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.certbus.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 a disadvantage of a statistical anomaly-based intrusion detection system?

A. it may truly detect a non-attack event that had caused a momentary anomaly in the system.

B. it may falsely detect a non-attack event that had caused a momentary anomaly in the system.

C. it may correctly detect a non-attack event that had caused a momentary anomaly in the system.

D. it may loosely detect a non-attack event that had caused a momentary anomaly in the system.

Correct Answer: B

Some disadvantages of a statistical anomaly-based ID are that it will not detect an attack that does not significantly change the system operating characteristics, or it may falsely detect a non- attack event that had caused a momentary anomaly in the system.

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 49.

QUESTION 2

Which of the following categories of hackers poses the greatest threat?

A. Disgruntled employees

B. Student hackers

C. Criminal hackers

D. Corporate spies

Correct Answer: A

According to the authors, hackers fall in these categories, in increasing threat order: security experts, students, underemployed adults, criminal hackers, corporate spies and disgruntled employees. Disgruntled employees are the most dangerous security problem of all because they are most likely to have a good knowledge of the organization\\'s IT systems and security measures.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2: Hackers.

QUESTION 3

Which of the following encryption algorithms does not deal with discrete logarithms?

A. El Gamal

B. Diffie-Hellman

C. RSA

D. Elliptic Curve

Correct Answer: C

The security of the RSA system is based on the assumption that factoring the product into two original large prime numbers is difficult

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 159).

Shon Harris, CISSP All-in-One Examine Guide, Third Edition, McGraw-Hill Companies, August 2005, Chapter 8: Cryptography, Page 636 - 639

QUESTION 4

A group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability is:

A. server cluster

B. client cluster

C. guest cluster

D. host cluster

Correct Answer: A

A server cluster is a group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability.

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 67.

QUESTION 5

Which of the following security models does NOT concern itself with the flow of data?

A. The information flow model

B. The Biba model

C. The Bell-LaPadula model

D. The noninterference model

Correct Answer: D

The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users, By maintaining strict separation of security levels, a noninterference model minimizes

leakages that might happen through a covert channel.

The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned with confidentiality and bases access control decsions on the classfication of objects and the clearences of subjects.

The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security classes.

The Biba model is incorrect. The Biba model is concerned with integrity and is a complement to the Bell-LaPadula model in that higher levels of integrity are more trusted than lower levels. Access control us based on these integrity levels to assure that read/write operations do not decrease an object\\'s integrity.

References: CBK, pp 325 - 326 AIO3, pp. 290 - 291

QUESTION 6

What is the MOST critical piece to disaster recovery and continuity planning?

A. Security policy

B. Management support

C. Availability of backup information processing facilities

D. Staff training

Correct Answer: B

The keyword is \\' MOST CRITICAL \\' and the correct answer is \\' Management Support \\' as the management must be convinced of its necessity and that\\'s why a business case must be made. The decision of how a company should recover from any disaster is purely a business decision and should be treated as so.

The other answers are incorrect because :

Security policy is incorrect as it is not the MOST CRITICAL piece.

Availability of backup information processing facilities is incorrect as this comes once the organization has

BCP Plans in place and for a BCP Plan , management support must be there.

Staff training comes after the plans are in place with the support from management.

Reference : Shon Harris , AIO v3 , Chapter-9: Business Continuity Planning , Page : 697.

QUESTION 7

During the salvage of the Local Area Network and Servers, which of the following steps would normally be performed first?

A. Damage mitigation

B. Install LAN communications network and servers

C. Assess damage to LAN and servers

D. Recover equipment

Correct Answer: C

The first activity in every recovery plan is damage assessment, immediately followed by damage mitigation.

This first activity would typically include assessing the damage to all network and server components (including cables, boards, file servers, workstations, printers, network equipment), making a list of all items to be repaired or replaced, selecting appropriate vendors and relaying findings to Emergency Management Team.

