SSCP$^{\text{Q\&As}}$

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

QUESTION 1

Which of the following is less likely to be used today in creating a Virtual Private Network?

A. L2TP

B. PPTP

C. IPSec

D. L2F

Correct Answer: D

L2F (Layer 2 Forwarding) provides no authentication or encryption. It is a Protocol that supports the creation of secure virtual private dial-up networks over the Internet. At one point L2F was merged with PPTP to produce L2TP to be used on networks and not only on dial up links. IPSec is now considered the best VPN solution for IP environments. Source: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 507).

QUESTION 2

The Computer Security Policy Model the Orange Book is based on is which of the following?

A. Bell-LaPadula

B. Data Encryption Standard

C. Kerberos

D. Tempest

Correct Answer: A

The Computer Security Policy Model Orange Book is based is the Bell-LaPadula Model. Orange Book

Glossary.

The Data Encryption Standard (DES) is a cryptographic algorithm. National Information Security Glossary.

TEMPEST is related to limiting the electromagnetic emanations from electronic equipment. Reference:

U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28STD. December 1985 (also available here).

QUESTION 3

What is the name of the third party authority that vouches for the binding between the data items in a digital certificate?

A. Registration authority

B. Certification authority

C. Issuing authority

D. Vouching authority

Correct Answer: B

A certification authority (CA) is a third party entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. An issuing authority could be considered a correct answer, but not the best answer, since it is too generic.

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

QUESTION 4

The basic language of modems and dial-up remote access systems is:

A. Asynchronous Communication.

B. Synchronous Communication.

C. Asynchronous Interaction.

D. Synchronous Interaction.

Correct Answer: A

Asynchronous Communication is the basic language of modems and dial-up remote access systems.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 100.

QUESTION 5

Public Key Infrastructure (PKI) uses asymmetric key encryption between parties. The originator encrypts information using the intended recipient\\'s "public" key in order to get confidentiality of the data being sent. The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology ensures that:

A. The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.

B. The channels through which the information flows are secure.

C. The recipient\\'s identity can be positively verified by the sender.

D. The sender of the message is the only other person with access to the recipient\\'s private key.

Correct Answer: C

Through the use of Public Key Infrastructure (PKI) the recipient\\'s identity can be positively verified by the

sender.

The sender of the message knows he is using a Public Key that belongs to a specific user. He can validate through the Certification Authority (CA) that a public key is in fact the valid public key of the receiver and the receiver is really who he claims to be. By using the public key of the recipient, only the recipient using the matching private key will be able to decrypt the message. When you wish to achieve confidentiality, you encrypt the message with the recipient public key.

If the sender would wish to prove to the recipient that he is really who he claims to be then the sender would apply a digital signature on the message before encrypting it with the public key of the receiver. This would provide Confidentiality and Authenticity of the message.

A PKI (Public Key Infrastructure) enables users of an insecure public network, such as the Internet, to securely and privately exchange data through the use of public key-pairs that are obtained and shared through a trusted authority, usually referred to as a Certificate Authority.

The PKI provides for digital certificates that can vouch for the identity of individuals or organizations, and for directory services that can store, and when necessary, revoke those digital certificates. A PKI is the underlying technology that addresses the issue of trust in a normally untrusted environment.

The following answers are incorrect:

The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use. Is incorrect because through the use of Public Key Infrastructure (PKI), the parties do not have to have a mutual agreement. They have a trusted 3rd party Certificate Authority to perform the verification of the sender.

The channels through which the information flows are secure. Is incorrect because the use of Public Key Infrastructure (PKI) does nothing to secure the channels.

The sender of the message is the only other person with access to the recipient\\'s private key. Is incorrect because the sender does not have access to the recipient\\'s private key though Public Key Infrastructure (PKI).

Reference(s) used for this question:

OIG CBK Cryptography (pages 253 - 254)

SSCP Study Guide SSCP Exam Questions SSCP Braindumps