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

QUESTION 1

Which of the following is not a method to protect objects and the data within the objects?

A. Layering

B. Data mining

C. Abstraction

D. Data hiding

Correct Answer: B

Data mining is used to reveal hidden relationships, patterns and trends by running queries on large data stores.

Data mining is the act of collecting and analyzing large quantities of information to determine patterns of use or behavior and use those patterns to form conclusions about past, current, or future behavior. Data mining is typically used by large organizations with large databases of customer or consumer behavior. Retail and credit companies will use data mining to identify buying patterns or trends in geographies, age groups, products, or services. Data mining is essentially the statistical analysis of general information in the absence of specific data.

The following are incorrect answers:

They are incorrect as they all apply to Protecting Objects and the data within them. Layering, abstraction and data hiding are related concepts that can work together to produce modular software that implements an organizations security policies and is more reliable in operation.

Layering is incorrect. Layering assigns specific functions to each layer and communication between layers is only possible through well-defined interfaces. This helps preclude tampering in violation of security policy. In computer programming, layering is the organization of programming into separate functional components that interact in some sequential and hierarchical way, with each layer usually having an interface only to the layer above it and the layer below it.

Abstraction is incorrect. Abstraction "hides" the particulars of how an object functions or stores information and requires the object to be manipulated through well-defined interfaces that can be designed to enforce security policy. Abstraction involves the removal of characteristics from an entity in order to easily represent its essential properties. Data hiding is incorrect. Data hiding conceals the details of information storage and manipulation within an object by only exposing well defined interfaces to the information rather than the information itslef. For example, the details of how passwords are stored could be hidden inside a password object with exposed interfaces such as check_password, set_password, etc. When a password needs to be verified, the test password is passed to the check_password method and a boolean (true/ false) result is returned to indicate if the password is correct without revealing any details of how/where the real passwords are stored. Data hiding maintains activities at different security levels to separate these levels from each other.

The following reference(s) were used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 27535-27540). Auerbach Publications. Kindle Edition.

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4269-4273). Auerbach Publications. Kindle Edition.

QUESTION 2

What is defined as the manner in which the network devices are organized to facilitate communications?

A. LAN transmission methods

B. LAN topologies

C. LAN transmission protocols

D. LAN media access methods

Correct Answer: B

A network topology defines the manner in which the network devices are organized to facilitate communications. Common LAN technologies are: bus ring star meshed LAN transmission methods refer to the way packets are sent on the network and are: unicast multicast

broadcast

LAN transmission protocols are the rules for communicating between computers on a LAN.

Common LAN transmission protocols are:

CSMA/CD polling token-passing

LAN media access methods control the use of a network (physical and data link layers). They can be: Ethernet ARCnet Token ring FDDI 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 105).

QUESTION 3

Which of the following could be BEST defined as the likelihood of a threat agent taking advantage of a vulnerability?

A. A risk

B. A residual risk

C. An exposure

D. A countermeasure

Correct Answer: A

Risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact. If a firewall has several ports open , there is a higher likelihood that an intruder will use one to access the network in an unauthorized method.

The following answers are incorrect :

Residual Risk is very different from the notion of total risk. Residual Risk would be the risks that still exists after countermeasures have been implemented. Total risk is the amount of risk a company faces if it

chooses not to implement any type of safeguard.

Exposure: An exposure is an instance of being exposed to losses from a threat agent.

Countermeasure: A countermeasure or a safeguard is put in place to mitigate the potential risk. Examples

of countermeasures include strong password management , a security guard.

REFERENCES : SHON HARRIS ALL IN ONE 3rd EDITION

Chapter - 3: Security Management Practices , Pages : 57-59

QUESTION 4

Virus scanning and content inspection of SMIME encrypted e-mail without doing any further processing is:

A. Not possible

B. Only possible with key recovery scheme of all user keys

C. It is possible only if X509 Version 3 certificates are used

D. It is possible only by "brute force" decryption

Correct Answer: A

Content security measures presumes that the content is available in cleartext on the central mail server.

Encrypted emails have to be decrypted before it can be filtered (e.g. to detect viruses), so you need the decryption key on the central "crypto mail server".

There are several ways for such key management, e.g. by message or key recovery methods. However, that would certainly require further processing in order to achieve such goal.

QUESTION 5

Which protocol is used to send email?

A. File Transfer Protocol (FTP).

B. Post Office Protocol (POP).

C. Network File System (NFS).

D. Simple Mail Transfer Protocol (SMTP).

Correct Answer: D

Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. POP is a protocol used to retrieve e-mail from a mail server. NFS is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture. FTP is the protocol that is used to facilitate file transfer between two machines.

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.