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

Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?

A. OAKLEY

B. Internet Security Association and Key Management Protocol (ISAKMP)

C. Simple Key-management for Internet Protocols (SKIP)

D. IPsec Key exchange (IKE)

Correct Answer: B

RFC 2828 (Internet Security Glossary) defines the Internet Security Association and Key Management Protocol (ISAKMP) as an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.

Let\\'s clear up some confusion here first. Internet Key Exchange (IKE) is a hybrid protocol, it consists of 3 "protocols"

ISAKMP: It\\'s not a key exchange protocol per se, it\\'s a framework on which key exchange protocols operate. ISAKMP is part of IKE. IKE establishs the shared security policy and authenticated keys. ISAKMP is the protocol that specifies the mechanics of the key exchange.

Oakley: Describes the "modes" of key exchange (e.g. perfect forward secrecy for keys, identity protection, and authentication). Oakley describes a series of key exchanges and services.

SKEME: Provides support for public-key-based key exchange, key distribution centres, and manual installation, it also outlines methods of secure and fast key refreshment. So yes, IPSec does use IKE, but ISAKMP is part of IKE.

The questions did not ask for the actual key negotiation being done but only for the "exchange of key generation and authentication data" being done. Under Oakly it would be Diffie Hellman (DH) that would be used for the actual key nogotiation.

The following are incorrect answers:

Simple Key-management for Internet Protocols (SKIP) is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

OAKLEY is a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP.

IPsec Key Exchange (IKE) is an Internet, IPsec, key-establishment protocol [R2409] (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.

Reference used for this question:

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

QUESTION 2

Which layer of the DoD TCP/IP model controls the communication flow between hosts?

A. Internet layer

B. Host-to-host transport layer

C. Application layer

D. Network access layer

Correct Answer: B

Whereas the host-to-host layer (equivalent to the OSI\\'s transport layer) provides end-to-end data delivery service, flow control, to the application layer.

The four layers in the DoD model, from top to bottom, are:

The Application Layer contains protocols that implement user-level functions, such as mail delivery, file transfer and remote login. The Host-to-Host Layer handles connection rendez vous, flow control, retransmission of lost data, and other generic data flow management between hosts. The mutually exclusive TCP and UDP protocols are this layer\\'s most important members.

The Internet Layer is responsible for delivering data across a series of different physical networks that interconnect a source and destination machine. Routing protocols are most closely associated with this layer, as is the IP Protocol, the Internet\\'s fundamental protocol.

The Network Access Layer is responsible for delivering data over the particular hardware media in use. Different protocols are selected from this layer, depending on the type of physical network The OSI model organizes communication services into seven groups called layers. The layers are as follows:

Layer 7, The Application Layer: The application layer serves as a window for users and application processes to access network services. It handles issues such as network transparency, resource allocation, etc. This layer is not an application in itself, although some applications may perform application layer functions.

Layer 6, The Presentation Layer: The presentation layer serves as the data translator for a network. It is usually a part of an operating system and converts incoming and outgoing data from one presentation format to another. This layer is also known as syntax layer.

Layer 5, The Session Layer: The session layer establishes a communication session between processes running on different communication entities in a network and can support a message- mode data transfer. It deals with session and connection coordination.

Layer 4, The Transport Layer: The transport layer ensures that messages are delivered in the order in which they are sent and that there is no loss or duplication. It ensures complete data transfer. This layer provides an additional connection below the Session layer and assists with managing some data flow control between hosts. Data is divided into packets on the sending node, and the receiving node\\'s Transport layer reassembles the message from packets. This layer is also responsible for error checking to guarantee error-free data delivery, and requests a retransmission if necessary. It is also responsible for sending acknowledgments of successful transmissions back to the sending host. A number of protocols run at the Transport layer, including TCP, UDP, Sequenced Packet Exchange (SPX), and NWLink. Layer 3, The Network Layer: The network layer controls the operation of the subnet. It determines the physical path that data takes on the basis of network conditions, priority of service, and other factors. The network layer is responsible for routing and forwarding data packets.

Layer 2, The Data-Link Layer: The data-link layer is responsible for error free transfer of data frames. This layer provides synchronization for the physical layer. ARP and RARP would be found at this layer.

Layer 1, The Physical Layer: The physical layer is responsible for packaging and transmitting data on the physical media. This layer conveys the bit stream through a network at the electrical and mechanical level.

See a great flash animation on the subject at:

http://www.maris.com/content/applets/flash/comp/fa0301.swf

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 85).

Also: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, chapter 7: Telecommunications and Network Security (page 344).

QUESTION 3

A trusted system does NOT involve which of the following?

