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.pass2lead.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 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 2

What level of assurance for a digital certificate verifies a user\\'s name, address, social security number, and other information against a credit bureau database?

A. Level 1/Class 1

B. Level 2/Class 2

C. Level 3/Class 3

D. Level 4/Class 4

Correct Answer: B

Users can obtain certificates with various levels of assurance. Here is a list that describe each of them:

-

Class 1/Level 1 for individuals, intended for email, no proof of identity

For example, level 1 certificates verify electronic mail addresses. This is done through the use of a personal information number that a user would supply when asked to register. This level of certificate may also provide a name as well as an electronic mail address; however, it may or may not be a genuine name (i.e., it could be an alias). This proves that a human being will reply back if you send an email to that name or email address.

-

Class 2/Level 2 is for organizations and companies for which proof of identity is required

Level 2 certificates verify a user\\'s name, address, social security number, and other information against a credit bureau database.

-

Class 3/Level 3 is for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority

Level 3 certificates are available to companies. This level of certificate provides photo identification to accompany the

other items of information provided by a level 2 certificate.

-

Class 4 for online business transactions between companies

-

Class 5 for private organizations or governmental security References:

http://en.wikipedia.org/wiki/Digital_certificate veriSign introduced the concept of classes of digital

certificates:

Also see:

Source: TIPTON, Harold F. and KRAUSE, Micki, Information Security Management Handbook, 4th edition

(volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 54).

QUESTION 3

What is the name of the protocol use to set up and manage Security Associations (SA) for IP Security (IPSec)?

A. Internet Key Exchange (IKE)

B. Secure Key Exchange Mechanism

C. Oakley

D. Internet Security Association and Key Management Protocol

Correct Answer: A

The Key management for IPSec is called the Internet Key Exchange (IKE)

Note: IKE underwent a series of improvements establishing IKEv2 with RFC 4306. The basis of this answer is IKEv2.

The IKE protocol is a hybrid of three other protocols: ISAKMP (Internet Security Association and Key Management Protocol), Oakley and SKEME. ISAKMP provides a framework for authentication and key exchange, but does not define them (neither authentication nor key exchange). The Oakley protocol describes a series of modes for key exchange and the SKEME protocol defines key exchange techniques.

IKE--Internet Key Exchange. A hybrid protocol that implements Oakley and Skeme key exchanges inside the ISAKMP framework. IKE can be used with other protocols, but its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.

IKE is implemented in accordance with RFC 2409, The Internet Key Exchange. The Internet Key Exchange (IKE) security protocol is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.

IKE is a hybrid protocol that implements the Oakley key exchange and the SKEME key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and SKEME are security protocols implemented by IKE.)

IKE automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without costly manual preconfiguration. Specifically, IKE provides these benefits:

Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.

Allows you to specify a lifetime for the IPSec security association.

Allows encryption keys to change during IPSec sessions.

Allows IPSec to provide anti-replay services.

Permits certification authority (CA) support for a manageable, scalable IPSec implementation.

Allows dynamic authentication of peers.

About ISAKMP

The Internet Security Association and Key Management Protocol (ISAKMP) is a framework that defines the phases for establishing a secure relationship and support for negotiation of security attributes, it does not establish sessions keys by itself, it is used along with the Oakley session key establishment protocol. The Secure Key Exchange Mechanism (SKEME) describes a secure exchange mechanism and Oakley defines the modes of operation needed to establish a secure connection.

ISAKMP provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. Alone, it does not establish session keys. However it can be used with various session key establishment protocols, such as Oakley, to provide a complete solution to Internet key management.

About Oakley

The Oakley protocol uses a hybrid Diffie-Hellman technique to establish session keys on Internet hosts and routers. Oakley provides the important security property of Perfect Forward Secrecy (PFS) and is based on cryptographic techniques that have survived substantial public scrutiny. Oakley can be used by itself, if no attribute negotiation is needed, or Oakley can be used in conjunction with ISAKMP. When ISAKMP is used with Oakley, key escrow is not feasible.

The ISAKMP and Oakley protocols have been combined into a hybrid protocol. The resolution of ISAKMP with Oakley uses the framework of ISAKMP to support a subset of Oakley key exchange modes. This new key exchange protocol provides optional PFS, full security association attribute negotiation, and authentication methods that provide both repudiation and non-repudiation. Implementations of this protocol can be used to establish VPNs and also allow for users from remote sites (who may have a dynamically allocated IP address) access to a secure network.

About IPSec

The IETF\\'s IPSec Working Group develops standards for IP-layer security mechanisms for both IPv4 and IPv6. The group also is developing generic key management protocols for use on the Internet. For more information, refer to the IP Security and Encryption Overview.

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. It acts at the network level and implements the following standards:

IPSec

Internet Key Exchange (IKE)

Data Encryption Standard (DES)

MD5 (HMAC variant)

SHA (HMAC variant)

Authentication Header (AH)

Encapsulating Security Payload (ESP)

IPSec services provide a robust security solution that is standards-based. IPSec also provides data

authentication and anti-replay services in addition to data confidentiality services.

For more information regarding IPSec, refer to the chapter "Configuring IPSec Network Security." About SKEME
SKEME constitutes a compact protocol that supports a variety of realistic scenarios and security models

over Internet. It provides clear tradeoffs between security and performance as required by the different scenarios without incurring in unnecessary system complexity. The protocol supports key exchange based on public key, key distribution centers, or manual installation, and provides for fast and secure key refreshment. In addition, SKEME selectively provides perfect forward secrecy, allows for replaceability and negotiation of the underlying cryptographic primitives, and addresses privacy issues as anonymity and repudiatability

SKEME\\'s basic mode is based on the use of public keys and a Diffie-Hellman shared secret generation.

