Question #1 *Topic 1*

Which of the following elements of planning gap measures the gap between the total potential for the market and the actual current usage by all the consumers in the market?

A. Project gap

B. Product gap

C. Competitive gap

D. Usage gap

Suggested Answer: *D*

Community vote distribution

D (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: D

D. Usage Gap

The usage gap measures the difference between the potential of a product or service and its actual use by customers. It represents the gap between what is possible in theory versus what is actually happening in practice. In this case, it refers to the difference between the total potential for a market and the current utilization by its consumers. The other options (project gap, product gap, competitive gap) are different types of gaps related to planning but do not relate specifically to this scenario.

upvoted 1 times

74gjd_37 1 year, 3 months ago

The term "usage gap" is not specific to any particular standard or framework. It is a widely used business and marketing term that describes the difference between potential market demand (based on factors such as market size, target audience, and available resources) and actual usage or consumption of products or services by customers. The concept has been discussed and explored in literature across multiple disciplines such as business strategy, marketing research, economics, and others. Therefore there is no single person who can be attributed to inventing or working on this terminology.

upvoted 1 times

jim22444 1 year, 6 months ago

Selected Answer: D

Sadly not a single question is close to what you will see on this...

upvoted 3 times

Question #2 *Topic 1*

Which of the following terms refers to the method that allows or restricts specific types of packets from crossing over the firewall?

A. Hacking

B. Packet filtering

C. Web caching

D. Spoofing

Suggested Answer: *B*

Community vote distribution

B (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: B

B.Packet filtering

Packet filtering is the process of examining each packet that passes through a firewall and determining whether it should be allowed or denied based on a set of predefined rules. It involves analyzing the characteristics of each packet, such as source and destination IP addresses, ports, and protocols, to make decisions on whether to permit or block them.

Packet filtering is one of the fundamental methods used to control network traffic and enforce security policies. It is an essential component of a firewall's functionality and helps in preventing unauthorized access to a network by allowing or restricting specific types of packets.

upvoted 1 times

Banzaaai 2 years, 4 months ago

Selected Answer: B

B. Packet filtering

upvoted 1 times

Question #3 *Topic 1*

You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e-mails. Which of the following will you use to accomplish this?

A. PGP

B. PPTP

C. IPSec

D. NTFS

Suggested Answer: *A*

Community vote distribution

A (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: A

A. PGP

PGP (Pretty Good Privacy) is a widely recognized and highly secure encryption protocol that is commonly used for securing email communications. It provides end-to-end encryption, which means that the message is encrypted at the sender's end and can only be decrypted by the intended recipient using their private key.

upvoted 1 times

74gjd_37 1 year, 3 months ago

Other options are not for email protection.

PPTP (Point-to-Point Tunneling Protocol) is primarily used for creating virtual private network (VPN) connections, but it does not provide built-in email encryption capabilities. It encapsulates data within an encrypted tunnel, but this encryption is meant to protect the integrity of transmitted data rather than specifically encrypting email contents.

IPSec (Internet Protocol Security) is also commonly used for VPNs and offers strong security features. However, it operates at the network layer rather than the application layer where emails reside. Although it can be configured to encrypt email traffic between networks or systems, implementing IPSec solely for email encryption may require additional configuration and setup.

NTFS (New Technology File System), on the other hand, is a file system used in Windows operating systems for organizing and storing files on disk drives. NTFS does not have native capabilities for encrypting emails.

upvoted 1 times

Question #4 *Topic 1*

Peter works as a Network Administrator for Net World Inc. The company wants to allow remote users to connect and access its private network through a dial-up connection via the Internet. All the data will be sent across a public network. For security reasons, the management wants the data sent through the Internet to be encrypted. The company plans to use a Layer 2 Tunneling Protocol (L2TP) connection. Which communication protocol will Peter use to accomplish the task?

A. IP Security (IPSec)

B. Microsoft Point-to-Point Encryption (MPPE)

C. Pretty Good Privacy (PGP)

D. Data Encryption Standard (DES)

Suggested Answer: *A*

Community vote distribution

A (100%)

Jay05 7 months ago

Selected Answer: A

A. IPSec. Question doesn't say that the encryption protocol needs to be a layer 2 protocol. It simply says a layer 2 protocol L2TP is used (for tunnel creation).

upvoted 1 times

n00r1 1 year, 6 months ago

ChatGPT

B. Microsoft Point-to-Point Encryption (MPPE)

Explanation:

Layer 2 Tunneling Protocol (L2TP) is often used in conjunction with Microsoft Point-to-Point Encryption (MPPE) for creating secure virtual private network (VPN) connections. MPPE is a protocol that provides encryption for the data sent over the L2TP connection, ensuring the confidentiality and security of the communication.

This is a trick question. Layer 2 is the key word. IPSec is layer 3.

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: A

A. IPSec

upvoted 1 times

74gjd_37 1 year, 9 months ago

A. IPSec

Peter will use IP Security (IPSec) to accomplish the task because IPSec provides a framework for securing IP communications and ensuring confidentiality, integrity, and authenticity of data transmitted across a public network. It offers encryption capabilities that can be used to encrypt data sent through the Internet. By implementing IPSec with L2TP, Peter can establish secure tunneling for remote users connecting to the private network of Net World Inc., thereby protecting sensitive information from unauthorized access or interception.

upvoted 1 times

74gjd_37 1 year, 9 months ago

PSec can be well integrated with L2TP to provide a secure solution for remote user access. In fact, the combination of L2TP and IPSec is commonly used together to create Virtual Private Network (VPN) connections.

L2TP establishes the tunnel between the remote user's device and the private network over which data will be transmitted. It creates a virtual connection encapsulated within IP packets.

IPSec, on the other hand, provides encryption and authentication for these IP packets transmitted through the public network. It adds an extra

layer of security by encrypting the payload of each packet using cryptographic algorithms.

By combining L2TP with IPSec, Peter can ensure that all communications between remote users' devices and Net World Inc.'s private network are protected from eavesdropping or tampering. The use of IPSec enhances confidentiality, integrity, and authenticity while leveraging L2TP for tunneling purposes.

upvoted 1 times

Question #5 *Topic 1*

Which of the following protocols multicasts messages and information among all member devices in an IP multicast group?

A. ARP

B. ICMP

C. TCP

D. IGMP

Suggested Answer: *D*

Community vote distribution

D (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: D

The correct answer is D. IGMP (Internet Group Management Protocol). IGMP is a protocol used by IP hosts to report their multicast group memberships to any neighboring multicast routers. It allows devices to join and leave specific multicast groups, ensuring that only interested members receive the multicast traffic.

upvoted 1 times

74gjd_37 1 year, 3 months ago

ICMP (Internet Control Message Protocol) and ARP (Address Resolution Protocol) are not the correct options because they do not multicast messages and information among all member devices in an IP multicast group.

ICMP is primarily used for diagnostic and error reporting purposes. It is typically used by network devices to send error messages or control packets to other network devices. While ICMP can be used for multicasting in some cases, its primary function is not related to multicasting.

ARP, on the other hand, is a protocol used for resolving IP addresses to MAC addresses in a local area network (LAN). It allows devices on a LAN to map an IP address of another device to its corresponding MAC address. ARP operates at the link layer of the TCP/IP model and does not specifically deal with multicasting functionality.

upvoted 1 times

Question #6 *Topic 1*

Which of the following security devices is presented to indicate some feat of service, a special accomplishment, a symbol of authority granted by taking an oath, a sign of legitimate employment or student status, or as a simple means of identification?

A. Sensor

B. Alarm

C. Motion detector

D. Badge

Suggested Answer: *D*

Community vote distribution

D (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: D

D. Badge. A badge is a security device that is presented to indicate some feat of service, a special accomplishment, a symbol of authority granted by taking an oath, or as a sign of legitimate employment or student status. It serves as a means of identification and can represent different levels of access privileges within an organization. Sensors, alarms, and motion detectors are not typically used for identification purposes but rather for detecting and alerting in case of security breaches or unauthorized activities.

upvoted 1 times

Question #7 *Topic 1*

Which of the following is a method for transforming a message into a masked form, together with a way of undoing the transformation to recover the message?

A. Cipher

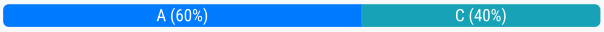
B. CrypTool

C. Steganography

D. MIME

Suggested Answer: *A*

Community vote distribution



byfener 1 year, 6 months ago

Selected Answer: A

The question specifically asked about a method for transforming a message into a masked form, together with a way of undoing the transformation to recover the message. While steganography is a method of hiding information within other non-secret data (such as embedding information in an image or audio file), it typically does not involve a reversible transformation like a cipher.

Steganography focuses on concealing the existence of information rather than encrypting it. The goal is to hide the fact that there is a secret message, not necessarily to make the message itself unintelligible without the proper key or method.

On the other hand, ciphers, as mentioned earlier, involve reversible transformations. They take plaintext, apply an encryption algorithm, and produce ciphertext, and this process can be reversed with the appropriate key or algorithm to recover the original plaintext. That's why the correct answer to the question is A. Cipher.

upvoted 2 times

byfener 1 year, 6 months ago

Selected Answer: A

A. Cipher

A cipher is a method for transforming a message into a masked form, and it also includes a way to reverse or undo the transformation to recover the original message.

