SSCP$^{Q\&As}$

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/sscp.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

QUESTION 1

Which of the following choice is NOT normally part of the questions that would be asked in regards to an organization\\'s information security policy?

A. Who is involved in establishing the security policy?

B. Where is the organization\\'s security policy defined?

C. What are the actions that need to be performed in case of a disaster?

D. Who is responsible for monitoring compliance to the organization\\'s security policy?

Correct Answer: C

Actions to be performed in case of a disaster are not normally part of an information security policy but part of a Disaster Recovery Plan (DRP).

Only personnel implicated in the plan should have a copy of the Disaster Recovery Plan whereas everyone should be aware of the contents of the organization\\'s information security policy. Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison- Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 398).

QUESTION 2

Why should batch files and scripts be stored in a protected area?

A. Because of the least privilege concept.

B. Because they cannot be accessed by operators.

C. Because they may contain credentials.

D. Because of the need-to-know concept.

Correct Answer: C

Because scripts contain credentials, they must be stored in a protected area and the transmission of the scripts must be dealt with carefully. Operators might need access to batch files and scripts. The least privilege concept requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services.

Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System and Methodology (page 3)

QUESTION 3

Which of the following can be used as a covert channel?

A. Storage and timing.

B. Storage and low bits.

C. Storage and permissions.

D. Storage and classification.

Correct Answer: A

The Orange book requires protection against two types of covert channels, Timing and Storage. The following answers are incorrect:

Storage and low bits. Is incorrect because, low bits would not be considered a covert channel.

Storage and permissions. Is incorrect because, permissions would not be considered a covert channel.

Storage and classification. Is incorrect because, classification would not be considered a covert channel.

QUESTION 4

Which of the following is best defined as a circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it?

A. Aggregation

B. Inference

C. Clustering

D. Collision

Correct Answer: A

The Internet Security Glossary (RFC2828) defines aggregation as a circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 5

In Mandatory Access Control, sensitivity labels attached to object contain what information?

A. The item\\'s classification

B. The item\\'s classification and category set

C. The item\\'s category

D. The items\\'s need to know

Correct Answer: B

A Sensitivity label must contain at least one classification and one category set. Category set and Compartment set are synonyms, they mean the same thing. The sensitivity label must contain at least one

Classification and at least one Category. It is common in some environments for a single item to belong to multiple categories. The list of all the categories to which an item belongs is called a compartment set or category set.

The following answers are incorrect:

the item\\'s classification. Is incorrect because you need a category set as well. the item\\'s category. Is incorrect because category set and classification would be both be required.

The item\\'s need to know. Is incorrect because there is no such thing. The need to know is indicated by the catergories the object belongs to. This is NOT the best answer.

Reference(s) used for this question:

OIG CBK, Access Control (pages 186 - 188)

AIO, 3rd Edition, Access Control (pages 162 - 163)

AIO, 4th Edittion, Access Control, pp 212-214.

Wikipedia - http://en.wikipedia.org/wiki/Mandatory_Access_Control

SSCP VCE Dumps SSCP Study Guide SSCP Exam Questions