SSCP$^{\text{Q\&As}}$

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

In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?

A. Both client and server

B. The client\\'s browser

C. The web server

D. The merchant\\'s Certificate Server

Correct Answer: B

Once the merchant server has been authenticated by the browser client, the browser generates a master secret that is to be shared only between the server and client. This secret serves as a seed to generate the session (private) keys. The master secret is then encrypted with the merchant\\'s public key and sent to the server. The fact that the master secret is generated by the client\\'s browser provides the client assurance that the server is not reusing keys that would have been used in a previous session with another client. Source: ANDRESS, Mandy, ram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 112). Also: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2001, page 569.

QUESTION 2

What can be defined as an event that could cause harm to the information systems?

A. A risk

B. A threat

C. A vulnerability

D. A weakness

Correct Answer: B

A threat is an event or activity that has the potential to cause harm to the information systems. A risk is the probability that a threat will materialize. A vulnerability, or weakness, is a lack of a safeguard, which may be exploited by a threat, causing harm to the information systems.

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 1: Access Control Systems (page 32).

QUESTION 3

How should a risk be HANDLED when the cost of the countermeasure OUTWEIGHS the cost of the risk?

A. Reject the risk

B. Perform another risk analysis

C. Accept the risk

D. Reduce the risk

Correct Answer: C

Which means the company understands the level of risk it is faced.

The following answers are incorrect because :

Reject the risk is incorrect as it means ignoring the risk which is dangerous.

Perform another risk analysis is also incorrect as the existing risk analysis has already shown the results.

Reduce the risk is incorrect is applicable after implementing the countermeasures.

Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 39

QUESTION 4

What is the proper term to refer to a single unit of IP data?

A. IP segment.

B. IP datagram.

C. IP frame.

D. IP fragment.

Correct Answer: B

IP is a datagram based technology.

DIFFERENCE BETWEEN PACKETS AND DATAGRAM

As specified at: http://en.wikipedia.org/wiki/Packet_(information_technology)

In general, the term packet applies to any message formatted as a packet, while the term datagram is generally reserved for packets of an "unreliable" service.

A "reliable" service is one that notifies the user if delivery fails, while an "unreliable" one does not notify the user if delivery fails. For example, IP provides an unreliable service.

Together, TCP and IP provide a reliable service, whereas UDP and IP provide an unreliable one. All these protocols use packets, but UDP packets are generally called datagrams.

If a network does not guarantee packet delivery, then it becomes the host\\'s responsibility to provide reliability by detecting and retransmitting lost packets. Subsequent experience on the ARPANET indicated that the network itself could not reliably detect all packet delivery failures, and this pushed responsibility for error detection onto the sending host in any case. This led to the development of the end-to-end principle,

which is one of the Internet\\'s fundamental design assumptions.

The following answers are incorrect:

IP segment. Is incorrect because IP segment is a detractor, the correct terminology is TCP segment. IP is

a datagram based technology.

IP frame. Is incorrect because IP frame is a detractor, the correct terminology is Ethernet frame.

IP is a datagram based technology.

IP fragment. Is incorrect because IP fragment is a detractor.

References:

Wikipedia http://en.wikipedia.org/wiki/Internet_Protocol

QUESTION 5

Which of the following is not a DES mode of operation?

A. Cipher block chaining

B. Electronic code book

C. Input feedback

D. Cipher feedback

Correct Answer: C

Output feedback (OFB) is a DES mode of operation, not input feedback.

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 149).

QUESTION 6

Computer-generated evidence is considered:

A. Best evidence

B. Second hand evidence

C. Demonstrative evidence

D. Direct evidence

Correct Answer: B

Computer-generated evidence normally falls under the category of hearsay evidence, or second- hand evidence, because it cannot be proven accurate and reliable. Under the U.S. Federal Rules of Evidence, hearsay evidence is generally not admissible in court. Best evidence is original or primary evidence rather than a copy or duplicate of the evidence. It does not apply to computer- generated evidence. Direct evidence is oral testimony by witness. Demonstrative evidence are used to aid the jury (models, illustrations, charts).

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 9: Law, Investigation, and Ethics (page 310).