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: C

C. Steganography is a method for transforming a message into a masked form and also includes a way of undoing the transformation to recover the message. Steganography involves hiding information within other innocuous data or media (such as images, audio files, or video) in order to conceal its existence.

upvoted 1 times

Banzaaai 2 years, 10 months ago

Selected Answer: C

C. Steganography

upvoted 1 times

Question #8 *Topic 1*

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

A. Policy Access Control

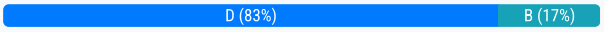
B. Mandatory Access Control

C. Discretionary Access Control

D. Role-Based Access Control

Suggested Answer: *D*

Community vote distribution



byfener 1 year, 6 months ago

Selected Answer: D

D. Role-Based Access Control

Role-Based Access Control (RBAC) is an access control model that allows access permissions to be assigned based on roles. In RBAC, users are assigned specific roles, and each role has certain permissions associated with it. This model is effective for managing access to resources by ensuring that users have the necessary permissions based on their roles within an organization.

Option C, Discretionary Access Control (DAC), also allows users to have control over their own objects and resources, but RBAC is more specifically focused on assigning permissions based on roles rather than individual discretion.

So, in the context of Mark wanting users to access only the resources required for their roles, the most appropriate choice is D. Role-Based Access Control.

upvoted 2 times

74gjd_37 1 year, 9 months ago

Selected Answer: D

D. RBAC

RBAC is a widely-accepted access control model that assigns permissions to users based on their roles within an organization. It allows administrators to define various roles and assign appropriate privileges and access rights to each role. Users are then assigned specific roles, which determine the actions they can perform and the resources they can access.

This approach aligns with Mark's objective of granting users only the necessary resources for their job functions while ensuring consistent enforcement of security policies across the network infrastructure.

In a mandatory access control model, security labels or classifications are assigned to both subjects (users/processes) and objects (resources). These labels determine the level of access that subjects can have to specific resources. The enforcement of access controls in MAC is typically based on pre-defined system-wide policies.

On the other hand, RBAC allows administrators to assign permissions and privileges based on roles rather than individual security labels. Users are then assigned specific roles which grant them appropriate levels of access based on their job functions within the organization.

upvoted 1 times

jim22444 2 years, 1 month ago

Selected Answer: B

I would go with B since he doesn't bring up anything related to his duties but just specifies that he only wants users to access what is required... Sounds more granular thatn RBAC

upvoted 1 times

jim22444 2 years, 1 month ago

Didn't notice the "them" in assigning permissions. I would go with RBAC. D

upvoted 2 times

74gjd_37 1 year, 9 months ago

Option B is incorrect because Mandatory Access Control (MAC) is typically associated with controlling access to documents or information rather than resources in general.

In a MAC model, subjects and objects are given security labels that represent their classification level or sensitivity. These labels determine the level of access and interactions that subjects can have with specific documents or information based on predefined system-wide policies.

This type of access control model is commonly used in environments where data confidentiality and integrity are critical, such as government agencies or organizations handling sensitive information.

In the context of Mark wanting users to only access necessary resources, MAC would not be directly applicable since it primarily focuses on controlling access to classified documents rather than broader resource management.

upvoted 1 times

Banzaaai 2 years, 10 months ago

Selected Answer: D

D. Role-Based Access Control

only for role

upvoted 2 times

Question #9 *Topic 1*

Which of the following is used to authenticate asymmetric keys?

A. Digital signature

B. MAC Address

C. Demilitarized zone (DMZ)

D. Password

Suggested Answer: *A*

Community vote distribution

A (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: A

The correct answer is A. Digital signature.

Digital signatures are used to authenticate asymmetric keys. They provide a means to verify the authenticity and integrity of messages or documents by using a cryptographic algorithm that uses both private and public keys. The digital signature ensures that the message has not been tampered with during transmission and that it was indeed sent by the claimed sender.

upvoted 2 times

Question #10 *Topic 1*

IPsec VPN provides a high degree of data privacy by establishing trust points between communicating devices and data encryption. Which of the following encryption methods does IPsec VPN use? Each correct answer represents a complete solution. Choose two.

A. MD5

B. LEAP

C. AES

D. 3DES

Suggested Answer: *DC*

Community vote distribution

CD (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: CD

C. AES

D. 3DES

LEAP (Lightweight Extensible Authentication Protocol) is not related to encryption.

upvoted 1 times

Question #11 *Topic 1*

A user is sending a large number of protocol packets to a network in order to saturate its resources and to disrupt connections to prevent communications between services. Which type of attack is this?

A. Denial-of-Service attack

B. Vulnerability attack

C. Social Engineering attack

D. Impersonation attack

Suggested Answer: *A*

Community vote distribution

A (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: A

A. Denial-of-Service attack

upvoted 1 times

Question #12 *Topic 1*

Which of the following types of firewall functions at the Session layer of OSI model?

A. Circuit-level firewall

B. Application-level firewall

C. Packet filtering firewall

D. Switch-level firewall

Suggested Answer: *A*

Community vote distribution

A (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: A

https://www.datamation.com/networks/circuit-level-gateways-definition-features-examples/

A circuit-level gateway is a type of firewall that operates on layer 5 of the Open Systems Interconnection (OSI) model, which is the session layer. It's the layer responsible for providing the mechanism of initiating, managing, and closing a communication session between end-user application processes.

upvoted 1 times

74gjd_37 1 year, 3 months ago

A circuit-level firewall is also known as a transparent proxy firewall. A transparent proxy firewall does not modify the request or response beyond what is required for proxy authentication and identification.

An example of a transparent proxy firewall is SOCKS (SOCKS proxy), which operates at the Session layer and allows clients to securely connect to remote servers through an intermediary server.

upvoted 1 times

74gjd_37 1 year, 3 months ago

SOCKS stands for "SOCKet Secure" and is a type of proxy protocol commonly used for routing network traffic through a firewall or proxy server. It allows clients to establish connections to servers via the intermediary server (proxy) without revealing their own IP addresses.

upvoted 1 times

Question #13 *Topic 1*

Which of the following statements about a stream cipher are true? Each correct answer represents a complete solution. Choose three.

A. It typically executes at a higher speed than a block cipher.

B. It divides a message into blocks for processing.

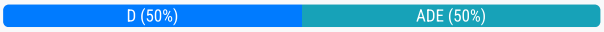
C. It typically executes at a slower speed than a block cipher.

D. It divides a message into bits for processing.

E. It is a symmetric key cipher.

Suggested Answer: *ADE*

Community vote distribution



bobby_kl 1 year, 2 months ago

Selected Answer: ADE

correct are A, D, and E

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: D

D.

it divides bits

upvoted 1 times

Question #14 *Topic 1*

Which of the following types of attack can be used to break the best physical and logical security mechanism to gain access to a system?

A. Social engineering attack

B. Cross site scripting attack

C. Mail bombing

D. Password guessing attack

Suggested Answer: *A*

Community vote distribution

A (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: A

A. Social engineering attack

The type of attack that can be used to break the best physical and logical security mechanism to gain access to a system is a social engineering attack. This type of attack involves manipulating individuals into divulging sensitive information or gaining unauthorized access by exploiting human vulnerabilities rather than technical vulnerabilities.

upvoted 1 times

Question #15 *Topic 1*

You are the Security Consultant advising a company on security methods. This is a highly secure location that deals with sensitive national defense related data.
They are very concerned about physical security as they had a breach last month. In that breach an individual had simply grabbed a laptop and ran out of the building. Which one of the following would have been most effective in preventing this?

A. Not using laptops.

B. Keeping all doors locked with a guard.

C. Using a man-trap.

D. A sign in log.

Suggested Answer: *C*

Community vote distribution

C (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: C

From an ISC2 CISS-ISSAP perspective, the most effective measure to prevent a similar breach in the scenario described would be option C - Using a man-trap.

A man-trap is a physical security measure that consists of two interlocking doors or gates. It allows only one person at a time into a restricted area, ensuring that unauthorized individuals cannot enter. In this case, if the laptop thief had encountered a man-trap at the exit, it would have prevented them from leaving with the stolen laptop.

upvoted 1 times

74gjd_37 1 year, 3 months ago

Option A - Not using laptops may not be feasible as laptops are often necessary for productivity and mobility purposes.

Option B - Keeping all doors locked with a guard could help increase physical security; however, it may still allow unauthorized individuals to gain access if they manage to get past or distract the guard.

Option D - A sign-in log alone does not provide any physical deterrent or preventive measures. Although it can assist with identifying who was present during certain incidents, it would not actively prevent someone from stealing equipment like in this scenario.

upvoted 1 times

Question #16 *Topic 1*

You want to implement a network topology that provides the best balance for regional topologies in terms of the number of virtual circuits, redundancy, and performance while establishing a WAN network. Which of the following network topologies will you use to accomplish the task?

A. Bus topology

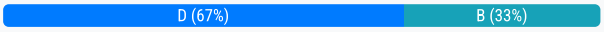
B. Fully meshed topology

C. Star topology

D. Partially meshed topology

Suggested Answer: *D*

Community vote distribution



byfener 1 year, 6 months ago

Selected Answer: B

Answer is more likely:
B. Fully meshed topology

A partially meshed topology involves connecting some, but not all, nodes in the network to each other. While this can be a valid choice in certain scenarios, it may not provide the best balance for regional topologies in terms of redundancy and performance.

In a partially meshed topology, there may be some nodes that are not directly connected to each other, leading to a lower level of redundancy compared to a fully meshed topology. Redundancy is crucial for network resilience, and a partially meshed topology might not offer as many alternate paths in case of link failures.

