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.pass4itsure.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 a valid reason to use external penetration service firms rather than corporate resources?

A. They are more cost-effective

B. They offer a lack of corporate bias

C. They use highly talented ex-hackers

D. They ensure a more complete reporting

Correct Answer: C

Two points are important to consider when it comes to ethical hacking: integrity and independence.

By not using an ethical hacking firm that hires or subcontracts to ex-hackers of others who have criminal records, an entire subset of risks can be avoided by an organization. Also, it is not cost- effective for a single firm to fund the effort of the ongoing research and development, systems development, and maintenance that is needed to operate state-of-the-art proprietary and open source testing tools and techniques.

External penetration firms are more effective than internal penetration testers because they are not influenced by any previous system security decisions, knowledge of the current system environment, or future system security plans. Moreover, an employee performing penetration testing might be reluctant to fully report security gaps. Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Appendix F: The Case for Ethical Hacking (page 517).

QUESTION 2

Which of the following mechanisms was created to overcome the problem of collisions that occur on wired networks when traffic is simultaneously transmitted from different nodes?

A. Carrier sense multiple access with collision avoidance (CSMA/CA)

B. Carrier sense multiple access with collision detection (CSMA/CD)

C. Polling

D. Token-passing

Correct Answer: D

QUESTION 3

Which backup method copies only files that have changed since the last full backup, but does not clear the archive bit?

A. Differential backup method.

B. Full backup method.

C. Incremental backup method.

D. Tape backup method.

Correct Answer: A

One of the key item to understand regarding backup is the archive bit. The archive bit is used to determine what files have been backuped already. The archive bit is set if a file is modified or a new file is created, this indicates to the backup program that it has to be saved on the next backup. When a full backup is performed the archive bit will be cleared indicating that the files were backup. This allows backup programs to do an incremental or differential backup that only backs up the changes to the filesystem since the last time the bit was cleared

Full Backup (or Reference Backup)

A Full backup will backup all the files and folders on the drive every time you run the full backup. The

archive bit is cleared on all files indicating they were all backuped.

Advantages:

All files from the selected drives and folders are backed up to one backup set.

In the event you need to restore files, they are easily restored from the single backup set.

Disadvantages:

A full backup is more time consuming than other backup options.

Full backups require more disk, tape, or network drive space.

Incremental Backup

An incremental backup provides a backup of files that have changed or are new since the last incremental

backup.

For the first incremental backup, all files in the file set are backed up (just as in a full backup). If you use

the same file set to perform a incremental backup later, only the files that have changed are backed up. If

you use the same file set for a third backup, only the files that have changed since the second backup are

backed up, and so on.

Incremental backup will clear the archive bit.

Advantages:

Backup time is faster than full backups.

Incremental backups require less disk, tape, or network drive space.

You can keep several versions of the same files on different backup sets.

Disadvantages:

In order to restore all the files, you must have all of the incremental backups available.

It may take longer to restore a specific file since you must search more than one backup set to find the

latest version of a file.

Differential Backup

A differential backup provides a backup of files that have changed since a full backup was performed. A

differential backup typically saves only the files that are different or new since the last full backup.

Together, a full backup and a differential backup include all the files on your computer, changed and

unchanged.

Differential backup do not clear the archive bits.

Advantages:

Differential backups require even less disk, tape, or network drive space than incremental backups.

Backup time is faster than full or incremental backups.

Disadvantages:

Restoring all your files may take considerably longer since you may have to restore both the last differential and full backup.

Restoring an individual file may take longer since you have to locate the file on either the differential or full backup.

For more info see: http://support.microsoft.com/kb/136621

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 69.

QUESTION 4

In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?

A. Known-plaintext attack

B. Ciphertext-only attack

C. Chosen-Ciphertext attack

D. Plaintext-only attack

Correct Answer: B

In a ciphertext-only attack, the attacker has the ciphertext of several messages encrypted with the same encryption algorithm. Its goal is to discover the plaintext of the messages by figuring out the key used in the encryption process. In a known-plaintext attack, the attacker has the plaintext and the ciphertext of one or more messages. In a chosen-ciphertext attack, the attacker can chose the ciphertext to be decrypted and has access to the resulting plaintext.

