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

Domain Name Service is a distributed database system that is used to map:

A. Domain Name to IP addresses.

B. MAC addresses to domain names.

C. MAC Address to IP addresses.

D. IP addresses to MAC Addresses.

Correct Answer: A

The Domain Name Service is a distributed database system that is used to map domain names to IP addresses and IP addresses to domain names.

The Domain Name System is maintained by a distributed database system, which uses the client- server model. The nodes of this database are the name servers. Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root nameservers, the servers to query when looking up (resolving) a TLD.

Reference(s) used for this question:

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.

and

https://en.wikipedia.org/wiki/Domain_Name_System

QUESTION 2

Which of the following best defines a Computer Security Incident Response Team (CSIRT)?

A. An organization that provides a secure channel for receiving reports about suspected security incidents.

B. An organization that ensures that security incidents are reported to the authorities.

C. An organization that coordinates and supports the response to security incidents.

D. An organization that disseminates incident-related information to its constituency and other involved parties.

Correct Answer: C

RFC 2828 (Internet Security Glossary) defines a Computer Security Incident Response Team (CSIRT) as an organization that coordinates and supports the response to security incidents that involves sites within a defined constituency. This is the proper definition for the CSIRT. To be considered a CSIRT, an organization must provide a secure channel for receiving reports about suspected security incidents, provide assistance to members of its constituency in handling the incidents and disseminate incident-related information to its constituency and other involved parties. Security-related incidents do not necessarily have to be reported to the authorities.

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

QUESTION 3

Which of the following is most relevant to determining the maximum effective cost of access control?

A. the value of information that is protected

B. management\\'s perceptions regarding data importance

C. budget planning related to base versus incremental spending.

D. the cost to replace lost data

Correct Answer: A

The cost of access control must be commensurate with the value of the information that is being protected.

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 4

In which of the following phases of system development life cycle (SDLC) is contingency planning most important?

A. Initiation

B. Development/acquisition

C. Implementation

D. Operation/maintenance

Correct Answer: A

Contingency planning requirements should be considered at every phase of SDLC, but most importantly when a new IT system is being conceived. In the initiation phase, system requirements are identified and matched to their related operational processes, allowing determination of the system\\'s appropriate recovery priority.

Source: SWANSON, Marianne, and al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 12).

and

The Official ISC2 Guide to the CBK, Second Edition, Application Security, page 180-185

QUESTION 5

Which type of firewall can be used to track connectionless protocols such as UDP and RPC?

A. Stateful inspection firewalls

B. Packet filtering firewalls

C. Application level firewalls

D. Circuit level firewalls

Correct Answer: A

Packets in a stateful inspection firewall are queued and then analyzed at all OSI layers, providing a more complete inspection of the data. By examining the state and context of the incoming data packets, it helps to track the protocols that are considered "connectionless", such as UDP-based applications and Remote Procedure Calls (RPC).

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 91).