For a WAN network where the goal is to achieve a balance between the number of virtual circuits, redundancy, and performance, a fully meshed topology is often preferred because it maximizes redundancy and allows for efficient communication between nodes.

In summary, while a partially meshed topology might be suitable in certain situations, a fully meshed topology is typically more aligned with the requirements stated in the question.

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: D

In terms of achieving a balance in the number of virtual circuits between regional topologies, a partially meshed topology could be a valid choice.

A partially meshed topology involves selectively connecting certain sites with direct links while allowing others to connect through intermediate nodes or hubs. This approach provides flexibility in designing the network based on requirements such as traffic patterns or site importance.

By choosing specific connections strategically, you can control the number of virtual circuits established within each regional topology. This flexibility enables you to optimize resources and manage costs efficiently. It also allows for easier scalability since new connections can be added as needed without having to establish direct links for all locations.

Therefore, if your primary consideration is achieving balance in terms of the number of virtual circuits among regional topologies, selecting Option D - Partially Meshed Topology would indeed be appropriate.

upvoted 1 times

Banzaaai 2 years, 10 months ago

Selected Answer: D

D. Partially meshed topology

upvoted 1 times

Question #17 *Topic 1*

Which of the following protocols is an alternative to certificate revocation lists (CRL) and allows the authenticity of a certificate to be immediately verified?

A. RSTP

B. SKIP

C. OCSP

D. HTTP

Suggested Answer: *C*

Community vote distribution

C (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: C

C. OCSP

upvoted 1 times

74gjd_37 1 year, 3 months ago

OCSP is a real-time revocation checking mechanism that addresses some of the limitations of using CRLs. Unlike CRLs, which are static lists containing revoked certificates and need to be periodically updated on client systems, OCSP provides more timely information by allowing clients to query a central server called an OCSP responder.

upvoted 1 times

Banzaaai 2 years, 4 months ago

Selected Answer: C

C. OCSP

upvoted 2 times

Question #18 *Topic 1*

Which of the following does PEAP use to authenticate the user inside an encrypted tunnel? Each correct answer represents a complete solution. Choose two.

A. GTC

B. MS-CHAP v2

C. AES

D. RC4

Suggested Answer: *BA*

Community vote distribution

AB (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: AB

A. GTC (Generic Token Card)

B. MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol version 2)

upvoted 1 times

74gjd_37 1 year, 3 months ago

MS-CHAP v2: Developed by Microsoft, MS-CHAP v2 is another widely used challenge-response protocol suitable for authenticating clients within a secured environment like PEAP.

upvoted 1 times

74gjd_37 1 year, 3 months ago

GTC is an example of a one-time password-based protocol that allows users to enter their login credentials, including username and password combination for verification during the authentication process.

upvoted 1 times

Banzaaai 2 years, 4 months ago

Selected Answer: AB

EAP Generic Token Card (EAP-GTC) — The PEAP-GTC authentication mechanism allows generic authentication

upvoted 1 times

Question #19 *Topic 1*

Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

A. Integrity

B. Confidentiality

C. Authentication

D. Non-repudiation

Suggested Answer: *D*

Community vote distribution

D (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: D

D. Non-repudiation

Authentication is not incorrect in the context of proving that the sender really sent a particular message, but it may not be the most precise answer.

Authentication does play a crucial role in verifying the identity of a sender, ensuring that they are who they claim to be. However, authentication alone does not provide explicit evidence or mechanisms to prove that a specific message was sent by a particular sender.

While authentication establishes trust and confirms the identity of individuals or systems involved in communication, non-repudiation provides proof and assurance regarding actions performed by those authenticated entities.

Non-repudiation mechanisms like digital signatures can link an individual's identity to specific messages or data, making it difficult for them to deny their involvement later on. These mechanisms offer legal liability protection by providing evidence that proves both message integrity and origin.

upvoted 1 times

Question #20 *Topic 1*

Adam works as a Security Analyst for Umbrella Inc. CEO of the company ordered him to implement two-factor authentication for the employees to access their networks. He has told him that he would like to use some type of hardware device in tandem with a security or identifying pin number. Adam decides to implement smart cards but they are not cost effective. Which of the following types of hardware devices will Adam use to implement two-factor authentication?

A. Biometric device

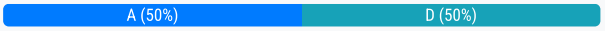
B. One Time Password

C. Proximity cards

D. Security token

Suggested Answer: *D*

Community vote distribution



mbombom 19 hours, 29 minutes ago

Selected Answer: D

These devices: Are cheaper than smart cards
Work with a PIN + token-generated code
Are widely used for 2FA

upvoted 1 times

FilipNel 1 year, 2 months ago

Biometric devices are indeed a form of two-factor authentication (something you are), but they are typically more costly than other options like security tokens and might not align with the CEO's directive for a hardware device paired with a PIN. Biometrics often don't use PINs as a second factor but instead rely on physical characteristics. Correct answer is D: Security Token.

upvoted 1 times

Banzaaai 3 years, 4 months ago

Selected Answer: D

D. Security token

upvoted 1 times

aosroyal 3 years, 9 months ago

Selected Answer: A

Saw the qn in exam today. Answer is A

upvoted 1 times

Stevey 3 years, 5 months ago

I believe the answer is D. Security Token. Why would it be "A. Biometric Device" if smart cards were not cost effective. Biometrics would be much more expensive.

upvoted 2 times

Question #21 *Topic 1*

Maria works as a Network Security Officer for Gentech Inc. She wants to encrypt her network traffic. The specific requirement for the encryption algorithm is that it must be a symmetric key block cipher. Which of the following techniques will she use to fulfill this requirement?

A. IDEA

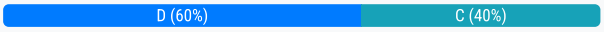
B. PGP

C. DES

D. AES

Suggested Answer: *D*

Community vote distribution



1ecb475 1 year, 1 month ago

the answer should be AES - "D"

upvoted 1 times

74gjd_37 1 year, 9 months ago

ACD is the correct answer

upvoted 1 times

Geddy1ng 2 years, 4 months ago

correct answers should be A,C,D as they all are symmetric block clippers, if need to be chosen one - D is the best answer.

upvoted 2 times

Geddy1ng 2 years, 7 months ago

Selected Answer: D

the answer should be AES - "D"

upvoted 1 times

Geddy1ng 2 years, 7 months ago

I am fully agree that answer should be "D"

upvoted 1 times

resortwri 2 years, 8 months ago

Selected Answer: D

AES is a symmetric block cypher and is stronger than DES.

upvoted 2 times

Banzaaai 2 years, 10 months ago

Selected Answer: C

C. DES

only

upvoted 2 times

Question #22 *Topic 1*

Which of the following protocols uses public-key cryptography to authenticate the remote computer?

A. SSH

B. Telnet

C. SCP

D. SSL

Suggested Answer: *A*

Community vote distribution

A (100%)

74gjd_37 1 year, 3 months ago

Valid replies are both A. (SSH) and D. (SSL)

In SSL, public-key cryptography is used to authenticate the remote computer by having the server present its digital certificate containing its public key during the handshake process. The client verifies this certificate using trusted certification authorities (CAs) to ensure the authenticity and integrity of the remote computer.

In SSH, the client keeps a digest of the last used public key of the remote computer and compares it during subsequent connections to ensure authenticity. Therefore, both SSL and SSH utilize public-key cryptography for authenticating the remote computer in different contexts.

upvoted 2 times

Banzaaai 2 years, 4 months ago

Selected Answer: A

to REMOTE computer, therefore A. SSH

upvoted 1 times

Guest4768 4 years, 8 months ago

C and D also uses public key authentication. Is the question really correct?

upvoted 1 times

Question #23 *Topic 1*

Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

A. Authentication

B. Non-repudiation

C. Integrity

D. Confidentiality

Suggested Answer: *D*

Community vote distribution

D (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: D

D. Confidentiality

upvoted 1 times

Question #24 *Topic 1*

Which of the following are the examples of technical controls? Each correct answer represents a complete solution. Choose three.

A. Auditing

B. Network acchitecture

C. System access

D. Data backups

Suggested Answer: *BCA*

Community vote distribution

BCD (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: BCD

B. Network architecture - This includes designing and implementing secure network configurations, firewalls, routers, intrusion detection systems (IDS), etc.

C. System access - This involves implementing mechanisms like authentication methods, multi-factor authentication (MFA), access control lists (ACLs), role-based access control (RBAC), and other measures to enforce proper system access management.

D. Data backups - Implementing regular data backup procedures along with appropriate storage and recovery mechanisms to ensure data integrity and availability in case of incidents or disasters.

upvoted 3 times

sbradford10 1 year, 6 months ago

i agree, auditing is not a technical control

upvoted 2 times

Banzaaai 2 years, 4 months ago

why auditing is technical control??

upvoted 3 times

Question #25 *Topic 1*

Which of the following tenets does the CIA triad provide for which security practices are measured? Each correct answer represents a part of the solution. Choose all that apply.

A. Integrity

B. Accountability

C. Availability

D. Confidentiality

Suggested Answer: *DAC*

Community vote distribution

ACD (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: ACD

The correct answers regarding which tenets are covered by the CIA triad are:

A. Integrity - Ensuring that data is accurate, complete, and protected from unauthorized modification.

C. Availability - Ensuring that information and systems are accessible and usable when needed by authorized users.

D. Confidentiality - Protecting sensitive information from unauthorized disclosure or access.

Therefore, the correct answers are A. Integrity, C. Availability, D. Confidentiality

upvoted 1 times

74gjd_37 1 year, 3 months ago

"Tenet" refers to a fundamental principle or belief that serves as the foundation for a particular doctrine, theory, or system of thought. In the context of information security and the CIA triad, tenets are core principles that guide the design, implementation, and evaluation of security practices.

