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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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.

QUESTION 2

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 3

Which of the following security-focused protocols has confidentiality services operating at a layer different from the others?

A. Secure HTTP (S-HTTP)

B. FTP Secure (FTPS)

C. Secure socket layer (SSL)

D. Sequenced Packet Exchange (SPX)

Correct Answer: A

All the previous protocols operate at the transport layer except for Secure HTTP (S-HTTP), which operates at the application layer. S-HTTP has been replaced by SSL and TLS. As it is very well explained in the Shon Harris book:

The transport layer receives data from many different applications and assembles the data into a stream to be properly transmitted over the network. The main protocols that work at this layer are TCP, UDP, Secure Sockets Layer (SSL), and Sequenced Packet Exchange (SPX).

NOTE:

Different references can place specific protocols at different layers. For example, many references place the SSL protocol in the session layer, while other references place it in the transport layer. It is not that one is right or wrong. The OSI model tries to draw boxes around reality, but some protocols straddle the different layers. SSL is made up of two protocols-- one works in the lower portion of the session layer and the other works in the transport layer.

For purposes of the CISSP exam, SSL resides in the transport layer.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One uide, 6th Edition (p. 526). McGraw-Hill. Kindle Edition.

QUESTION 4

One of these statements about the key elements of a good configuration process is NOT true

A. Accommodate the reuse of proven standards and best practices

B. Ensure that all requirements remain clear, concise, and valid

C. Control modifications to system hardware in order to prevent resource changes

D. Ensure changes, standards, and requirements are communicated promptly and precisely

Correct Answer: C

Configuration management isn\\'t about preventing change but ensuring the integrity of IT resources by preventing unauthorised or improper changes.

According to the Official ISC2 guide to the CISSP exam, a good CM process is one that can:

(1)

accommodate change;

(2)

accommodate the reuse of proven standards and best practices;

(3)

ensure that all requirements remain clear, concise, and valid;

(4)

ensure changes, standards, and requirements are communicated promptly and precisely; and

(5)

ensure that the results conform to each instance of the product.

Configuration management

Configuration management (CM) is the detailed recording and updating of information that describes an enterprise\\'s computer systems and networks, including all hardware and software components. Such information typically includes the versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. Special configuration management software is available. When a system needs a hardware or software upgrade, a computer technician can accesses the configuration management program and database to see what is currently installed. The technician can then make a more informed decision about the upgrade needed.

An advantage of a configuration management application is that the entire collection of systems can be reviewed to make sure any changes made to one system do not adversely affect any of the other systems

Configuration management is also used in software development, where it is called Unified Configuration Management (UCM). Using UCM, developers can keep track of the source code, documentation, problems, changes requested, and changes made.

Change management

In a computer system environment, change management refers to a systematic approach to keeping track of the details of the system (for example, what operating system release is running on each computer and

which fixes have been applied).

QUESTION 5

Which of the following results in the most devastating business interruptions?

A. Loss of Hardware/Software

B. Loss of Data

C. Loss of Communication Links

D. Loss of Applications

Correct Answer: B

Source: Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1.

All of the others can be replaced or repaired. Data that is lost and was not backed up, cannot be restored.