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.passapply.com/sscp.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following questions are least likely to help in assessing controls covering audit trails?

A. Does the audit trail provide a trace of user actions?

B. Are incidents monitored and tracked until resolved?

C. Is access to online logs strictly controlled?

D. Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?

Correct Answer: B

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. Audit trail controls are considered technical controls. Monitoring and tracking of incidents is more an operational control related to incident response capability.

Reference(s) used for this question:

SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-50 to A-51).

NOTE: NIST SP 800-26 has been superceded By: FIPS 200, SP 800-53, SP 800-53A

You can find the new replacement at: http://csrc.nist.gov/publications/PubsSPs.html

However, if you really wish to see the old standard, it is listed as an archived document at:

http://csrc.nist.gov/publications/PubsSPArch.html

QUESTION 2

Which of the following server contingency solutions offers the highest availability?

A. System backups

B. Electronic vaulting/remote journaling

C. Redundant arrays of independent disks (RAID)

D. Load balancing/disk replication

Correct Answer: D

Of the offered technologies, load balancing/disk replication offers the highest availability, measured in terms of minutes of lost data or server downtime. A Network-Attached Storage (NAS) or a Storage Area Network (SAN) solution combined with virtualization would offer an even higher availability.

Source: SWANSON, Marianne, and al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 49).

QUESTION 3

Which of the following is true about link encryption?

A. Each entity has a common key with the destination node.

B. Encrypted messages are only decrypted by the final node.

C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.

D. Only secure nodes are used in this type of transmission.

Correct Answer: C

In link encryption, each entity has keys in common with its two neighboring nodes in the transmission chain.

Thus, a node receives the encrypted message from its predecessor, decrypts it, and then re- encrypts it with a new key, common to the successor node. Obviously, this mode does not provide protection if anyone of the nodes along the transmission path is compromised.

Encryption can be performed at different communication levels, each with different types of protection and implications. Two general modes of encryption implementation are link encryption and end-to-end encryption.

Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers.

In end-to-end encryption, the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition (pp. 845-846). McGraw- Hill. And:

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 4: Cryptography (page 132).

QUESTION 4

What principle focuses on the uniqueness of separate objects that must be joined together to perform a task? It is sometimes referred to as "what each must bring" and joined together when getting access or decrypting a file. Each of which does not reveal the other?

A. Dual control

B. Separation of duties

C. Split knowledge

D. Need to know

Correct Answer: C

Split knowledge involves encryption keys being separated into two components, each of which does not reveal the other. Split knowledge is the other complementary access control principle to dual control.

In cryptographic terms, one could say dual control and split knowledge are properly implemented if no one person has access to or knowledge of the content of the complete cryptographic key being protected by the two rocesses. The sound implementation of dual control and split knowledge in a cryptographic environment necessarily means that the quickest way to break the key would be through the best attack known for the algorithm of that key. The principles of dual control and split knowledge primarily apply to access to plaintext keys.

Access to cryptographic keys used for encrypting and decrypting data or access to keys that are encrypted under a master key (which may or may not be maintained under dual control and split knowledge) do not require dual control and split knowledge. Dual control and split knowledge can be summed up as the determination of any part of a key being protected must require the collusion between two or more persons with each supplying unique cryptographic materials that must be joined together to access the protected key.

Any feasible method to violate the axiom means that the principles of dual control and split knowledge are not being upheld.

Split knowledge is the unique "what each must bring" and joined together when implementing dual control. To illustrate, a box containing petty cash is secured by one combination lock and one keyed lock. One employee is given the combination to the combo lock and another employee has possession of the correct key to the keyed lock.

In order to get the cash out of the box both employees must be present at the cash box at the same time. One cannot open the box without the other. This is the aspect of dual control.

On the other hand, split knowledge is exemplified here by the different objects (the combination to the combo lock and the correct physical key), both of which are unique and necessary, that each brings to the meeting. Split knowledge focuses on the uniqueness of separate objects that must be joined together.

Dual control has to do with forcing the collusion of at least two or more persons to combine their split knowledge to gain access to an asset. Both split knowledge and dual control complement each other and are necessary functions that implement the segregation of duties in high integrity cryptographic environments. The following are incorrect answers:

Dual control is a procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource. Dual control is implemented as a security procedure that requires two or more persons to come together and collude to complete a process. In a cryptographic system the two (or more) persons would each supply a unique key, that when taken together, performs a cryptographic process. Split knowledge is the other complementary access control principle to dual control.

Separation of duties - The practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process.

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.

Reference(s) used for this question:

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Cryptography (Kindle Locations 1621-1635). . Kindle Edition.

and

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :

Cryptography (Kindle Locations 1643-1650). . Kindle Edition.

and

Shon Harris, CISSP All In One (AIO), 6th Edition , page 126

QUESTION 5

What is the essential difference between a self-audit and an independent audit?

A. Tools used

B. Results

C. Objectivity

D. Competence

Correct Answer: C

To maintain operational assurance, organizations use two basic methods: system audits and monitoring. Monitoring refers to an ongoing activity whereas audits are one-time or periodic events and can be either internal or external. The essential difference between a self-audit and an independent audit is objectivity, thus indirectly affecting the results of the audit. Internal and external auditors should have the same level of competence and can use the same tools.

Source: SWANSON, Marianne and GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 25).

SSCP PDF Dumps SSCP VCE Dumps SSCP Exam Questions