The CIA triad consists of three key tenets:

Confidentiality: This tenet ensures that sensitive information is kept private and inaccessible to unauthorized individuals or entities.
Integrity: The integrity tenet focuses on maintaining the accuracy, consistency, and trustworthiness of data by protecting it from unauthorized modification or tampering.
Availability: Availability emphasizes ensuring timely access to information and resources whenever needed by authorized users without disruptions caused by attacks, failures, or other factors.

By adhering to these foundational principles (tenets), organizations can establish a comprehensive approach to safeguarding their systems and data while achieving desired levels of protection against security threats.

upvoted 1 times

Question #26 *Topic 1*

Which of the following types of attacks cannot be prevented by technical measures only?

A. Social engineering

B. Brute force

C. Smurf DoS

D. Ping flood attack

Suggested Answer: *A*

Community vote distribution

A (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: A

A. Social engineering

upvoted 1 times

Question #27 *Topic 1*

Which of the following attacks can be overcome by applying cryptography?

A. Web ripping

B. DoS

C. Sniffing

D. Buffer overflow

Suggested Answer: *C*

74gjd_37 1 year, 3 months ago

the following attacks can be overcome by applying cryptography:

- Web ripping (Option A): Cryptography can be used to protect sensitive data transmitted over the web and prevent unauthorized access, thereby preventing web ripping attacks.

- Sniffing (Option C): Cryptographic methods such as encryption can help in securing network communications against sniffing attacks where an attacker intercepts and collects traffic data packets. By encrypting the data, it becomes unreadable to the attackers even if intercepted.

upvoted 1 times

Question #28 *Topic 1*

Which of the following authentication methods prevents unauthorized execution of code on remote systems?

A. TACACS

B. S-RPC

C. RADIUS

D. CHAP

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

The simplest form of a firewall is a packet filtering firewall. Typically a router works as a packet-filtering firewall and has the capability to filter on some of the contents of packets. On which of the following layers of the OSI reference model do these routers filter information? Each correct answer represents a complete solution. Choose all that apply.

A. Transport layer

B. Physical layer

C. Data Link layer

D. Network layer

Suggested Answer: *DA*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Andrew works as a Network Administrator for Infonet Inc. The company's network has a Web server that hosts the company's Web site. Andrew wants to increase the security of the Web site by implementing Secure Sockets Layer (SSL). Which of the following types of encryption does SSL use? Each correct answer represents a complete solution. Choose two.

A. Synchronous

B. Secret

C. Asymmetric

D. Symmetric

Suggested Answer: *CD*

Community vote distribution

CD (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: CD

the correct answers in this scenario are C. Asymmetric and D. Symmetric:

C. Asymmetric encryption (also known as public-key encryption) is used during the SSL handshake process to establish a secure connection between the client and server. It involves using a pair of keys - a private key kept by the server and a public key distributed to clients.

D. Symmetric encryption is used after the SSL handshake process to encrypt data transmission between the client and server. It involves using a single shared secret key that both parties use for encryption and decryption.

upvoted 1 times

Question #31 *Topic 1*

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. John notices that the We-are- secure network is vulnerable to a man-in-the-middle attack since the key exchange process of the cryptographic algorithm it is using does not thenticate participants. Which of the following cryptographic algorithms is being used by the We-are-secure server?

A. Blowfish

B. Twofish

C. RSA

D. Diffie-Hellman

Suggested Answer: *D*

Community vote distribution

D (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: D

D. Diffie-Hellman

Diffie-Hellman is a key exchange protocol that allows two parties to establish a shared secret key over an insecure communication channel without any prior secrets. However, it does not provide authentication of participants, making it vulnerable to man-in-the-middle attacks.

A. Blowfish and B. Twofish are symmetric encryption algorithms and are not directly related to the key exchange process or vulnerability of Man-in-the-Middle attacks.

C. RSA is an asymmetric encryption algorithm commonly used for secure communications but is not specifically associated with the key exchange process vulnerable to MITM attacks.

upvoted 1 times

Banzaaai 2 years, 4 months ago

Selected Answer: D

D. Diffie-Hellman

Diffie–Hellman key agreement itself is a non-authenticated key-agreement protocol

upvoted 1 times

Question #32 *Topic 1*

Which of the following electrical events shows a sudden drop of power source that can cause a wide variety of problems on a PC or a network?

A. Blackout

B. Power spike

C. Power sag

D. Power surge

Suggested Answer: *A*

Community vote distribution

C (100%)

Spini 8 months ago

Selected Answer: C

Power sag is the only drop in power out of all options

upvoted 1 times

n00r1 1 year, 6 months ago

The electrical event that shows a sudden drop of power source, which can cause a wide variety of problems on a PC or a network, is option C, Power sag. A power sag is a temporary decrease in voltage levels, often referred to as a "brownout." It can lead to issues such as data corruption, malfunctions, or even system crashes as the power supply drops below the required levels.

Options A (Blackout), B (Power spike), and D (Power surge) are events associated with sudden loss of power, sudden increase in voltage, and sudden increase in power, respectively.

Answer: Power Sag

upvoted 3 times

Question #33 *Topic 1*

Which of the following is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity?

A. RCO

B. RTO

C. RPO

D. RTA

Suggested Answer: *B*

Community vote distribution

B (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: B

B. RTO (Recovery Time Objective). RTO represents the duration of time within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity.

- A. RCO (Recovery Checkpoint Objective) is not a commonly used term in the context of business continuity and disaster recovery.

- C. RPO (Recovery Point Objective) represents the maximum acceptable amount of data loss measured in time, indicating when backups need to be restored after a disaster event.

- D. RTA (Response Time Agreement) is unrelated to business continuity and disaster recovery; it typically refers to an agreement or contract regarding responsiveness or resolution times for service-level agreements.

upvoted 1 times

Question #34 *Topic 1*

You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of
Service attack (DOS) from a network linked to your internal enterprise network. Which of the following phases of the Incident handling process should you follow next to handle this incident?

A. Containment

B. Preparation

C. Recovery

D. Identification

Suggested Answer: *A*

74gjd_37 1 year, 3 months ago

A. Containment.

Containment involves implementing measures to prevent further damage and minimize the impact of an incident. In the case of a DOS attack, this could involve isolating affected systems or networks, blocking traffic from known malicious IP addresses, adjusting firewall rules to filter out malicious traffic patterns, or utilizing load balancers to distribute incoming requests more effectively.

Once containment has been achieved and immediate threats have been neutralized, the incident handler can then proceed to other phases such as identification (to determine how and why the incident occurred), recovery (to restore affected services or systems), and preparation (to implement preventive measures for future incidents).

in this specific scenario where it has already been identified that the problem is a Denial of Service (DOS) attack, the next phase in the Incident handling process should not be Identification.

Since you have already identified that it is a DOS attack from a network linked to your internal enterprise network, the next phase should indeed be A. Containment. The Containment phase involves taking immediate actions to mitigate and limit further damage caused by the incident, as mentioned earlier.

upvoted 1 times

Question #35 *Topic 1*

You have decided to implement video surveillance in your company in order to enhance network security. Which of the following locations must have a camera in order to provide the minimum level of security for the network resources? Each correct answer represents a complete solution. Choose two.

A. Parking lot

B. All hallways

C. Server Rooms

D. All offices

E. All entrance doors

Suggested Answer: *EC*

Community vote distribution

AB (100%)

joe77777 1 year ago

Selected Answer: AB

This question is asking for mimimum level of security. If we put CCTV camera in server room isnt that the maximum we could do? i go with A & B as that wont do much in protecting network resources

upvoted 1 times

Question #36 *Topic 1*

You work as a Network Administrator for NetTech Inc. You want to have secure communication on the company's intranet. You decide to use public key and private key pairs. What will you implement to accomplish this?

A. Microsoft Internet Information Server (IIS)

B. VPN

C. FTP server

D. Certificate server

Suggested Answer: *D*

Community vote distribution

D (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: D

D. Certificate server

upvoted 1 times

Banzaaai 2 years, 4 months ago

Selected Answer: D

D. Certificate server

upvoted 2 times

Question #37 *Topic 1*

Which of the following protocols is used to compare two values calculated using the Message Digest (MD5) hashing function?

A. CHAP

B. PEAP

C. EAP

D. EAP-TLS

Suggested Answer: *A*

74gjd_37 1 year, 3 months ago

The correct answer is A. CHAP.

CHAP (Challenge Handshake Authentication Protocol) is a protocol commonly used in authentication processes, often in remote access scenarios. It uses the Message Digest (MD5) hashing function to compare two values - one generated by the client and the other stored on the server. The comparison helps verify the identity of the client trying to establish a connection with an authenticator.

PEAP (Protected Extensible Authentication Protocol), EAP (Extensible Authentication Protocol), and EAP-TLS (EAP-Transport Layer Security) are also authentication protocols, but they do not specifically involve comparing values calculated using MD5 hashing for their operation.

upvoted 2 times

Question #38 *Topic 1*

Which of the following is a technique used for modifying messages, providing Information and Cyber security, and reducing the risk of hacking attacks during communications and message passing over the Internet?