However, SKEME is not restricted to the use of public keys, but also allows the use of a pre- shared key.

This key can be obtained by manual distribution or by the intermediary of a key distribution center (KDC)

such as Kerberos.

In short, SKEME contains four distinct modes:

Basic mode, which provides a key exchange based on public keys and ensures PFS thanks to Diffie-

Hellman.

A key exchange based on the use of public keys, but without Diffie-Hellman.

A key exchange based on the use of a pre-shared key and on Diffie-Hellman.

A mechanism of fast rekeying based only on symmetrical algorithms.

In addition, SKEME is composed of three phases: SHARE, EXCH and AUTH.

During the SHARE phase, the peers exchange half-keys, encrypted with their respective public keys.

These two half-keys are used to compute a secret key K. If anonymity is wanted, the identities of the two

peers are also encrypted. If a shared secret already exists, this phase is skipped.

The exchange phase (EXCH) is used, depending on the selected mode, to exchange either Diffie-Hellman public values or nonces. The Diffie-Hellman shared secret will only be computed after the end of the exchanges.

The public values or nonces are authenticated during the authentication phase (AUTH), using the secret

key established during the SHARE phase.

The messages from these three phases do not necessarily follow the order described above; in actual

practice they are combined to minimize the number of exchanged messages.

References used for this question:

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 172).

http://tools.ietf.org/html/rfc4306

http://tools.ietf.org/html/rfc4301

http://en.wikipedia.org/wiki/Internet_Key_Exchange

CISCO ISAKMP and OAKLEY information CISCO Configuring Internet Key Exchange Protocol

http://www.hsc.fr/ressources/articles/ipsec-tech/index.html.en

QUESTION 4

Which expert system operating mode allows determining if a given hypothesis is valid?

A. Blackboard

B. Lateral chaining

C. Forward chaining

D. Backward chaining

Correct Answer: D

Backward-chaining mode - the expert system backtracks to determine if a given hypothesis is valid. Backward-chaining is generally used when there are a large number of possible solutions relative to the number of inputs.

Incorrect answers are: In a forward-chaining mode, the expert system acquires information and comes to a conclusion based on that information. Forward-chaining is the reasoning approach that can be used when there is a small number of solutions relative to the number of inputs.

Blackboard is an expert system-reasoning methodology in which a solution is generated by the use of a virtual blackboard, wherein information or potential solutions are placed on the blackboard by a plurality of individuals or expert knowledge sources. As more information is placed on the blackboard in an iterative process, a solution is generated. Lateral-chaining mode - No such expert system mode.

Sources:

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 7: Applications and Systems Development (page 259).

KRUTZ, Ronald and VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Expert Systems (page 354).

QUESTION 5

Which of the following is not a one-way hashing algorithm?

A. MD2

B. RC4

C. SHA-1

D. HAVAL

Correct Answer: B

RC4 was designed by Ron Rivest of RSA Security in 1987. While it is officially termed "Rivest Cipher 4", the RC acronym is alternatively understood to stand for "Ron\\'s Code" (see also RC2, RC5 and RC6).

RC4 was initially a trade secret, but in September 1994 a description of it was anonymously posted to the Cypherpunks mailing list. It was soon posted on the sci.crypt newsgroup, and from there to many sites on the Internet. The leaked code was confirmed to be genuine as its output was found to match that of proprietary software using licensed RC4. Because the algorithm is known, it is no longer a trade secret. The name RC4 is trademarked, so RC4 is often referred to as ARCFOUR or ARC4 (meaning alleged RC4) to avoid trademark problems. RSA Security has never officially released the algorithm; Rivest has, however, linked to the English Wikipedia article on RC4 in his own course notes. RC4 has become part of some commonly used encryption protocols and standards, including WEP and WPA for wireless cards and TLS.

The main factors in RC4\\'s success over such a wide range of applications are its speed and simplicity: efficient implementations in both software and hardware are very easy to develop.

The following answer were not correct choices:

SHA-1 is a one-way hashing algorithms. SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard. SHA stands for "secure hash algorithm".

The three SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, and SHA-2. SHA-1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used security applications and protocols. In 2005, security flaws were identified in SHA- 1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although no successful attacks have yet been reported on the SHA-2 variants, they are algorithmically similar to SHA-1 and so efforts are underway to develop improved alternatives. A new hash standard, SHA-3, is currently under development -- an ongoing NIST hash function competition is scheduled to end with the selection of a winning function in 2012.

SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design.

MD2 is a one-way hashing algorithms. The MD2 Message-Digest Algorithm is a cryptographic hash function developed by Ronald Rivest in 1989. The algorithm is optimized for 8-bit computers. MD2 is specified in RFC 1319. Although MD2 is no longer considered secure, even as of 2010 it remains in use in public key infrastructures as part of certificates generated with MD2 and RSA.

Haval is a one-way hashing algorithms. HAVAL is a cryptographic hash function. Unlike MD5, but like most modern cryptographic hash functions, HAVAL can produce hashes of different lengths. HAVAL can produce hashes in lengths of 128 bits, 160 bits, 192 bits, 224 bits, and 256 bits. HAVAL also allows users to specify the number of rounds (3, 4, or 5) to be used to generate the hash.

The following reference(s) were used for this question: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000. and https://en.wikipedia.org/wiki/HAVAL and https://en.wikipedia.org/wiki/MD2_%28cryptography%29 and

https://en.wikipedia.org/wiki/SHA-1