# 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**

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 2**

Which of the following technologies has been developed to support TCP/IP networking over low-speed serial interfaces?

A. ISDN

B. SLIP

C. xDSL

D. T1

Correct Answer: B

Serial Line IP (SLIP) was developed in 1984 to support TCP/IP networking over low-speed serial interfaces.

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 114).

**QUESTION 3**

Which of the following should NOT normally be allowed through a firewall?

A. SNMP

B. SMTP

C. HTTP

D. SSH

Correct Answer: A

The Simple Network Management Protocol (SNMP) is a useful tool for remotely managing network

devices.

Since it can be used to reconfigure devices, SNMP traffic should be blocked at the organization\\'s firewall.

Using a VPN with encryption or some type of Tunneling software would be highly recommended in this

case.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4:

Sockets and Services from a Security Viewpoint.

**QUESTION 4**

Which of the following access control techniques best gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization\\'s structure?

A. Access control lists

B. Discretionary access control

C. Role-based access control D. Non-mandatory access control

Correct Answer: C

Role-based access control (RBAC) gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization\\'s structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are given to users in that role. An access control list (ACL) is a table that tells a system which access rights each user has to a particular system object. With discretionary access control, administration is decentralized and owners of resources control other users\\' access. Non- mandatory access control is not a defined access control technique.

Source: ANDRESS, Mandy, ram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 9).

**QUESTION 5**

Which of the following is the FIRST step in protecting data\\'s confidentiality?

A. Install a firewall

B. Implement encryption

C. Identify which information is sensitive

D. Review all user access rights

Correct Answer: C

In order to protect the confidentiality of the data.

The following answers are incorrect because :

Install a firewall is incorrect as this would come after the information has been identified for sensitivity levels.

Implement encryption is also incorrect as this is one of the mechanisms to protect the data once it has been identified.

Review all user access rights is also incorrect as this is also a protection mechanism for the identified information.

Reference : Shon Harris AIO v3 , Chapter-4 : Access Control , Page : 126