Source: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, Chapter

8: Cryptography (page 578).

QUESTION 5

When preparing a business continuity plan, who of the following is responsible for identifying and prioritizing time-critical systems?

A. Executive management staff

B. Senior business unit management

C. BCP committee

D. Functional business units

Correct Answer: B

Many elements of a BCP will address senior management, such as the statement of importance and priorities, the statement of organizational responsibility, and the statement of urgency and timing. Executive management staff initiates the project, gives final approval and gives ongoing support. The BCP committee directs the planning, implementation, and tests processes whereas functional business units participate in implementation and testing.

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 8: Business Continuity Planning and Disaster Recovery Planning (page 275).

QUESTION 6

How many rounds are used by DES?

A. 16

B. 32

C. 64

D. 48

Correct Answer: A

DES is a block encryption algorithm using 56-bit keys and 64-bit blocks that are divided in half and each character is encrypted one at a time. The characters are put through 16 rounds of transposition and substitution functions. Triple DES uses 48 rounds.

Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 3).

QUESTION 7

Which of the following backup methods is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets?

A. full backup method.

B. incremental backup method.

C. differential backup method.

D. tape backup method.

Correct Answer: A

The Full Backup Method is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets.

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 69.

QUESTION 8

What is the role of IKE within the IPsec protocol?

A. peer authentication and key exchange

B. data encryption

C. data signature

D. enforcing quality of service

Correct Answer: A

Reference: RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand and HARKINS, Dan, Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 9

What security model is dependent on security labels?

A. Discretionary access control

B. Label-based access control

C. Mandatory access control

D. Non-discretionary access control

Correct Answer: C

With mandatory access control (MAC), the authorization of a subject\\'s access to an object is dependant upon labels, which indicate the subject\\'s clearance, and the classification or sensitivity of the object. Label-based access control is not defined.

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 2: Access control systems (page 33).

QUESTION 10

Communications devices must operate:

A. at different speeds to communicate.

B. at the same speed to communicate.

C. at varying speeds to interact.

D. at high speed to interact.

Correct Answer: B

Communications devices must operate at the same speed to communicate.

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 11

Which of the following statements pertaining to RADIUS is incorrect:

A. A RADIUS server can act as a proxy server, forwarding client requests to other authentication domains.

B. Most of RADIUS clients have a capability to query secondary RADIUS servers for redundancy.

C. Most RADIUS servers have built-in database connectivity for billing and reporting purposes.

D. Most RADIUS servers can work with DIAMETER servers.

Correct Answer: D

This is the correct answer because it is FALSE.

Diameter is an AAA protocol, AAA stands for authentication, authorization and accounting protocol for computer networks, and it is a successor to RADIUS.

The name is a pun on the RADIUS protocol, which is the predecessor (a diameter is twice the radius). The main differences are as follows:

Reliable transport protocols (TCP or SCTP, not UDP) The IETF is in the process of standardizing TCP Transport for RADIUS Network or transport layer security (IPsec or TLS) The IETF is in the process of standardizing Transport Layer Security for RADIUS Transition support for RADIUS, although Diameter is not fully compatible with RADIUS Larger address space for attribute-value pairs (AVPs) and identifiers (32 bits instead of 8 bits) Clientserver protocol, with exception of supporting some server-initiated messages as well Both stateful and stateless models can be used Dynamic discovery of peers (using DNS SRV and NAPTR) Capability negotiation Supports application layer acknowledgements, defines failover methods and state machines (RFC 3539) Error notification Better roaming support More easily extended; new commands and attributes can be defined Aligned on 32-bit boundaries Basic support for user-sessions and accounting A Diameter Application is not a software application, but a protocol based on the Diameter base protocol

(defined in RFC 3588). Each application is defined by an application identifier and can add new command codes and/or new mandatory AVPs. Adding a new optional AVP does not require a new application.