And: ROTHKE, Ben, CISSP CBK Review presentation on domain 9.

QUESTION 7

A momentary low voltage, from 1 cycle to a few seconds, is a:

A. spike

B. blackout

C. sag

D. fault

Correct Answer: C

A momentary low voltage is a sag. A synonym would be a dip. Risks to electrical power supply: POWER FAILURE Blackout: complete loss of electrical power Fault: momentary power outage POWER DEGRADATION Brownout: an intentional reduction of voltage by the power company. Sag/dip: a short period of low voltage POWER EXCESS Surge: Prolonged rise in voltage Spike: Momentary High Voltage In-rush current: the initial surge of current required by a load before it reaches normal operation.

Transient: line noise or disturbance is superimposed on the supply circuit and can cause fluctuations in

electrical power

Refence(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition (p. 462). McGraw-Hill.

Kindle Edition.

QUESTION 8

Why is Network File System (NFS) used?

A. It enables two different types of file systems to interoperate.

B. It enables two different types of file systems to share Sun applications.

C. It enables two different types of file systems to use IP/IPX.

D. It enables two different types of file systems to emulate each other.

Correct Answer: A

Network File System (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.

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 9

Which of the following Kerberos components holds all users\\' and services\\' cryptographic keys?

A. The Key Distribution Service

B. The Authentication Service

C. The Key Distribution Center

D. The Key Granting Service

Correct Answer: C

The Key Distribution Center (KDC) holds all users\\' and services\\' cryptographic keys. It provides authentication services, as well as key distribution functionality. The Authentication Service is the part of the KDC that authenticates a principal. The Key Distribution Service and Key Granting Service are distracters and are not defined Kerberos components.

Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System and Methodology (page 3)

QUESTION 10

Which of the following category of UTP cables is specified to be able to handle gigabit Ethernet (1 Gbps) according to the EIA/TIA-568-B standards?

A. Category 5e UTP

B. Category 2 UTP

C. Category 3 UTP

D. Category 1e UTP

Correct Answer: A

Categories 1 through 6 are based on the EIA/TIA-568-B standards.

On the newer wiring for LANs is CAT5e, an improved version of CAT5 which used to be outside of the standard, for more information on twisted pair, please see: twisted pair.

Category Cable Type Mhz Usage Speed

===

CAT1 UTP Analog voice, Plain Old Telephone System (POTS)

CAT2 UTP 4 Mbps on Token Ring, also used on Arcnet networks

CAT3 UTP, ScTP, STP 16 MHz 10 Mbps

CAT4 UTP, ScTP, STP 20 MHz 16 Mbps on Token Ring Networks

CAT5 UTP, ScTP, STP 100 MHz 100 Mbps on ethernet, 155 Mbps on ATM

CAT5e UTP, ScTP, STP 100 MHz 1 Gbps (out of standard version, improved version of CAT5)

CAT6 UTP, ScTP, STP 250 MHz 10 Gbps CAT7 ScTP, STP 600 M 100 Gbps Category 6 has a minumum of 250 MHz of bandwidth. Allowing 10/100/1000 use with up to 100 meter

cable length, along with 10GbE over shorter distances.

Category 6a or Augmented Category 6 has a minimum of 500 MHz of bandwidth. It is the newest standard

and allows up to 10GbE with a length up to 100m.

Category 7 is a future cabling standard that should allow for up to 100GbE over 100 meters of cable.

Expected availability is in 2013. It has not been approved as a cable standard, and anyone now selling you

Cat. 7 cable is fooling you.

REFERENCES:

http://donutey.com/ethernet.php

http://en.wikipedia.org/wiki/TIA/EIA-568-B

http://en.wikipedia.org/wiki/Category_1_cable

QUESTION 11

What is the PRIMARY goal of incident handling?

A. Successfully retrieve all evidence that can be used to prosecute

B. Improve the company\\'s ability to be prepared for threats and disasters

C. Improve the company\\'s disaster recovery plan

D. Contain and repair any damage caused by an event.

Correct Answer: D

This is the PRIMARY goal of an incident handling process.