A. Risk analysis

B. OODA loop

C. Cryptography

D. Firewall security

Suggested Answer: *C*

Community vote distribution

C (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: C

C. Cryptography.

Cryptography involves securing communication by encrypting messages to prevent unauthorized access or tampering. It uses mathematical algorithms to transform plaintext into ciphertext, making it unreadable without the cryptographic key. This ensures confidentiality and integrity of data being transmitted over networks or stored in storage systems.

Cryptographic techniques also enable secure authentication by verifying the identity of parties involved in a communication using digital signatures or certificates. Additionally, cryptography provides non-repudiation services so that senders cannot deny having sent a particular message.

While tools such as risk analysis (A), OODA loop (B), and firewall security (D) play important roles in information and cybersecurity, they do not provide encryption capabilities for modifying messages like cryptography does.

upvoted 1 times

Question #39 *Topic 1*

Which of the following statements about Public Key Infrastructure (PKI) are true? Each correct answer represents a complete solution. Choose two.

A. It uses symmetric key pairs.

B. It provides security using data encryption and digital signature.

C. It uses asymmetric key pairs.

D. It is a digital representation of information that identifies users.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Which of the following types of halon is found in portable extinguishers and is stored as a liquid?

A. Halon-f

B. Halon 1301

C. Halon 11

D. Halon 1211

Suggested Answer: *D*

74gjd_37 1 year, 3 months ago

D.

It is stored as a liquid under pressure and vaporizes when discharged to suppress fires.

upvoted 1 times

cisspdubai 4 years, 6 months ago

What is the difference between Halon 1301 and 1211?

halon 1211 is a liquefied, compressed gas contain- ing carbon, fluorine, chlorine, and bromine. it has a slightly greater toxicity than halon 1301 and is used with hand-held portable fire extinguishers and wheeled and outdoor mobile streaming devices.

upvoted 2 times

Stevey 2 years, 5 months ago

Halon 1301 is used only in fixed extinguisher installations typically cargo holds or engines and is a total flooding agent.

upvoted 1 times

Question #41 *Topic 1*

Mark has been hired by a company to work as a Network Assistant. He is assigned the task to configure a dial-up connection. He is configuring a laptop. Which of the following protocols should he disable to ensure that the password is encrypted during remote access?

A. SPAP

B. MSCHAP

C. PAP

D. MSCHAP V2

Suggested Answer: *C*

Community vote distribution

C (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: C

disable C. PAP (Password Authentication Protocol).

PAP sends passwords in clear text format, without encryption, which makes it vulnerable to interception and unauthorized access. Disabling PAP ensures that the password is not transmitted insecurely over the network.

On the other hand, several authentication protocols provide stronger security by encrypting passwords during remote access. The available options are:

A. SPAP (Shiva Password Authentication Protocol): This protocol uses one-way hashing to protect passwords in transit and offers better security than PAP.
B. MSCHAP (Microsoft Challenge Handshake Authentication Protocol): Introduced as an improvement over CHAP, MSCHAP encrypts passwords using reversible encryption.
D. MSCHAP V2: An even more secure version of MSCHAPP that provides mutual authentication through the use of digital certificates.

Therefore, disabling PAP and enabling any of the stronger authentication protocols like SPAP or MSCHAP/MSCAHPP V2 would help ensure that the password is encrypted during remote access configuration on a laptop for a dial-up connection.
upvoted 1 times

Question #42 *Topic 1*

Which of the following disaster recovery tests includes the operations that shut down at the primary site, and are shifted to the recovery site according to the disaster recovery plan?

A. Structured walk-through test

B. Simulation test

C. Full-interruption test

D. Parallel test

Suggested Answer: *C*

Community vote distribution

C (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: C

rom an ISC2 CISS-ISSAP perspective, the scenario described aligns with C. Full-interruption test.

In a full-interruption test, all operations at the primary site are deliberately shut down to simulate a complete failure or disaster situation. These operations are then shifted and resumed at the recovery site according to the organization's established disaster recovery plan. This test helps evaluate the effectiveness of the plan in managing a full-scale disruption and measures how well systems can be brought up and functional at the recovery site.

Let's briefly describe the other options for clarity:

A. Structured walk-through test: A structured walk-through involves discussing and reviewing procedures without actual execution, typically involving key personnel going through various aspects of a plan or process.
B. Simulation test: A simulation test aims to replicate specific scenarios or events related to potential disasters but does not involve actually shutting down operations.
D. Parallel test: In parallel testing, both primary and secondary sites are operational simultaneously as part of normal business processes to assess functionality and performance without experiencing an actual disruption.

upvoted 1 times

Banzaaai 2 years, 3 months ago

Selected Answer: C

C. Full-interruption test
because full shut down

upvoted 2 times

Question #43 *Topic 1*

In which of the following network topologies does the data travel around a loop in a single direction and pass through each device?

A. Ring topology

B. Tree topology

C. Star topology

D. Mesh topology

Suggested Answer: *A*

Community vote distribution

A (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: A

A. Ring

upvoted 1 times

Question #44 *Topic 1*

You are the Network Administrator for a small business. You need a widely used, but highly secure hashing algorithm. Which of the following should you choose?

A. AES

B. SHA

C. EAP

D. CRC32

Suggested Answer: *B*

Community vote distribution

B (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: B

B. SHA

upvoted 1 times

Banzaaai 2 years, 4 months ago

Selected Answer: B

B. SHA

upvoted 1 times

Question #45 *Topic 1*

Which of the following can be configured so that when an alarm is activated, all doors lock and the suspect or intruder is caught between the doors in the dead- space?

A. Man trap

B. Biometric device

C. Host Intrusion Detection System (HIDS)

D. Network Intrusion Detection System (NIDS)

Suggested Answer: *A*

Community vote distribution

A (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: A

A. Man trap

upvoted 1 times

Question #46 *Topic 1*

Which of the following refers to a location away from the computer center where document copies and backup media are kept?

A. Storage Area network

B. Off-site storage

C. On-site storage

D. Network attached storage

Suggested Answer: *B*

Community vote distribution

B (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: B

From an ISC2 CISS-ISSAP perspective, the term that refers to a location away from the computer center where document copies and backup media are kept is B. Off-site storage.

Off-site storage involves storing documents, data backups, and other physical media in a different physical location than the primary computer center or data center. This is done to mitigate risks such as natural disasters, theft, or physical damage that could impact both the primary site and its stored information simultaneously.

By keeping document copies and backup media off-site, organizations ensure that critical information can be retrieved and restored in case of a disaster at the primary location. Off-site storage adds an additional layer of protection for sensitive or essential data by minimizing single points of failure.

upvoted 2 times

Banzaaai 2 years, 3 months ago

Selected Answer: B

B. Off-site storage

location away

upvoted 1 times

Question #47 *Topic 1*

Which of the following encryption methods does the SSL protocol use in order to provide communication privacy, authentication, and message integrity? Each correct answer represents a part of the solution. Choose two.

A. Public key

B. IPsec

C. MS-CHAP

D. Symmetric

Suggested Answer: *DA*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail. Which of the following techniques is he performing to accomplish his task?

A. Email spoofing

B. Social engineering

C. Web ripping

D. Steganography

Suggested Answer: *D*

Community vote distribution

D (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: D

D. Steganography

upvoted 1 times

Question #49 *Topic 1*

Which of the following intrusion detection systems (IDS) monitors network traffic and compares it against an established baseline?

A. Network-based

B. Anomaly-based

C. File-based

D. Signature-based

Suggested Answer: *B*

Community vote distribution

B (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: B

B.

https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system#:~:text=Anomaly-based%20intrusion%20detection%20system%20%28AIDS%29%3A%20This%20solution%20monitors,the%20network%2C%20including%20bandwidth%2C%20d

Anomaly-based intrusion detection system (AIDS): This solution monitors traffic on a network and compares it with a predefined baseline that is considered " behavior across the network, including bandwidth, devices, ports, and protocols. An AIDS solution uses machine-learning techniques to build a baseline of nc security policy. This ensures businesses can discover new, evolving threats that solutions like SIDS cannot.

upvoted 1 times

Banzaaai 2 years, 3 months ago

Selected Answer: B

B. Anomaly-based

because deviation from baseline

upvoted 2 times

Question #50 *Topic 1*

Which of the following are the initial steps required to perform a risk analysis process? Each correct answer represents a part of the solution. Choose three.

A. Estimate the potential losses to assets by determining their value.

B. Establish the threats likelihood and regularity.

C. Valuations of the critical assets in hard costs.

D. Evaluate potential threats to the assets.

Suggested Answer: *ADB*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 1*

Which of the following protocols uses the Internet key Exchange (IKE) protocol to set up security associations (SA)?

A. IPSec

B. L2TP

C. LEAP

D. ISAKMP

Suggested Answer: *D*

Community vote distribution

A (100%)

n00r1 1 year, 6 months ago

The protocol that uses the Internet Key Exchange (IKE) protocol to set up security associations (SA) is IPSec (Internet Protocol Security). Therefore, the correct option is:

A. IPSec

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: A

A. IPsec.

The key material exchanged during IKE phase II is used for building the IPsec keys.

upvoted 1 times

74gjd_37 1 year, 9 months ago

IPSec (Internet Protocol Security) is a suite of protocols used to secure network communication at the IP layer. It provides features like authentication, confidentiality, and integrity. The Internet Key Exchange (IKE) protocol is utilized by IPSec for the setup and management of security associations (SA). IKE establishes the shared secret keys between communicating parties, negotiates encryption algorithms and parameters, and handles other aspects required for secure communication.

upvoted 1 times

74gjd_37 1 year, 9 months ago

D. ISAKMP: Internet Security Association and Key Management Protocol (ISAKMP) is an older version of the IKE protocol specifically designed to establish security associations while negotiating cryptographic attributes.

upvoted 1 times

Question #52 *Topic 1*

Sam is creating an e-commerce site. He wants a simple security solution that does not require each customer to have an individual key. Which of the following encryption methods will he use?