Examples of Diameter applications:

Diameter Mobile IPv4 Application (MobileIP, RFC 4004)

Diameter Network Access Server Application (NASREQ, RFC 4005)

Diameter Extensible Authentication Protocol (EAP) Application (RFC 4072)

Diameter Credit-Control Application (DCCA, RFC 4006)

Diameter Session Initiation Protocol Application (RFC 4740)

Various applications in the 3GPP IP Multimedia Subsystem

All of the other choices presented are true. So Diameter is backwork compatible with Radius (to some extent) but the opposite is false.

Reference(s) used for this question:

TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 38.

and

https://secure.wikimedia.org/wikipedia/en/wiki/Diameter_%28protocol%29

QUESTION 12

Which of the following division is defined in the TCSEC (Orange Book) as minimal protection?

A. Division D

B. Division C

C. Division B

D. Division A

Correct Answer: A

The criteria are divided into four divisions: D, C, B, and A ordered in a hierarchical manner with the highest division (A) being reserved for systems providing the most comprehensive security.

Each division represents a major improvement in the overall confidence one can place in the system for the protection of sensitive information.

Within divisions C and B there are a number of subdivisions known as classes. The classes are also ordered in a hierarchical manner with systems representative of division C and lower classes of division B being characterized by the set of computer security mechanisms that they possess. Assurance of correct and complete design and implementation

for these systems is gained mostly through testing of the security- relevant portions of the system. The security-relevant portions of a system are referred to throughout this document as the Trusted Computing Base (TCB).

Systems representative of higher classes in division B and division A derive their security attributes more from their design and implementation structure. Increased assurance that the required features are operative, correct, and tamperproof under all circumstances is gained through progressively more rigorous analysis during the design process.

TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels:

Division D - minimal security

Division C - discretionary protection

Division B - mandatory protection

Division A - verified protection

Reference: page 358 AIO V.5 Shon Harris

also

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of

Computer Security, page 197.

Also:

THE source for all TCSEC "level" questions:

http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

QUESTION 13

Which of the following answers is described as a random value used in cryptographic algorithms to ensure that patterns are not created during the encryption process?

A. IV - Initialization Vector

B. Stream Cipher

C. OTP - One Time Pad

D. Ciphertext

Correct Answer: A

The basic power in cryptography is randomness. This uncertainty is why encrypted data is unusable to someone without the key to decrypt.

Initialization Vectors are a used with encryption keys to add an extra layer of randomness to encrypted data. If no IV is used the attacker can possibly break the keyspace because of patterns resulting in the encryption process. Implementation such as DES in Code Book Mode (CBC) would allow frequency analysis attack to take place.

In cryptography, an initialization vector (IV) or starting variable (SV)is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve

semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by so-called modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.

It is define by TechTarget as:

An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.

The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding sequences in the message were also identical. The IV prevents the appearance of corresponding duplicate character sequences in the ciphertext.

The following answers are incorrect:

-Stream Cipher: This isn\\'t correct. A stream cipher is a symmetric key cipher where plaintext digits are combined with pseudorandom key stream to product cipher text.

-OTP - One Time Pad: This isn\\'t correct but OTP is made up of random values used as key material. (Encryption key) It is considered by most to be unbreakable but must be changed with a new key after it is used which makes it impractical for common use.

-Ciphertext: Sorry, incorrect answer. Ciphertext is basically text that has been encrypted with key material (Encryption key)

The following reference(s) was used to create this question:

For more details on this TOPIC and other

QUESTION 14

Which of the following is NOT a compensating measure for access violations?

A. Backups

B. Business continuity planning

C. Insurance

D. Security awareness

Correct Answer: D

Security awareness is a preventive measure, not a compensating measure for access violations.

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 2: Access control systems (page 50).

QUESTION 15

How often should a Business Continuity Plan be reviewed?

A. At least once a month

B. At least every six months

C. At least once a year

D. At least Quarterly

Correct Answer: C

As stated in SP 800-34 Rev. 1:

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies.

As a general rule, the plan should be reviewed for accuracy and completeness at an organization- defined frequency (at least once a year for the purpose of the exam) or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews.

Remember, there could be two good answers as specified above. Either once a year or whenever significant changes occur to the plan. You will of course get only one of the two presented within you

exam.

Reference(s) used for this question:

NIST SP 800-34 Revision 1