Following damage mitigation, equipment can be recovered and LAN communications network and servers can be reinstalled.

Source: BARNES, James C. and ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley and Sons, 2001 (page 135).

QUESTION 8

Which of the following is NOT a basic component of security architecture?

A. Motherboard

B. Central Processing Unit (CPU

C. Storage Devices

D. Peripherals (input/output devices)

Correct Answer: A

The CPU, storage devices and peripherals each have specialized roles in the security archecture. The CPU, or microprocessor, is the brains behind a computer system and performs calculations as it solves problemes and performs system tasks. Storage devices provide both long- and short- term stoarge of information that the CPU has either processed or may process. Peripherals (scanners, printers, modems, etc) are devices that either input datra or receive the data output by the CPU.

The motherboard is the main circuit board of a microcomputer and contains the connectors for attaching additional boards. Typically, the motherboard contains the CPU, BIOS, memory, mass storage interfaces, serial and parallel ports, expansion slots, and all the controllers required to control standard peripheral devices.

Reference(s) used for this question:

TIPTON, Harold F., The Official (ISC)2 Guide to the CISSP CBK (2007), page 308.

QUESTION 9

Which of the following best corresponds to the type of memory addressing where the address location that is specified in the program instruction contains the address of the final desired location?

A. Direct addressing

B. Indirect addressing

C. Indexed addressing

D. Program addressing

Correct Answer: B

Indirect addressing is when the address location that is specified in the program instruction contains the address of the final desired location. Direct addressing is when a portion of primary memory is accessed by specifying the actual address of the memory location. Indexed addressing is when the contents of the address defined in the program\\'s instruction is added to that of an index register. Program addressing is not a defined memory addressing mode.

Source: WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 2).

QUESTION 10

Failure of a contingency plan is usually: A. A technical failure.

B. A management failure.

C. Because of a lack of awareness.

D. Because of a lack of training.

Correct Answer: B

Failure of a contingency plan is usually management failure to exhibit ongoing interest and concern about the BCP/DRP effort, and to provide financial and other resources as needed. Lack of management support will result in a lack awareness and training.

Source: ANDRESS, Mandy, ram CISSP, Coriolis, 2001, Chapter 9: Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) (page 163).

QUESTION 11

Which of the following binds a subject name to a public key value?

A. A public-key certificate

B. A public key infrastructure

C. A secret key infrastructure

D. A private key certificate

Correct Answer: A

Remember the term Public-Key Certificate is synonymous with Digital Certificate or Identity certificate.

The certificate itself provides the binding but it is the certificate authority who will go through the Certificate Practice Statements (CPS) actually validating the bindings and vouch for the identity of the owner of the key within the certificate.

As explained in Wikipedia:

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind together a public key with an identity -information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme such as PGP or GPG, the signature is of either the user (a self- signed certificate) or other users ("endorsements") by getting people to sign each other keys. In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.

RFC 2828 defines the certification authority (CA) as:

An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

An authority trusted by one or more users to create and assign certificates. Optionally, the certification authority may create the user\\'s keys.

X509 Certificate users depend on the validity of information provided by a certificate. Thus, a CA should be someone that certificate users trust, and usually holds an official position created and granted power by a government, a corporation, or some other organization. A CA is responsible for managing the life cycle of certificates and, depending on the type of certificate and the CPS that applies, may be responsible for the life cycle of key pairs associated with the certificates

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

and

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

QUESTION 12

In response to Access-request from a client such as a Network Access Server (NAS), which of the following is not one of the response from a RADIUS Server?

A. Access-Accept

B. Access-Reject

C. Access-Granted

D. Access-Challenge

Correct Answer: C

In response to an access-request from a client, a RADIUS server returns one of three authentication responses: access-accept, access-reject, or access-challenge, the latter being a request for additional authentication information such as a one-time password from a token or a callback identifier.

Source: TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 36.