A. Asymmetric encryption

B. Symmetric encryption

C. S/MIME

D. PGP

Suggested Answer: *B*

Community vote distribution

A (100%)

SQCISSP 1 year, 6 months ago

If Sam uses Asymmetric encryption, he can provide the public key to all customers, and only he will have the private key. This means that customers can send their sensitive data securely, and Sam can decrypt it using his private key. Therefore, Asymmetric encryption is a suitable option for Sam's requirement.

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: A

A. Assymetric

Sam should use asymmetric encryption if he wants to provide customers with simple security without requiring them to have their own individual keys.

upvoted 1 times

Geddy1ng 2 years, 4 months ago

ChatGTP answer: Symmetric encryption :D

upvoted 1 times

Banzaaai 2 years, 10 months ago

Selected Answer: A

assymentric PKI

upvoted 1 times

MarkusL 3 years, 10 months ago

Answer should be A

upvoted 1 times

Question #53 *Topic 1*

Computer networks and the Internet are the prime mode of Information transfer today. Which of the following is a technique used for modifying messages, providing Information and Cyber security, and reducing the risk of hacking attacks during communications and message passing over the Internet?

A. Risk analysis

B. Firewall security

C. Cryptography

D. OODA loop

Suggested Answer: *C*

Community vote distribution

C (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: C

the correct answer is C. Cryptography.

Cryptography is a technique used for modifying messages to provide information and cyber security while reducing the risk of hacking attacks during communications and message passing over the internet. It involves encoding or encrypting data in such a way that it can only be accessed or understood by authorized parties who possess the decryption key.

Let's briefly describe the other options mentioned:

upvoted 1 times

74gjd_37 1 year, 3 months ago

A. Risk analysis: Risk analysis is a process that involves identifying, assessing, and prioritizing risks to determine appropriate actions for mitigating those risks. While risk analysis plays an important role in overall security management, it does not directly relate to modifying messages or providing security during communications.

B. Firewall security: Firewalls are network security devices designed to monitor incoming and outgoing traffic based on preset rulesets. They serve as a barrier between trusted internal networks (such as company intranets) and untrusted external networks (such as the Internet). While firewalls contribute to overall network security, they do not specifically address message modification or communication security.

D. OODA loop: The OODA (Observe-Orient-Decide-Act) loop is a decision-making cycle used in military strategy where rapid adaptation and response are critical factors. While this concept may have applications within information/cybersecurity planning and incident response scenarios, it does not directly relate to modifying messages or providing communication-security techniques.

upvoted 1 times

Question #54 *Topic 1*

An organization wants to allow a certificate authority to gain access to the encrypted data and create digital signatures on behalf of the user. The data is encrypted using the public key from a user's certificate. Which of the following processes fulfills the above requirements?

A. Key escrow

B. Key storage

C. Key revocation

D. Key recovery

Suggested Answer: *A*

Community vote distribution

A (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: A

Key escrow involves storing copies of encryption keys with a trusted third party, such as a certificate authority. In this case, if the organization wants to allow the certificate authority access to encrypted data and enable them to create digital signatures on behalf of users, key escrow would provide a mechanism for securely sharing the private key corresponding to each user's public key used for encryption.

By having access to these private keys stored in an escrow system maintained by the CA, they could perform actions on behalf of those users while ensuring secure authorization and integrity of cryptographic operations.

upvoted 1 times

Question #55 *Topic 1*

Which of the following are the primary components of a discretionary access control (DAC) model? Each correct answer represents a complete solution. Choose two.

A. User's group

B. File and data ownership

C. Smart card

D. Access rights and permissions

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 1*

Which of the following encryption modes can make protocols without integrity protection even more susceptible to replay attacks, since each block gets decrypted in exactly the same way?

A. Cipher feedback mode

B. Cipher block chaining mode

C. Output feedback mode

D. Electronic codebook mode

Suggested Answer: *D*

Community vote distribution

D (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: D

D: Electronic codebook mode (ECB) can make protocols without integrity protection even more susceptible to replay attacks since each block gets decrypted in exactly the same way

upvoted 1 times

Question #57 *Topic 1*

You work as a technician for Trade Well Inc. The company is in the business of share trading. To enhance security, the company wants users to provide a third key (apart from ID and password) to access the company's Web site. Which of the following technologies will you implement to accomplish the task?

A. Smart cards

B. Key fobs

C. VPN

D. Biometrics

Suggested Answer: *B*

Community vote distribution

B (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: B

B. Key fobs

Key fobs are small devices that generate one-time passwords (OTPs) at regular intervals, typically synchronized with server-side systems. Users enter these OTPs along with their existing credentials during authentication. Key fobs act as token-based authenticators, providing an extra layer of security beyond traditional login details.

In the context of the scenario where Trade Well Inc. wants users to provide a third key apart from ID and password to access their website, key fobs can serve this purpose effectively by requiring users to have possession of both their credentials and the physical key fob device.

upvoted 2 times

Question #58 *Topic 1*

Which of the following layers of the OSI model corresponds to the Host-to-Host layer of the TCP/IP model?

A. The transport layer

B. The presentation layer

C. The session layer

D. The application layer

Suggested Answer: *A*

Community vote distribution

A (100%)

74gjd_37 1 year, 3 months ago

Selected Answer: A

A: The transport layer

upvoted 1 times

Question #59 *Topic 1*

You are the Network Administrator for a college. You watch a large number of people (some not even students) going in and out of areas with campus computers
(libraries, computer labs, etc.). You have had a problem with laptops being stolen. What is the most cost effective method to prevent this?

A. Smart card access to all areas with computers.

B. Use laptop locks.

C. Video surveillance on all areas with computers.

D. Appoint a security guard.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 1*

The ATM of a bank is robbed by breaking the ATM machine. Which of the following physical security devices can now be used for verification and historical analysis of the ATM robbery?

A. Key card

B. Biometric devices

C. Intrusion detection systems

D. CCTV Cameras

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #61 *Topic 1*

You have been assigned the task of selecting a hash algorithm. The algorithm will be specifically used to ensure the integrity of certain sensitive files. It must use a
128 bit hash value. Which of the following should you use?

A. AES

B. SHA

C. MD5

D. DES

Suggested Answer: *C*

n00r1 1 year, 6 months ago

ChatGPT
For ensuring the integrity of sensitive files with a 128-bit hash value, you should choose option B, SHA (Secure Hash Algorithm). Specifically, you may consider using SHA-256, which produces a 256-bit hash value, but truncating it to the required 128-bit length if necessary.

Option C (MD5) also produces a 128-bit hash value, but MD5 is considered weaker and more susceptible to collision attacks compared to SHA. Therefore, SHA is generally preferred for security purposes.

So, the recommended choice is:

B. SHA (Secure Hash Algorithm)
upvoted 3 times

Question #62 *Topic 1*

Which of the following are the countermeasures against a man-in-the-middle attack? Each correct answer represents a complete solution. Choose all that apply.

A. Using public key infrastructure authentication.

B. Using basic authentication.

C. Using Secret keys for authentication.

D. Using Off-channel verification.

Suggested Answer: *ACD*

n00r1 1 year, 6 months ago

The countermeasures against a man-in-the-middle attack include:

A. Using public key infrastructure (PKI) authentication.
C. Using secret keys for authentication.

These methods help enhance authentication security and protect against unauthorized interception or manipulation of communication. Basic authentication (option B) is more susceptible to interception and is not as secure as using advanced cryptographic methods like public key infrastructure or secret keys.

Option D (Off-channel verification) is not a standard term in the context of common security measures against man-in-the-middle attacks. The commonly employed methods are public key infrastructure and secret keys.

upvoted 1 times

Question #63 *Topic 1*

Which of the following is an electrical event shows that there is enough power on the grid to prevent from a total power loss but there is no enough power to meet the current electrical demand?

A. Power Surge

B. Power Spike

C. Blackout

D. Brownout

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #64 *Topic 1*

Which of the following protocols is designed to efficiently handle high-speed data over wide area networks (WANs)?

A. PPP

B. X.25

C. Frame relay

D. SLIP

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 1*

Which of the following statements best describes a certification authority?

A. A certification authority is a technique to authenticate digital documents by using computer cryptography.

B. A certification authority is a type of encryption that uses a public key and a private key pair for data encryption.

C. A certification authority is an entity that issues digital certificates for use by other parties.

D. A certification authority is a type of encryption that uses a single key to encrypt and decrypt data.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility?

A. Hot Site

B. Mobile Site

C. Warm Site

D. Cold Site

Suggested Answer: *A*

Community vote distribution

A (100%)

Banzaaai 1 year, 3 months ago

Selected Answer: A

A. Hot Site

because fully maintained

upvoted 1 times

Question #67 *Topic 1*

Which of the following should the administrator ensure during the test of a disaster recovery plan?

