Vendor:ISC

Exam Code:CISSP

Exam Name: Certified Information Systems Security Professional

Version: Demo

QUESTION 1

Which of the following BEST provides for non-repudiation od user account actions?

A. Centralized authentication system

B. File auditing system

C. Managed Intrusion Detection System (IDS) D. Centralized logging system

Correct Answer: D

QUESTION 2

Refer to the information below to answer the question.

A large, multinational organization has decided to outsource a portion of their Information Technology (IT) organization to a third-party provider\\'s facility. This provider will be responsible for the design, development, testing, and support of several critical, customer-based applications used by the organization.

The organization should ensure that the third party\\'s physical security controls are in place so that they A. are more rigorous than the original controls.

B. are able to limit access to sensitive information.

C. allow access by the organization staff at any time.

D. cannot be accessed by subcontractors of the third party.

Correct Answer: B

QUESTION 3

An organization plan on purchasing a custom software product developed by a small vendor to support its business model.

Which unique consideration should be made part of the contractual agreement potential long-term risks associated with creating this dependency?

A. A source code escrow clause

B. Right to request an independent review of the software source code

C. Due diligence form requesting statements of compliance with security requirements

D. Access to the technical documentation

Correct Answer: B

QUESTION 4

What is an advantage of Elliptic Curve Cryptography (ECC)?

A. Cryptographic approach that does not require a fixed-length key

B. Military-strength security that does not depend upon secrecy of the algorithm

C. Opportunity to use shorter keys for the same level of security

D. Ability to use much longer keys for greater security

Correct Answer: C

QUESTION 5

A new employee formally reported suspicious behavior to the organization security team. The report claims that someone not affiliated with the organization was inquiring about the member\\'s work location, length of employment, and building access controls. The employee\\'s reporting is MOST likely the result of which of the following?

A. Risk avoidance

B. Security engineering

C. security awareness

D. Phishing

Correct Answer: C

QUESTION 6

Which of the following techniques BEST prevents buffer overflows?

A. Boundary and perimeter offset

B. Character set encoding

C. Code auditing

D. Variant type and bit length

Correct Answer: B

Some products installed on systems can also watch for input values that might result in buffer overflows, but the best countermeasure is proper programming. This means use bounds checking. If an input value is only sup-posed to be nine characters, then the application should only accept nine characters and no more. Some languages are more susceptible to buffer overflows than others, so programmers should understand these issues, use the right languages for the right purposes, and carry out code review to identify buffer overflow vulnerabilities.

QUESTION 7

How does identity as a service (IDaaS) provide an easy mechanism for integrating identity service into individual applications with minimal development effort?

A. By allowing the identification logic and storage of an identity\\'s attributes to be maintained externally

B. By integrating internal provisioning procedures with external authentication processes

C. By allowing for internal provisioning of user accounts

D. By keeping all user information in easily accessible cloud repositories

Correct Answer: D

QUESTION 8

A system developer has a requirement for an application to check for a secure digital signature before the application is accessed on a user\\'s laptop. Which security mechanism addresses this requirement?

A. Hardware encryption

B. Certificate revocation list (CRL) policy

C. Trusted Platform Module (TPM)

D. Key exchange

Correct Answer: B

QUESTION 9

Which of the following is the MOST important activity an organization performs to ensure that security is part of the overall organization culture?

A. Perform formal reviews of security incidents.

B. Work with senior management to meet business goals.

C. Ensure security policies are issued to all employees.

D. Manage a program of security audits.

Correct Answer: A

Reference: https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom

---

QUESTION 10

When performing an investigation with the potential for legal action, what should be the analyst\\'s FIRST consideration?

A. Chain-of-custody

B. Authorization to collect

C. Court admissibility

D. Data decryption

Correct Answer: A

QUESTION 11

Which testing method requires very limited or no information about the network infrastructure?

A. White box

B. Static

C. Black box

D. Stress

Correct Answer: C

QUESTION 12

Which of the following is a security weakness in the evaluation of Common Criteria (CC) products?

A. The manufacturer can state what configuration of the product is to be evaluated

B. The product can be evaluated by labs in other countries

C. The Target of Evaluation\\'s (TOE) testing environment is identical to the operating environment

D. The evaluations are expensive and time-consuming to perform

Correct Answer: A