Correct Answer: B

QUESTION 1207
Which of the following statements pertaining to secure information processing facilities is incorrect?

A. Walls should have an acceptable fire rating.
B. Windows should be protected by bars.
C. Doors must resist forcible entry.
D. Location and type of fire suppression systems should be known.

Correct Answer: B

QUESTION 1208
Making sure that the data is accessible when and where it is needed is which of the following?

A. Confidentiality
B. Integrity
C. Acceptability
D. Availability

Correct Answer: D

QUESTION 1209
Business continuity plan development depends most on?

A. Directives of Senior Management
B. Business Impact Analysis (BIA)
C. Scope and Plan Initiation
D. Skills of BCP committee

Correct Answer: B

QUESTION 1210
Which layer defines the X.25, V.35, X.21 and HSSI standard interfaces?

A. Transport layer
B. Network layer
C. Data link layer
D. Physical layer

Correct Answer: D

QUESTION 1211

Related to information security, availability is the opposite of which of the following?

A. Delegation
B. Distribution
C. Documentation
D. Destruction

Correct Answer: D

QUESTION 1212

Which of the following is a disadvantage of a behavior-based ID system?

A. The activity and behavior of the users while in the networked system may not be static enough to effectively implement a behavior-based ID system.
B. The activity and behavior of the users while in the networked system may be dynamic enough to effectively implement a behavior-based ID system.
C. The activity and behavior of the users while in the networked system may not be dynamic enough to effectively implement a behavior-based ID system.
D. The system is characterized by high false negative rates where intrusions are missed.

Correct Answer: A

QUESTION 1213

Which of the following statements pertaining to VPN protocol standards is false?

A. L2TP is a combination of PPTP and L2F.
B. L2TP and PPTP were designed for single point-to-point client to server communication.
C. L2TP operates at the network layer.
D. PPTP uses native PPP authentication and encryption services.

Correct Answer: C

QUESTION 1214

What is the most critical characteristic of a biometric identifying system?

A. Perceived intrusiveness
B. Storage requirements

C. Accuracy
D. Reliability

Correct Answer: C

QUESTION 1215
RAID Software can run faster in the operating system because neither use the hardware-level parity drives by?

A. Simple striping or mirroring.
B. Hard striping or mirroring.
C. Simple hamming code parity or mirroring.
D. Simple striping or hamming code parity.

Correct Answer: A

QUESTION 1216
The guarantee that the message sent is the message received, and that the message was not intentionally or unintentionally altered is?

A. Integrity
B. Confidentiality
C. Availability
D. Identity

Correct Answer: A

QUESTION 1217
Which of the following is a preventive control?

A. Motion detectors
B. Guard dogs
C. Audit logs
D. Intrusion detection systems

Correct Answer: B

QUESTION 1218

What uses a key of the same length as the message?

A. Running key cipher
B. One-time pad
C. Steganography
D. Cipher block chaining

Correct Answer: B

QUESTION 1219

Which of the following protocols operates at the session layer (layer 5)?

A. RPC
B. IGMP
C. LDP
D. SPX

Correct Answer: A

QUESTION 1220

Which of the following are NOT a countermeasure to traffic analysis?

A. Padding messages
B. Eavesdropping
C. Sending noise
D. Covert channel analysis

Correct Answer: B

QUESTION 1221

Which of the following layers of the ISO/OSI model do packet filtering firewalls operate at?

A. Application layer
B. Session layer
C. Network layer
D. Presentation layer

Correct Answer: C

QUESTION 1222

A prolonged high voltage is?

A. Spike
B. Blackout
C. Surge
D. Fault

Correct Answer: C

QUESTION 1223

How do the Information Labels of Compartmented Mode Workstation differ from the Sensitivity Levels of B3 evaluated systems?

A. Information Labels in CMW are homologous to Sensitivity Labels, but a different term was chosen to emphasize that CMW's are not described in the Orange Book.
B. Information Labels contain more information than Sensitivity Labels, thus allowing more granular access decisions to be made.
C. Sensitivity Labels contain more information than Information Labels because B3+ systems should store more sensitive data than workstations.
D. Information Labels contain more information than Sensitivity Labels, but are not used by the Reference Monitor to determine access permissions.

Correct Answer: D

QUESTION 1224

In what security mode can a system be operating if all users have the clearance or authorization and need-to-know to all data processed within the system?

A. Dedicated security mode.
B. System-high security mode.
C. Compartmented security mode.
D. Multilevel security mode.

Correct Answer: A

QUESTION 1225

What are the three conditions that must be met by the reference monitor?

A. Confidentiality, availability and integrity.
B. Policy, mechanism and assurance.