A. Ensure that the plan works properly

B. Ensure that all the servers in the organization are shut down.

C. Ensure that each member of the disaster recovery team is aware of their responsibility.

D. Ensure that all client computers in the organization are shut down.

Suggested Answer: *CA*

n00r1 1 year, 6 months ago

ChatGPT

During the test of a disaster recovery plan, the administrator should ensure:

A. Ensure that the plan works properly

Testing the disaster recovery plan involves verifying that all components of the plan function as intended, including backup systems, communication processes, and recovery procedures. This ensures that in the event of a disaster, the organization can successfully recover and resume operations according to the plan.

Options B, C, and D may be important considerations in the overall disaster recovery plan, but the primary focus during testing is to confirm the effectiveness of the plan itself.

upvoted 1 times

Question #68 *Topic 1*

The service-oriented modeling framework (SOMF) provides a common modeling notation to address alignment between business and IT organizations. Which of the following principles does the SOMF concentrate on? Each correct answer represents a part of the solution. Choose all that apply.

A. Disaster recovery planning

B. SOA value proposition

C. Software assets reuse

D. Architectural components abstraction

E. Business traceability

Suggested Answer: *EBCD*

Currently there are no comments in this discussion, be the first to comment!

Question #69 *Topic 1*

You want to connect a twisted pair cable segment to a fiber-optic cable segment. Which of the following networking devices will you use to accomplish the task?

A. Hub

B. Switch

C. Repeater

D. Router

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #70 *Topic 1*

In your office, you are building a new wireless network that contains Windows 2003 servers. To establish a network for secure communication, you have to implement IPSec security policy on the servers. What authentication methods can you use for this implementation? Each correct answer represents a complete solution. Choose all that apply.

A. Public-key cryptography

B. Kerberos

C. Preshared keys

D. Digital certificates

Suggested Answer: *BDC*

Currently there are no comments in this discussion, be the first to comment!

Question #71 *Topic 1*

Which of the following two components does Kerberos Key Distribution Center (KDC) consist of? Each correct answer represents a complete solution. Choose two.

A. Data service

B. Ticket-granting service

C. Account service

D. Authentication service

Suggested Answer: *DB*

Currently there are no comments in this discussion, be the first to comment!

Question #72 *Topic 1*

Kerberos is a computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. Which of the following statements are true about the Kerberos authentication scheme? Each correct answer represents a complete solution.
Choose all that apply.

A. Kerberos requires continuous availability of a central server.

B. Dictionary and brute force attacks on the initial TGS response to a client may reveal the subject's passwords.

C. Kerberos builds on Asymmetric key cryptography and requires a trusted third party.

D. Kerberos requires the clocks of the involved hosts to be synchronized.

Suggested Answer: *ADB*

Community vote distribution

AD (100%)

Clomirtauy 1 year, 1 month ago

Selected Answer: AD

B is false. kerbeos never transmit passwords between client and server

upvoted 1 times

Question #73 *Topic 1*

An organization is seeking to implement a hot site and wants to maintain a live database server at the backup site. Which of the following solutions will be the best for the organization?

A. Electronic vaulting

B. Remote journaling

C. Remote mirroring

D. Transaction logging

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #74 *Topic 1*

A helpdesk technician received a phone call from an administrator at a remote branch office. The administrator claimed to have forgotten the password for the root account on UNIX servers and asked for it. Although the technician didn't know any administrator at the branch office, the guy sounded really friendly and since he knew the root password himself, he supplied the caller with the password. What type of attack has just occurred?

A. Social Engineering attack

B. Brute Force attack

C. War dialing attack

D. Replay attack

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #75 *Topic 1*

You work as a Network Administrator of a TCP/IP network. You are having DNS resolution problem. Which of the following utilities will you use to diagnose the problem?

A. TRACERT

B. PING

C. IPCONFIG

D. NSLOOKUP

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #76 *Topic 1*

The IPSec protocol is configured in an organization's network in order to maintain a complete infrastructure for secured network communications. IPSec uses four components for this. Which of the following components reduces the size of data transmitted over congested network connections and increases the speed of such networks without losing data?

A. AH

B. ESP

C. IPcomp

D. IKE

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #77 *Topic 1*

You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You want to perform the following tasks: Develop a risk-driven enterprise information security architecture. Deliver security infrastructure solutions that support critical business initiatives. Which of the following methods will you use to accomplish these tasks?

A. Service-oriented architecture

B. Sherwood Applied Business Security Architecture

C. Service-oriented modeling framework

D. Service-oriented modeling and architecture

Suggested Answer: *B*

Community vote distribution

B (100%)

Banzaaai 1 year, 3 months ago

Selected Answer: B

B. Sherwood Applied Business Security Architecture

because risk-driven security architecture

upvoted 1 times

Question #78 *Topic 1*

A network is configured on a Bus topology. Which of the following conditions could cause a network failure? Each correct answer represents a complete solution.
Choose all that apply.

A. A break in a network cable

B. 75 ohm terminators at open ends

C. A powered off workstation

D. An open-ended cable without terminators

Suggested Answer: *DBA*

n00r1 1 year, 6 months ago
In a Bus topology network, the following conditions could cause a network failure:

A. A break in a network cable: If there is a break in the network cable, the continuity of the network is disrupted, and communication may fail.

D. An open-ended cable without terminators: If there is an open-ended cable without terminators, it can lead to signal reflection issues and disrupt the proper functioning of the network.

Option B (75 ohm terminators at open ends) is not typically associated with Bus topology. Option C (A powered off workstation) might affect communication to that specific workstation but is less likely to cause a complete network failure.
upvoted 1 times

MarkusL 3 years, 10 months ago
Answer should be A & D
upvoted 1 times

Question #79 *Topic 1*

Which of the following is an input device that is used for controlling machines such as cranes, trucks, underwater unmanned vehicles, wheelchairs, surveillance cameras, and zero turning radius lawn mowers?

A. PS/2

B. Joystick

C. Microphone

D. AGP

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #80 *Topic 1*

Which of the following types of attacks is often performed by looking surreptitiously at the keyboard or monitor of an employee's computer?

A. Buffer-overflow attack

B. Man-in-the-middle attack

C. Shoulder surfing attack

D. Denial-of-Service (DoS) attack

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #81 *Topic 1*

A digital signature is a type of public key cryptography. Which of the following statements are true about digital signatures? Each correct answer represents a complete solution. Choose all that apply.

A. In order to digitally sign an electronic record, a person must use his/her public key.

B. In order to verify a digital signature, the signer's private key must be used.

C. In order to digitally sign an electronic record, a person must use his/her private key.

D. In order to verify a digital signature, the signer's public key must be used.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #82 *Topic 1*

An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

A. Mutual

B. Anonymous

C. Multi-factor

D. Biometrics

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #83 *Topic 1*

You work as an Incident handling manager for Orangesect Inc. You detect a virus attack incident in the network of your company. You develop a signature based on the characteristics of the detected virus. Which of the following phases in the Incident handling process will utilize the signature to resolve this incident?

A. Eradication

B. Identification

C. Recovery

D. Containment

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #84 *Topic 1*

In which of the following access control models can a user not grant permissions to other users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?

A. Discretionary Access Control (DAC)

B. Role Based Access Control (RBAC)

C. Mandatory Access Control (MAC)

D. Access Control List (ACL)

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #85 *Topic 1*

Which of the following protocols provides connectionless integrity and data origin authentication of IP packets?

A. ESP

B. AH

C. IKE

D. ISAKMP

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #86 *Topic 1*

The network you administer allows owners of objects to manage the access to those objects via access control lists. This is an example of what type of access control?

A. RBAC

B. MAC

C. CIA

D. DAC

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #87 *Topic 1*

Which of the following processes is used to identify relationships between mission critical applications, processes, and operations and all supporting elements?

A. Critical path analysis

B. Functional analysis

C. Risk analysis

D. Business impact analysis

Suggested Answer: *A*

Community vote distribution

bobby_kl 1 year, 2 months ago

Selected Answer: D

D. Business impact analysis

upvoted 1 times

n00r1 1 year, 6 months ago

The process used to identify relationships between mission-critical applications, processes, and operations, along with all supporting elements, is:

D. Business impact analysis

Business impact analysis (BIA) is a process that helps in understanding the criticality of various business functions and their dependencies. It identifies how disruptions or failures in specific applications or processes can impact overall business operations. BIA is crucial for effective business continuity planning and risk management.

upvoted 2 times

Banzaaai 2 years, 10 months ago

Selected Answer: A

A. Critical path analysis

upvoted 1 times

Question #88 *Topic 1*

Which of the following devices is a least expensive power protection device for filtering the electrical stream to control power surges, noise, power sags, and power spikes?

A. Line Conditioner

B. Surge Suppressor

C. Uninterrupted Power Supply (UPS)

D. Expansion Bus

Suggested Answer: *C*

SQCISSP 1 year, 6 months ago

Surge Suppressor

The least expensive power protection device for filtering the electrical stream to control power surges, noise, power sags, and power spikes is a Surge Suppresso

upvoted 1 times

Question #89 *Topic 1*

You work as a Project Manager for Tech Perfect Inc. You are creating a document which emphasizes the formal study of what your organization is doing currently and where it will be in the future. Which of the following analysis will help you in accomplishing the task?

A. Cost-benefit analysis

B. Gap analysis

C. Requirement analysis

D. Vulnerability analysis

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #90 *Topic 1*

SSH is a network protocol that allows data to be exchanged between two networks using a secure channel. Which of the following encryption algorithms can be used by the SSH protocol? Each correct answer represents a complete solution. Choose all that apply.