QUESTION 13

In which of the following security models is the subject\\'s clearance compared to the object\\'s classification such that specific rules can be applied to control how the subject-to-object interactions take place?

A. Bell-LaPadula model

B. Biba model

C. Access Matrix model

D. Take-Grant model

Correct Answer: A

The Bell-LAPadula model is also called a multilevel security system because users with different clearances use the system and the system processes data with different classifications. Developed by the US Military in the 1970s.

A security model maps the abstract goals of the policy to information system terms by specifying explicit data structures and techniques necessary to enforce the security policy. A security model is usually represented in mathematics and analytical ideas, which are mapped to system specifications and then developed by programmers through programming code. So we have a policy that encompasses security goals, such as "each subject must be authenticated and authorized before accessing an object." The security model takes this requirement and provides the necessary mathematical formulas, relationships, and logic structure to be followed to accomplish this goal.

A system that employs the Bell-LaPadula model is called a multilevel security system because users with different clearances use the system, and the system processes data at different classification levels. The level at which information is classified determines the handling procedures that should be used. The Bell-LaPadula model is a state machine model that enforces the confidentiality aspects of access control. A matrix and security levels are used to determine if subjects can access different objects. The subject\\'s clearance is compared to the object\\'s classification and then specific rules are applied to control how subject-to-object subject-to- object interactions can take place.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition (p. 369). McGraw-Hill. Kindle Edition.

QUESTION 14

When submitting a passphrase for authentication, the passphrase is converted into ...

A. a virtual password by the system

B. a new passphrase by the system

C. a new passphrase by the encryption technology

D. a real password by the system which can be used forever

Correct Answer: A

Passwords can be compromised and must be protected. In the ideal case, a password should only be used once. The changing of passwords can also fall between these two extremes.

Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password\\'s frequency of use.

Obviously, the more times a password is used, the more chance there is of it being compromised.

It is recommended to use a passphrase instead of a password. A passphrase is more resistant to attacks. The passphrase is converted into a virtual password by the system. Often time the passphrase will exceed the maximum length supported by the system and it must be trucated into a Virtual Password.

Reference(s) used for this question:

http://www.itl.nist.gov/fipspubs/fip112.htm

and

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 36 and 37.

QUESTION 15

Which of the following statements is true about data encryption as a method of protecting data?

A. It should sometimes be used for password files

B. It is usually easily administered

C. It makes few demands on system resources

D. It requires careful key management

Correct Answer: D

In cryptography, you always assume the "bad guy" has the encryption algorithm (indeed, many algorithms such as DES, Triple DES, AES, etc. are public domain). What the bad guy lacks is the key used to complete that algorithm and encrypt/decrypt information. Therefore, protection of the key, controlled distribution, scheduled key change, timely destruction, and several other factors require careful consideration. All of these factors are covered under the umbrella term of "key management".

Another significant consideration is the case of "data encryption as a method of protecting data" as the question states. If that data is to be stored over a long period of time (such as on backup), you must ensure that your key management scheme stores old keys for as long as they will be needed to decrypt the information they encrypted.

The other answers are not correct because:

"It should sometimes be used for password files." - Encryption is often used to encrypt passwords stored within password files, but it is not typically effective for the password file itself. On most systems, if a user cannot access the contents of a password file, they cannot authenticate. Encrypting the entire file prevents that access.

"It is usually easily administered." - Developments over the last several years have made cryptography significantly easier to manage and administer. But it remains a significant challenge. This is not a good answer.

"It makes few demands on system resources." - Cryptography is, essentially, a large complex mathematical algorithm. In order to encrypt and decrypt information, the system must perform this algorithm hundreds, thousands, or even millions/billions/trillions of times. This becomes system resource intensive, making this a very bad answer.

Reference:

Official ISC2 Guide page: 266 (poor explanation)

All in One Third Edition page: 657 (excellent explanation)

Key Management - Page 732, All in One Fourth Edition