The other answers are incorrect because :

Successfully retrieve all evidence that can be used to prosecute is more often used in identifying weaknesses than in prosecuting.

Improve the company\\'s ability to be prepared for threats and disasters is more appropriate for a disaster

recovery plan.

Improve the company\\'s disaster recovery plan is also more appropriate for disaster recovery plan.

Reference : Shon Harris AIO v3 , Chapter - 10 : Law, Investigation, and Ethics , Page : 727-728

QUESTION 12

What is a characteristic of using the Electronic Code Book mode of DES encryption?

A. A given block of plaintext and a given key will always produce the same ciphertext.

B. Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.

C. Individual characters are encoded by combining output from earlier encryption routines with plaintext.

D. The previous DES output is used as input.

Correct Answer: A

A given message and key always produce the same ciphertext.

The following answers are incorrect: Repetitive encryption obscures any repeated patterns that may have been present in the plaintext. Is incorrect because with Electronic Code Book a given 64 bit block of plaintext always produces the same ciphertext

Individual characters are encoded by combining output from earlier encryption routines with plaintext. This is incorrect because with Electronic Code Book processing 64 bits at a time until the end of the file was reached. This is a characteristic of Cipher Feedback. Cipher Feedback the ciphertext is run through a key-generating device to create the key for the next block of plaintext.

The previous DES output is used as input. Is incorrect because This is incorrect because with Electronic Code Book processing 64 bits at a time until the end of the file was reached . This is a characteristic of Cipher Block Chaining. Cipher Block Chaining uses the output from the previous block to encrypt the next block.

QUESTION 13

Which access control model achieves data integrity through well-formed transactions and separation of duties?

A. Clark-Wilson model

B. Biba model

C. Non-interference model

D. Sutherland model

Correct Answer: A

The Clark-Wilson model differs from other models that are subject- and object- oriented by introducing a third access element programs resulting in what is called an access triple, which prevents unauthorized users from modifying data or programs. The Biba model uses objects and subjects and addresses integrity based on a hierarchical lattice of integrity levels. The non- interference model is related to the information flow model with restrictions on the information flow. The Sutherland model approaches integrity by focusing on the problem of inference.

Source: ANDRESS, Mandy, ram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 12).

And: KRAUSE, Micki and TIPTON, Harold F., Handbook of Information Security Management, CRC Press, 1997, Domain 1: Access Control.

QUESTION 14

Which of the following is true about link encryption?

A. Each entity has a common key with the destination node.

B. Encrypted messages are only decrypted by the final node.

C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.

D. Only secure nodes are used in this type of transmission.

Correct Answer: C

In link encryption, each entity has keys in common with its two neighboring nodes in the transmission chain.

Thus, a node receives the encrypted message from its predecessor, decrypts it, and then re- encrypts it with a new key, common to the successor node. Obviously, this mode does not provide protection if anyone of the nodes along the transmission path is compromised.

Encryption can be performed at different communication levels, each with different types of protection and implications. Two general modes of encryption implementation are link encryption and end-to-end encryption.

Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers.

In end-to-end encryption, the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition (pp. 845-846). McGraw- Hill. And:

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 132).

QUESTION 15

How do you distinguish between a bridge and a router?

A. A bridge simply connects multiple networks, a router examines each packet to determine which network to forward it to.

B. "Bridge" and "router" are synonyms for equipment used to join two networks.

C. The bridge is a specific type of router used to connect a LAN to the global Internet.

D. The bridge connects multiple networks at the data link layer, while router connects multiple networks at the network layer.

Correct Answer: D

A bridge operates at the Data Link Layer and a router operates at the Network Layer.

The following answers are incorrect:

A bridge simply connects multiple networks, a router examines each packet to determine which network to

forward it to. Is incorrect because both forward packets this is not distinctive enough.

"Bridge" and "router" are synonyms for equipment used to join two networks. Is incorrect because the two are unique and operate at different layers of the OSI model. The bridge is a specific type of router used to connect a LAN to the global Internet. Is incorrect because a

bridge does not connect a LAN to the global internet, but connects networks together creating a LAN.

SSCP VCE Dumps SSCP Study Guide SSCP Exam Questions