

CISSP Sample

QUESTION 1:

Which of the following is a means of restricting access to objects based on the identity of the subject to which they belong?

- A. Mandatory access control
- B. Group access control
- C. Discretionary access control
- D. User access control

Answer: C

Explanation:

The question does not ask about the identity of the accessing subject, the question refers to the subject to which the object belongs (ie the owner).

The owner setting the access rights is the definition of DAC.

"DAC systems grant or deny access based on the identity of the subject." Harris, 3rd Ed, p 163

QUESTION 2:

What tool is being used to determine whether attackers have altered system files of executables?

- A. File Integrity Checker
- B. Vulnerability Analysis Systems
- C. Honey Pots
- D. Padded Cells

Answer: A

Explanation:

Although File Integrity Checkers are most often used to determine whether attackers have altered system files or executables, they can also help determine whether vendor-supplied bug patches or other desired changes have been applied to system binaries. They are extremely valuable to those conducting a forensic examination of systems that have been attacked, as they allow quick and reliable diagnosis of the footprint of an attack. This enables system managers to optimize the restoration of service after incidents occur.

QUESTION 3:

Disaster Recovery Plan emergency produces is a plan of action that commences immediately to prevent or minimize property damage and to:

- A. Prevent interruption of service.
- B. Minimize embarrassment.
- C. Prevent loss of life.
- D. Evacuate the facility.

Answer: C

Explanation:

Protection of life is of the utmost importance and should be dealt with first before looking to save material objects. - Shon Harris

CISSP Sample

All-in-one CISSP Certification Guide pg 625

QUESTION 4:

The confidentiality of alcohol and drug abuse patient records maintained by this program is protected by federal law and regulations. Generally, the program may not say to a person outside the program that a patient attends the program, or disclose any information identifying a patient as an alcohol or drug abuser even if:

- A.) The person outside the program gives a written request for the information
- B.) the patient consent in writing
- C.) the disclosure is allowed by a court order
- D.) the disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit, or program evaluation.

Answer: D

Explanation:

Incident handling is not related to disaster recovery, it is related to security incidents.

QUESTION 5:

Which of the following best describes the Secure Electronic Transaction (SET) protocol?

- A. Originated by VISA and MasterCard as an Internet credit card protocol.
- B. Originated by VISA and MasterCard as an Internet credit card protocol using digital signatures.
- C. Originated by VISA and MasterCard as an Internet credit card protocol using the transport layer.
- D. Originated by VISA and MasterCard as an Internet credit card protocol using SSL.

Answer: B

Explanation:

This protocol was created by VISA and MasterCard as a common effort to make the buying process over the Internet secure through the distribution line of those companies. It is located in layer 7 of the OSI model. SET uses a system of locks and keys along with certified account IDs for both consumers and merchants. Then, through a unique process of "encrypting" or scrambling the information exchanged between the shopper and the online store, SET ensures a payment process that is convenient, private and most of all secure.

Specifically, SET:

1. Establishes industry standards to keep your order and payment information confidential.
2. Increases integrity for all transmitted data through encryption.
3. Provides authentication that a cardholder is a legitimate user of a branded payment card account.
4. Provides authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.
5. Allows the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.

The SET process relies strongly on the use of certificates and digital signatures for the process of authentication and integrity of the information.