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.leads4pass.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

The general philosophy for DMZ\\'s is that:

A. any system on the DMZ can be compromized because it\\'s accessible from the Internet.

B. any system on the DMZ cannot be compromized because it\\'s not accessible from the Internet.

C. some systems on the DMZ can be compromized because they are accessible from the Internet.

D. any system on the DMZ cannot be compromized because it\\'s by definition 100 percent safe and not accessible from the Internet.

Correct Answer: A

Because the DMZ systems are accessible from the Internet, they are more at risk for attacka nd compromise and must be hardened appropriately.

"Any system on the DMZ cannot be compromised because it\\'s not accessible from the Internet" is incorrect. The reason a system is placed in the DMZ is so it can be accessible from the Internet.

"Some systems on the DMZ can be compromised because they are accessible from the Internet" is incorrect. All systems in the DMZ face an increased risk of attack and compromise because they are accessible from the Internet.

"Any system on the DMZ cannot be compromised because it\\'s by definition 100 percent safe and not accessible from the Internet" is incorrect. Again, a system is placed in the DMZ because it must be accessible from the Internet.

References:

CBK, p. 434

AIO3, p. 483

QUESTION 2

A periodic review of user account management should not determine:

A. Conformity with the concept of least privilege.

B. Whether active accounts are still being used.

C. Strength of user-chosen passwords.

D. Whether management authorizations are up-to-date.

Correct Answer: C

Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts;

(2) tracking users and their respective access authorizations; and (3) managing these functions.

Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up- to-date, whether required training has been

completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis.

The strength of user passwords is beyond the scope of a simple user account management review, since it requires specific tools to try and crack the password file/database through either a dictionary or brute-force attack in order to check the strength of passwords.

Reference(s) used for this question:

SWANSON, Marianne and GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 28).

QUESTION 3

Which of the following ASYMMETRIC encryption algorithms is based on the difficulty of FACTORING LARGE NUMBERS?

A. El Gamal

B. Elliptic Curve Cryptosystems (ECCs)

C. RSA

D. International Data Encryption Algorithm (IDEA)

Correct Answer: C

Named after its inventors Ron Rivest , Adi Shamir and Leonard Adleman is based on the difficulty of factoring large prime numbers.

Factoring a number means representing it as the product of prime numbers. Prime numbers, such as 2, 3, 5, 7, 11, and 13, are those numbers that are not evenly divisible by any smaller number, except 1. A non-prime, or composite number, can be written as the product of smaller primes, known as its prime factors. 665, for example is the product of the primes 5, 7, and 19. A number is said to be factored when all of its prime factors are identified. As the size of the number increases, the difficulty of factoring increases rapidly.

The other answers are incorrect because:

El Gamal is based on the discrete logarithms in a finite field.

Elliptic Curve Cryptosystems (ECCs) computes discrete logarithms of elliptic curves.

International Data Encryption Algorithm (IDEA) is a block cipher and operates on 64 bit blocks of data and is a SYMMETRIC algorithm.

Reference : Shon Harris , AIO v3 , Chapter-8 : Cryptography , Page : 638

QUESTION 4

A department manager has read access to the salaries of the employees in his/her department but not to the salaries of employees in other departments. A database security mechanism that enforces this policy would typically be said to provide which of the following?

A. Content-dependent access control

B. Context-dependent access control

C. Least privileges access control

D. Ownership-based access control

Correct Answer: A

When access control is based on the content of an object, it is considered to be content dependent access control.

Content-dependent access control is based on the content itself.

The following answers are incorrect:

context-dependent access control. Is incorrect because this type of control is based on what the context is, facts about the data rather than what the object contains. least privileges access control. Is incorrect because this is based on the least amount of rights needed to perform their jobs and not based on what is contained in the database. ownership-based access control. Is incorrect because this is based on the owner of the data and and not based on what is contained in the database.

References:

OIG CBK Access Control (page 191)

QUESTION 5

What is the primary reason why some sites choose not to implement Trivial File Transfer Protocol (TFTP)?

A. It is too complex to manage user access restrictions under TFTP

B. Due to the inherent security risks

C. It does not offer high level encryption like FTP

D. It cannot support the Lightwight Directory Access Protocol (LDAP)

Correct Answer: B

Some sites choose not to implement Trivial File Transfer Protocol (TFTP) due to the inherent security risks. TFTP is a UDP-based file transfer program that provides no security. There is no user authentication.

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 88.