A. Enforcement of a security policy.

B. Sufficiency and effectiveness of mechanisms to be able to enforce a security policy.

C. Assurance that the security policy can be enforced in an efficient and reliable manner.

D. Independently-verifiable evidence that the security policy-enforcing mechanisms are sufficient and effective.

Correct Answer: C

A trusted system is one that meets its intended security requirements. It involves sufficiency and effectiveness, not necessarily efficiency, in enforcing a security policy. Put succinctly, trusted systems have

(1) policy, (2) mechanism, and (3) assurance.

Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 4

Which backup method only copies files that have been recently added or changed and also leaves the archive bit unchanged?

A. Full backup method

B. Incremental backup method

C. Fast backup method

D. Differential backup method

Correct Answer: D

A differential backup is a partial backup that copies a selected file to tape only if the archive bit for that file is turned on, indicating that it has changed since the last full backup. A differential backup leaves the archive bits unchanged on the files it copies.

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 69).

Also see: http://e-articles.info/e/a/title/Backup-Types/

Backup software can use or ignore the archive bit in determining which files to back up, and can either turn the archive bit off or leave it unchanged when the backup is complete. How the archive bit is used and manipulated determines what type of backup is done, as follows

Full backup

A full backup, which Microsoft calls a normal backup, backs up every selected file, regardless of the status of the archive bit. When the backup completes, the backup software turns off the archive bit for every file that was backed up. Note that "full" is a misnomer because a full backup backs up only the files you have selected, which may be as little as one directory or even a single file, so in that sense Microsoft\\'s terminology is actually more accurate. Given the choice, full backup is the method to use because all files are on one tape, which makes it much easier to retrieve files from tape when necessary. Relative to partial backups, full backups also increase redundancy because all files are on all tapes. That means that if one tape fails, you may still be able to retrieve a given file from another tape.

Differential backup

A differential backup is a partial backup that copies a selected file to tape only if the archive bit for that file is turned on, indicating that it has changed since the last full backup. A differential backup leaves the archive bits unchanged on the files it copies. Accordingly, any differential backup set contains all files that have changed since the last full backup. A differential backup set run soon after a full backup will contain relatively few files. One run soon before the next full backup is due will contain many files, including those contained on all previous differential backup sets since the last full backup. When you use differential backup, a complete backup set comprises only two tapes or tape sets: the tape that contains the last full backup and the tape that contains the most recent differential backup.

Incremental backup

An incremental backup is another form of partial backup. Like differential backups, Incremental Backups copy a selected file to tape only if the archive bit for that file is turned on. Unlike the differential backup, however, the incremental backup clears the archive bits for the files it backs up. An incremental backup set therefore contains only files that have changed since the last full backup or the last incremental backup. If you run an incremental backup daily, files changed on Monday are on the Monday tape, files changed on Tuesday are on the Tuesday tape, and so forth. When you use an incremental backup scheme, a complete backup set comprises the tape that contains the last full backup and all of the tapes that contain every incremental backup done since the last normal backup. The only advantages of incremental backups are that they minimize backup time and keep multiple versions of files that change frequently. The disadvantages are that backed-up files are scattered across multiple tapes, making it difficult to locate any particular file you need to restore, and that there is no redundancy. That is, each file is stored only on one tape.

Full copy backup

A full copy backup (which Microsoft calls a copy backup) is identical to a full backup except for the last step. The full backup finishes by turning off the archive bit on all files that have been backed up. The full copy backup instead leaves the archive bits unchanged. The full copy backup is useful only if you are using a combination of full backups and incremental or differential partial backups. The full copy backup allows you to make a duplicate "full" backup--e.g., for storage offsite, without altering the state of the hard drive you are backing up, which would destroy the integrity of the partial backup rotation.

Some Microsoft backup software provides a bizarre backup method Microsoft calls a daily copy backup. This method ignores the archive bit entirely and instead depends on the date- and timestamp of files to determine which files should be backed up. The problem is, it\\'s quite possible for software to change a file without changing the date- and timestamp, or to change the date- and timestamp without changing the contents of the file. For this reason, we regard the daily copy backup as entirely unreliable and recommend you avoid using it.

QUESTION 5

Which of the following statements pertaining to VPN protocol standards is false?

A. L2TP is a combination of PPTP and L2F.

B. L2TP and PPTP were designed for single point-to-point client to server communication.

C. L2TP operates at the network layer.

D. PPTP uses native PPP authentication and encryption services.

Correct Answer: C

L2TP and PPTP were both designed for individual client to server connections; they enable only a single point-to-point connection per session. Dial-up VPNs use L2TP often. Both L2TP and PPTP operate at the data link layer (layer 2) of the OSI model. PPTP uses native PPP authentication and encryption services and L2TP is a combination of PPTP and Layer 2 Forwarding protocol (L2F).

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 95).