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 not appropriate in addressing object reuse?

A. Degaussing magnetic tapes when they\\'re no longer needed.

B. Deleting files on disk before reusing the space.

C. Clearing memory blocks before they are allocated to a program or data.

D. Clearing buffered pages, documents, or screens from the local memory of a terminal or printer.

Correct Answer: B

Object reuse requirements, applying to systems rated TCSEC C2 and above, are used to protect files, memory, and other objects in a trusted system from being accidentally accessed by users who are not authorized to access them. Deleting files on disk merely erases file headers in a directory structure. It does not clear data from the disk surface, thus making files still recoverable. All other options involve clearing used space, preventing any unauthorized access.

Source: RUSSEL, Deborah and GANGEMI, G.T. Sr., Computer Security Basics, O\\'Reilly, July 1992 (page 119).

QUESTION 2

Why is traffic across a packet switched network difficult to monitor?

A. Packets are link encrypted by the carrier

B. Government regulations forbids monitoring

C. Packets can take multiple paths when transmitted

D. The network factor is too high

Correct Answer: C

With a packet switched network, packets are difficult to monitor because they can be transmitted using different paths. A packet-switched network is a digital communications network that groups all transmitted data, irrespective of content, type, or structure into suitably sized blocks, called packets. The network over which packets are transmitted is a shared network which routes each packet independently from all others and allocates transmission resources as needed. The principal goals of packet switching are to optimize utilization of available link capacity, minimize response times and increase the robustness of communication. When traversing network adapters, switches and other network nodes, packets are buffered and queued, resulting in variable delay and throughput, depending on the traffic load in the network. Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies. In contrast, normal telephone service is based on a circuit-switching technology, in which a dedicated line is allocated for transmission between two parties. Circuit-switching is ideal when data must be transmitted quickly and must arrive in the same order in which it\\'s sent. This is the case with most real-time data, such as live audio and video. Packet switching is more efficient and robust for data that can withstand some delays in transmission, such as e-mail messages and Web pages. All of the other answer are wrong Reference(s) used for this question: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation. and https://en.wikipedia.org/wiki/Packet-switched_network and http://www.webopedia.com/TERM/P/packet_switching.html

QUESTION 3

The Diffie-Hellman algorithm is primarily used to provide which of the following?

A. Confidentiality

B. Key Agreement

C. Integrity

D. Non-repudiation

Correct Answer: B

Diffie and Hellman describe a means for two parties to agree upon a shared secret in such a way that the secret will be unavailable to eavesdroppers. This secret may then be converted into cryptographic keying material for other (symmetric) algorithms. A large number of minor variants of this process exist. See RFC 2631 Diffie-Hellman Key Agreement Method for more details.

In 1976, Diffie and Hellman were the first to introduce the notion of public key cryptography, requiring a system allowing the exchange of secret keys over non-secure channels. The Diffie- Hellman algorithm is used for key exchange between two parties communicating with each other, it cannot be used for encrypting and decrypting messages, or digital signature.

Diffie and Hellman sought to address the issue of having to exchange keys via courier and other unsecure means. Their efforts were the FIRST asymmetric key agreement algorithm. Since the Diffie-Hellman algorithm cannot be used for encrypting and decrypting it cannot provide confidentiality nor integrity. This algorithm also does not provide for digital signature functionality and thus non-repudiation is not a choice.

NOTE: The DH algorithm is susceptible to man-in-the-middle attacks.

KEY AGREEMENT VERSUS KEY EXCHANGE

A key exchange can be done multiple way. It can be done in person, I can generate a key and then encrypt the key to get it securely to you by encrypting it with your public key. A Key Agreement protocol is done over a public medium such as the internet using a mathematical formula to come out with a common value on both sides of the communication link, without the ennemy being able to know what the common agreement is. The following answers were incorrect:

All of the other choices were not correct choices

Reference(s) used for this question:

Shon Harris, CISSP All In One (AIO), 6th edition . Chapter 7, Cryptography, Page 812.

http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

http://www.google.com/patents?vid=4200770

QUESTION 4

What key size is used by the Clipper Chip?

A. 40 bits

B. 56 bits

C. 64 bits

D. 80 bits

Correct Answer: D

The Clipper Chip is a NSA designed tamperproof chip for encrypting data and it uses the SkipJack algorithm. Each Clipper Chip has a unique serial number and a copy of the unit key is stored in the database under this serial number. The sending Clipper Chip generates and sends a Law Enforcement Access Field (LEAF) value included in the transmitted message. It is based on a 80-bit key and a 16-bit checksum.

Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 1).

QUESTION 5

Which of the following phases of a system development life-cycle is most concerned with establishing a good security policy as the foundation for design?

A. Development/acquisition

B. Implementation

C. Initiation

D. Maintenance

Correct Answer: C

A security policy is an important document to develop while designing an information system. The security policy begins with the organization\\'s basic commitment to information security formulated as a general policy statement.

The policy is then applied to all aspects of the system design or security solution. The policy identifies security goals (e.g., confidentiality, integrity, availability, accountability, and assurance) the system should support, and these goals guide the procedures, standards and controls used in the IT security architecture design. The policy also should require definition of critical assets, the perceived threat, and security-related roles and responsibilities.

Source: STONEBURNER, Gary and al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 6).