D.   Trustworthy procedures.

Correct Answer: C

QUESTION 1546

Which choice would be an example of a cost-effective way to enhance security awareness in an organization?

A.   Train only managers in implementing InfoSec controls.
B.   Calculate the cost-benefit ratio of the asset valuations for a risk analysis.
C.   Train every employee in advanced InfoSec.
D.   Create an award or recognition program for employees.

Correct Answer: D

QUESTION 1547

In a relational database, security is provided to the access of data through:

A.   Candidate keys
B.   Views
C.   Joins
D.   Attributes

Correct Answer: B

QUESTION 1548

The Open Group has defined functional objectives in support of a user single sign-on (SSO) interface. Which of the following is NOT one of those objectives and would possibly represent a vulnerability?

A.   Provision for user-initiated change of nonuser-configured authentication information.
B.   Support shall be provided for a subject to establish a default user profile.
C.   The interface shall be independent of the type of authentication information handled.
D.   It shall not predefine the timing of secondary sign-on operations.

Correct Answer: A

QUESTION 1549

Which choice below is NOT an accurate statement about an organization's incident-handling capability?

A. The organization's incident-handling capability should be used to contain and repair damage done from incidents.
B. It should be used to prevent future damage from incidents.
C. The organization's incident-handling capability should be used to detect and punish senior-level executive wrong-doing.
D. It should be used to provide the ability to respond quickly and effectively to an incident.

Correct Answer: C

QUESTION 1550

Which is NOT a layer in the OSI architecture model?

A. Data Link
B. Internet
C. Transport
D. Session

Correct Answer: B

QUESTION 1551

A standard data manipulation and relational database definition language is:

A. OOD
B. SQL
C. Script
D. SLL

Correct Answer: B

QUESTION 1552

The main approach to obtaining the true biometric information from a collected sample of an individual's physiological or behavioral characteristics is:

A. False rejection
B. Enrollment

C. Digraphs
D. Feature extraction

Correct Answer: D

QUESTION 1553

The Secure European System for Applications in a Multivendor Environment (SESAME) implements a Kerberos-like distribution of secret keys. Which of the following is NOT a characteristic of SESAME?

A. Uses a trusted authentication server at each host.
B. Incorporates two certificates or tickets, one for authentication and one defining access privileges.
C. Uses secret key cryptography for the distribution of secret keys.
D. Uses public key cryptography for the distribution of secret keys.

Correct Answer: C

QUESTION 1554

Using symmetric key cryptography, Kerberos authenticates clients to other entities on a network and facilitates communications through the assignment of:

A. Tokens
B. Passwords
C. Public keys
D. Session keys

Correct Answer: D

QUESTION 1555

Which group represents the MOST likely source of an asset loss through inappropriate computer use?

A. Saboteurs
B. Hackers
C. Crackers
D. Employees

Correct Answer: D

QUESTION 1556

A reference monitor is a system component that enforces access controls on an object. Specifically, the reference monitor concept is an abstract machine that mediates all access of subjects to objects. The hardware, firmware, and software elements of a trusted computing base that implement the reference monitor concept are called:

A. Identification and authentication (I & A) mechanisms.
B. The auditing subsystem.
C. The security kernel.
D. The authorization database.

Correct Answer: C

QUESTION 1557

Which choice below is NOT an element of IPSec?

A. Encapsulating Security Payload.
B. Authentication Header.
C. Layer Two Tunneling Protocol.
D. Security Association.

Correct Answer: C

QUESTION 1558

Which choice below is an accurate statement about the difference between monitoring and auditing?

A. A system audit is an ongoing real-time activity that examines a system.
B. A system audit cannot be automated.
C. Monitoring is an ongoing activity that examines either the system or the users.
D. Monitoring is a one-time event to evaluate security.

Correct Answer: C

QUESTION 1559

The type of access control that is used in local, dynamic situations where subjects have the ability to specify what resources certain users can access is called:

A.   Mandatory access control.
B.   Rule-based access control.
C.   Discretionary access control.
D.   Sensitivity-based access control.

Correct Answer: C

QUESTION 1560
The number of times a password should be changed is NOT a function of:

A.   The responsibilities and clearance of the user.
B.   The criticality of the information to be protected.
C.   The type of workstation used.
D.   The frequency of the password's use.

Correct Answer: C

QUESTION 1561
Three things that must be considered for the planning and implementation of access control mechanisms are:

A.   Threats, assets, and objectives.
B.   Threats, vulnerabilities, and risks.
C.   Vulnerabilities, secret keys, and exposures.
D.   Exposures, threats, and countermeasures.

Correct Answer: B

QUESTION 1562
Access control that is a function of factors such as location, time of day, and previous access history is called:

A.   Information flow
B.   Context-dependent
C.   Positive
D.   Content-dependent

Correct Answer: B

QUESTION 1563