Free Questions for ISSAP by certscare

Shared by Reese on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following protocols provides the highest level of VPN security with a VPN connection that uses the L2TP protocol?

Options:

A- IPSec

B- PPPoE

C- PPP

D- TFTP

Answer:

A

Explanation:

everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password.

IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP).

Answer option B is incorrect. Point to Point Protocol over Ethernet (PPPoE) is a specification for establishing PPP connections through Ethernet

network adapters. It connects users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line or cable

modem. PPPoE is described in RFC 2516.

Answer option C is incorrect. Point-to-Point Protocol (PPP) is a remote access protocol commonly used to connect to the Internet. PPP

supports compression and encryption and can be used to connect to a variety of networks. It can connect to a network running on IPX,

TCP/IP, or NetBEUI protocol. PPP supports multi-protocol and dynamic IP assignments.

Answer option D is incorrect. Trivial File Transfer Protocol (TFTP) is a file transfer protocol, with the functionality of a very basic form of File

Transfer Protocol (FTP). TFTP can be implemented in a very small amount of memory. It is useful for booting computers such as routers which

did not have any data storage devices. It is used to transfer small amounts of data between hosts on a network, such as IP phone firmware

or operating system images when a remote X Window System terminal or any other thin client boots from a network host or server. The initial

stages of some network based installation systems (such as Solaris Jumpstart, Red Hat Kickstart and Windows NT's Remote Installation

Services) use TFTP to load a basic kernel that performs the actual installation. TFTP uses UDP port 69 for communication.

Question 2

Question Type: MultipleChoice

Which of the following cryptographic algorithm uses public key and private key to encrypt or decrypt data ?

Options:

A- Asymmetric

B- Hashing

C- Numeric

D- Symmetric

Answer:

A

Question 3

Question Type: MultipleChoice

You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement? Each correct answer represents a complete solution. Choose two.

Options:

A- MAC filtering the router

B- Not broadcasting SSID

C- Using WEP encryption

D- Using WPA encryption

Answer:

C, D

Explanation:

like). So this won't be an inconvenience for customers.

Question 4

Question Type: MultipleChoice

You are the administrator for YupNo.com. You want to increase and enhance the security of your computers and simplify deployment. You are especially concerned with any portable computers that are used by remote employees. What can you use to increase security, while still allowing your users to perform critical tasks?

Options:

A- BitLocker

B- Smart Cards

C- Service Accounts

D- AppLocker

Answer:

B

Explanation:

Smart Cards.

Answer options D and A are incorrect. AppLocker and BitLocker might help enhance the security of the company computers, but they will not

simplify deployment.

Answer option C is incorrect. Service Accounts would not enhance security or simplify deployment. They are used to enable applications to run

as a local service or local system.

Question 5

Question Type: MultipleChoice

In which of the following phases of the SDLC does the software and other components of the system faithfully incorporate the design specifications and provide proper documentation and training?

Options:

A- Initiation

B- Programming and training

C- Design

D- Evaluation and acceptance

Answer:

B

Explanation:

specifications, and proper documentation and training are provided.

Answer option A is incorrect. During the initiation phase, the need for a system is expressed and the purpose of the system is documented.

Answer option C is incorrect. During the design phase, systems requirements are incorporated into design. This phase specifies to include

controls that support the auditing of the system.

Answer option D is incorrect. During the evaluation and acceptance phase, the system and data are validated, all the control requirements

and the user requirements are met by the system.

Question 6

Question Type: MultipleChoice

Sonya, a user, reports that she works in an electrically unstable environment where brownouts are a regular occurrence. Which of the following will you tell her to use to protect her computer?

Options:

A- UPS

B- Multimeter

C- SMPS

D- CMOS battery

Answer:

A

Explanation:

failure occurs, the UPS is switched to the battery provided inside the device. It is used with computers, as power failure can cause loss of

data, which has not been saved by a user.

Answer option C is incorrect. Switch Mode Power Supply (SMPS) is a device that converts raw input power to controlled voltage and current for

the operation of electronic equipment. SMPS uses switches for high efficiency.

Answer option D is incorrect. Complimentary Metal Oxide Semiconductor (CMOS) is a chip installed on the motherboard, which stores the

hardware configuration of a computer.

Question 7

Question Type: **MultipleChoice**

Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using?

Options:

A- Risk acceptance

B- Risk avoidance

C- Risk transfer

D- Risk mitigation

Answer:

C

Explanation:

policy providing various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc., it means

it has transferred its security risks to the insurance company.

Answer option B is incorrect. Risk avoidance is the practice of not performing an activity that could carry risk. Avoidance may seem the answer

to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed.

Answer option D is incorrect. Risk mitigation is the practice of reducing the severity of the loss or the likelihood of the loss from occurring.

Answer option A is incorrect. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also

weigh the cost versus the benefit of dealing with the risk in another way.

Question 8

Question Type: MultipleChoice

Which of the following encryption modes has the property to allow many error correcting codes to function normally even when applied before encryption?

Options:

A- OFB mode

B- CFB mode

C- CBC mode

D- PCBC mode

Answer:

A

Explanation:

XORed with the plaintext blocks to get the ciphertext. With other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the

plaintext at the same location. This property allows many error correcting codes to function normally even when applied before encryption.

Answer option C is incorrect. In the cipher-block chaining (CBC) mode, each block of plaintext is XORed with the previous ciphertext block

before being encrypted.

Answer option D is incorrect. The propagating cipher-block chaining or plaintext cipher-block chaining (PCBC) mode is designed to cause small

changes in the ciphertext to propagate indefinitely when decrypting, as well as when encrypting.

Answer option B is incorrect. The cipher feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream

cipher.

Question 9

Question Type: MultipleChoice

Which of the following are the goals of a public key infrastructure (PKI)?

Each correct answer represents a part of the solution. Choose all that apply.

Options:

A- Authenticity

B- Globalization

C- Mobility

D- Integrity

E- Confidentiality

F- Nonrepudiation

Answer:

A, D, E, F

Explanation:

Confidentiality: A PKI encrypts stored or transmitted data.

Integrity: A PKI digitally signs the data. A digital signature can identify whether the data is modified by another user or not.

Authenticity: A PKI uses several authentication methods to authenticate the users. Authentication data produces a message digest by passing through hash algorithms. The message digest is digitally signed by using the sender's private key to verify that this message digest is produced by the sender.

Nonrepudiation: The digital signature of the data offers a way to proof the integrity and origin of the data. A third party can verify this integrity and origin of the data at any time. The owner of the certificate cannot disprove this verification.

Answer options C and B are incorrect. These are not the goals of a public key infrastructure.