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.geekcert.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

Encapsulating Security Payload (ESP) provides some of the services of Authentication Headers (AH), but it is primarily designed to provide:

A. Confidentiality

B. Cryptography

C. Digital signatures

D. Access Control

Correct Answer: A

Source: TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 164.

QUESTION 2

Which of the following does NOT use token-passing?

A. ARCnet

B. FDDI

C. Token-ring

D. IEEE 802.3

Correct Answer: D

IEEE 802.3 specifies the standard for Ethernet and uses CSMA/CD, not token-passing.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 3: Telecommunications and Network Security (page 104).

QUESTION 3

Smart cards are an example of which type of control?

A. Detective control

B. Administrative control

C. Technical control

D. Physical control

Correct Answer: C

Logical or technical controls involve the restriction of access to systems and the protection of information. Smart cards and encryption are examples of these types of control.

Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Many types of technical controls enable a user to access a system and the resources within that system. A technical control may be a username and password combination, a Kerberos implementation, biometrics, public key infrastructure (PKI), RADIUS, TACACS +, or authentication using a smart card through a reader connected to a system. These technologies verify the user is who he says he is by using different types of authentication methods. Once a user is properly authenticated, he can be authorized and allowed access to network resources.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition (p. 245). McGraw-Hill. Kindle Edition.

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 2: Access control systems (page 32).

QUESTION 4

Access Control techniques do not include which of the following choices?

A. Relevant Access Controls

B. Discretionary Access Control

C. Mandatory Access Control

D. Lattice Based Access Control

Correct Answer: A

Access Control Techniques Discretionary Access Control Mandatory Access Control Lattice Based Access Control Rule-Based Access Control Role-Based Access Control Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open

Study Group Study Guide for Domain 1, Page 13.

QUESTION 5

Which of the following standards concerns digital certificates?

A. X.400

B. X.25

C. X.509

D. X.75

Correct Answer: C

X.509 is used in digital certificates. X.400 is used in e-mail as a message handling protocol. X.25 is a standard for the network and data link levels of a communication network and X.75 is a standard defining ways of connecting two X.25 networks.

Source: 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 164).