exploitation

B. Zero Trust security architectures will require homomorphic encryption.

C. Perfect forward secrecy will prevent deployment of advanced firewall monitoring techniques

D. Quantum computers will enable malicious actors to capture IP traffic in real time

Correct Answer: A

Advancements in quantum computing pose a significant threat to current encryption systems, especially those based on the difficulty of factoring large prime numbers, such as RSA. Quantum computers have the potential to solve these

problems exponentially faster than classical computers, making current cryptographic systems vulnerable.

Why Large Prime Numbers are Vulnerable:

Shor\\'s Algorithm: Quantum computers can use Shor\\'s algorithm to factorize large integers efficiently, which undermines the security of RSA encryption. Cryptographic Breakthrough: The ability to quickly factor large prime numbers means that

encrypted data, which relies on the hardness of this mathematical problem, can be decrypted.

Other options, while relevant, do not capture the primary reason for the shift towards new encryption algorithms:

B. Zero Trust security architectures: While important, the shift to homomorphic encryption is not the main driver for new encryption algorithms. C. Perfect forward secrecy: It enhances security but is not the main reason for new encryption

algorithms.

D. Real-time IP traffic capture: Quantum computers pose a more significant threat to the underlying cryptographic algorithms than to the real-time capture of traffic.

References:

CompTIA SecurityX Study Guide

NIST Special Publication 800-208, "Recommendation for Stateful Hash-Based Signature Schemes"

"Quantum Computing and Cryptography," MIT Technology Review

QUESTION 2

A company is rewriting a vulnerable application and adding the mprotect() system call in multiple parts of the application\\'s code that was being leveraged by a recent exploitation tool. Which of the following should be enabled to ensure the application can leverage the new system call against similar attacks in the future?

A. TPM

B. Secure boot

C. NX bit

D. HSM

Correct Answer: C

Enabling the NX bit ensures that the rewritten application can effectively use the mprotect() system call to manage memory execution permissions, thereby strengthening its defenses against exploitation tools that attempt to execute code from unauthorized memory regions. This approach aligns with best practices in modern application security to mitigate memory-based vulnerabilities

QUESTION 3

A security researcher identified the following messages while testing a web application:

/file/admin/myprofile.php ERROR file does not exist.

/file/admin/userinfo.php ERROR file does not exist.

/file/admin/adminprofile.php ERROR file does not exist.

/file/admin/admininfo.php ERROR file does not exist.

/file/admin/universalprofile.php ERROR file does not exist. /file/admin/universalinfo.php ERROR file does not exist.

/file/admin/restrictedprofile.php ACCESS is denied.

/file/admin/restrictedinfo.php ERROR file does not exist.

Which of the following should the researcher recommend to remediate the issue?

A. Software composition analysis

B. Packet inspection

C. Proper error handling

D. Elimination of the use of unsafe functions

Correct Answer: C

The messages provide information about the existence and access permissions of certain files, which can be useful to an attacker. Proper error handling involves:

Ensuring that error messages do not reveal sensitive information about the server or its structure. Customizing error messages to be generic and user-friendly without disclosing specifics about the error (e.g., "An error occurred" instead of "ERROR file does not exist" or "ACCESS is denied"). Logging detailed error information on the server-side for debugging purposes without exposing it to the end user.

QUESTION 4

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 5

Asecuntv administrator is performing a gap assessment against a specific OS benchmark The benchmark requires the following configurations be applied to endpomts:

1.

Full disk encryption

2.

Host-based firewall

3.

Time synchronization

4.

Password policies

5.

Application allow listing

6.

Zero Trust application access

Which of the following solutions best addresses the requirements? (Select two).

A. CASB

B. SBoM

C. SCAP

D. SASE

E. HIDS

Correct Answer: CD

To address the specific OS benchmark configurations, the following solutions are most appropriate:

C. SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies. D. SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data. These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.

References:

CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures. NIST Special Publication 800-126, "The Technical Specification for the Security Content Automation

Protocol (SCAP)": Details SCAP\\'s role in security automation. "Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth: Covers the principles of Zero Trust and how SASE can implement them.

By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintained effectively.