A. Blowfish

B. DES

C. IDEA

D. RC4

Suggested Answer: *CBA*

Currently there are no comments in this discussion, be the first to comment!

Question #91 *Topic 1*

Which of the following firewalls inspects the actual contents of packets?

A. Packet filtering firewall

B. Stateful inspection firewall

C. Application-level firewall

D. Circuit-level firewall

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #92 *Topic 1*

Which of the following statements about incremental backup are true? Each correct answer represents a complete solution. Choose two.

A. It is the fastest method of backing up data.

B. It is the slowest method for taking a data backup.

C. It backs up the entire database, including the transaction log.

D. It backs up only the files changed since the most recent backup and clears the archive bit.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #93 *Topic 1*

You work as a Network Administrator for Blue Bell Inc. The company has a TCP-based network. The company has two offices in different cities. The company wants to connect the two offices by using a public network. You decide to configure a virtual private network (VPN) between the offices. Which of the following protocols is used by VPN for tunneling?

A. L2TP

B. HTTPS

C. SSL

D. IPSec

Suggested Answer: *A*

Community vote distribution

D (100%)

n00r1 1 year, 6 months ago

The protocol commonly used by VPNs for tunneling is:

D. IPSec (Internet Protocol Security)

IPSec is widely used for creating secure communication tunnels over public networks. It provides a secure framework for authentication and encryption, ensuring the confidentiality and integrity of data transmitted between the two offices. Options A (L2TP), B (HTTPS), and C (SSL) are also used in various VPN implementations, but IPSec is a commonly used protocol for VPN tunneling.

upvoted 1 times

jim22444 2 years, 1 month ago

Selected Answer: D

IPsec vs L2TP I always saw IPsec has to be used with L2TP to keep it secure. If so then I see no reason to use L2TP over IPsec

upvoted 1 times

Banzaaai 2 years, 10 months ago

why not IPSEC

upvoted 2 times

Question #94 *Topic 1*

John works as a Network Administrator for NetPerfect Inc. The company has a Windows-based network. John has been assigned a project to build a network for the sales department of the company. It is important for the LAN to continue working even if there is a break in the cabling. Which of the following topologies should John use to accomplish the task?

A. Star

B. Mesh

C. Bus

D. Ring

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #1 *Topic 2*

Which of the following encryption algorithms are based on block ciphers?

A. RC4

B. Twofish

C. Rijndael

D. RC5

Suggested Answer: *DCB*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 2*

Adam works as a Network Administrator. He discovers that the wireless AP transmits 128 bytes of plaintext, and the station responds by encrypting the plaintext. It then transmits the resulting ciphertext using the same key and cipher that are used by WEP to encrypt subsequent network traffic. Which of the following types of authentication mechanism is used here?

A. Pre-shared key authentication

B. Open system authentication

C. Shared key authentication

D. Single key authentication

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 2*

The OSI model is the most common networking model used in the industry. Applications, network functions, and protocols are typically referenced using one or more of the seven OSI layers. Of the following, choose the two best statements that describe the OSI layer functions. Each correct answer represents a complete solution. Choose two.

A. Layers 1 and 2 deal with application functionality and data formatting. These layers reside at the top of the model.

B. Layers 4 through 7 define the functionality of IP Addressing, Physical Standards, and Data Link protocols.

C. Layers 5, 6, and 7 focus on the Network Application, which includes data formatting and session control.

D. Layers 1, 2, 3, and 4 deal with physical connectivity, encapsulation, IP Addressing, and Error Recovery. These layers define the end-to-end functions of data

Suggested Answer: *DC*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 2*

Which of the following is the technology of indoor or automotive environmental comfort?

A. HIPS

B. HVAC

C. NIPS

D. CCTV

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 2*

Which of the following protocols provides certificate-based authentication for virtual private networks (VPNs)?

A. PPTP

B. SMTP

C. HTTPS

D. L2TP

Suggested Answer: *D*

Community vote distribution

D (100%)

SQCISSP 1 year, 6 months ago

Extensible Authentication Protocol (EAP)

In addition to older and less-secure password-based authentication methods (which should be avoided), the built-in VPN solution uses Extensible Authentication Protocol (EAP) to provide secure authentication using both user name and password, and certificate-based methods.

upvoted 1 times

n00r1 1 year, 6 months ago

The protocol that provides certificate-based authentication for virtual private networks (VPNs) is:

C. HTTPS (Hypertext Transfer Protocol Secure)

HTTPS is commonly used for secure communication over the Internet, and it utilizes certificates for authentication. While other protocols like PPTP, SMTP, and L2TP are used for various purposes, HTTPS is specifically associated with secure web communication and often used in VPNs for certificate-based authentication.

upvoted 1 times

Banzaaai 2 years, 10 months ago

Selected Answer: D

D. L2TP

upvoted 1 times

Question #6 *Topic 2*

Which of the following types of ciphers are included in the historical ciphers? Each correct answer represents a complete solution. Choose two.

A. Block ciphers

B. Transposition ciphers

C. Stream ciphers

D. Substitution ciphers

Suggested Answer: *DB*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 2*

John works as a security manager for SoftTech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?

A. Evacuation drill

B. Walk-through drill

C. Structured walk-through test

D. Full-scale exercise

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 2*

Which of the following security protocols provides confidentiality, integrity, and authentication of network traffic with end-to-end and intermediate-hop security?

A. IPSec

B. SET

C. SWIPE

D. SKIP

Suggested Answer: *C*

Community vote distribution

A (100%)

bobby_kl 1 year, 2 months ago

Selected Answer: A

A. IPSec

upvoted 1 times

n00r1 1 year, 6 months ago

The security protocol that provides confidentiality, integrity, and authentication of network traffic with end-to-end and intermediate-hop security is:

A. IPSec (Internet Protocol Security)

upvoted 1 times

Question #9 *Topic 2*

You are calculating the Annualized Loss Expectancy (ALE) using the following formula: ALE=AV * EF * ARO What information does the AV (Asset Value) convey?

A. It represents how many times per year a specific threat occurs.

B. It represents the percentage of loss that an asset experiences if an anticipated threat occurs.

C. It is expected loss for an asset due to a risk over a one year period.

D. It represents the total cost of an asset, including the purchase price, recurring maintenance, expenses, and all other costs.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 2*

You work as a Network Administrator for NetTech Inc. When you enter http://66.111.64.227 in the browser's address bar, you are able to access the site. But, you are unable to access the site when you enter http://www.company.com. What is the most likely cause?

A. The site's Web server is offline.

B. The site's Web server has heavy traffic.

C. WINS server has no NetBIOS name entry for the server.

D. DNS entry is not available for the host name.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 2*

In software development, which of the following analysis is used to document the services and functions that have been accidentally left out, deliberately eliminated or still need to be developed?

A. Gap analysis

B. Requirement analysis

C. Cost-benefit analysis

D. Vulnerability analysis

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 2*

Which of the following processes identifies the threats that can impact the business continuity of operations?

A. Function analysis

B. Risk analysis

C. Business impact analysis

D. Requirement analysis

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 2*

What are the benefits of using AAA security service in a network? Each correct answer represents a part of the solution. Choose all that apply.

A. It provides scalability.

B. It supports a single backup system.

C. It increases flexibility and control of access configuration.

D. It supports RADIUS, TACACS+, and Kerberos authentication methods.

Suggested Answer: *CAD*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 2*

In which of the following SDLC phases are the software and other components of the system faithfully incorporated into the design specifications?

A. Programming and training

B. Evaluation and acceptance

C. Definition

D. Initiation

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 2*

Which of the following life cycle modeling activities establishes service relationships and message exchange paths?

A. Service-oriented logical design modeling

B. Service-oriented conceptual architecture modeling

C. Service-oriented discovery and analysis modeling

D. Service-oriented business integration modeling

Suggested Answer: *A*

Community vote distribution

A (100%)

n00r1 1 year, 6 months ago

The life cycle modeling activity that establishes service relationships and message exchange paths is:

B. Service-oriented conceptual architecture modeling

In the context of service-oriented architecture (SOA), conceptual architecture modeling involves defining the high-level structure of services, their relationships, and the ways in which they exchange messages. This phase is essential for laying the foundation for the subsequent design and implementation of services.

upvoted 1 times

Banzaaai 2 years, 10 months ago

Selected Answer: A

A. Service-oriented logical design modeling

upvoted 1 times

Question #16 *Topic 2*

Which of the following authentication methods support mutual authentication? Each correct answer represents a complete solution. Choose two.

A. MS-CHAP v2

B. NTLM

C. EAP-MD5

D. EAP-TLS

Suggested Answer: *DA*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 2*

Which of the following keys is derived from a preshared key and Extensible Authentication Protocol (EAP)?

A. Pairwise Transient Key

B. Group Temporal Key

C. Private Key

D. Pairwise Master Key

Suggested Answer: *D*

Community vote distribution

D (100%)

Banzaaai 1 year, 4 months ago

Selected Answer: D

D. Pairwise Master Key

upvoted 1 times

Question #18 *Topic 2*

Which of the following schemes is used by the Kerberos authentication?

A. Public key cryptography

B. One time password

C. Private key cryptography

D. OPIE

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 2*

You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

A. Warm site

B. Cold site

C. Off site

D. Hot site

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 2*

Which of the following are the centralized administration technologies? Each correct answer represents a complete solution. Choose all that apply.

A. RADIUS

B. TACACS+

C. Media Access control

D. Peer-to-Peer

Suggested Answer: *BA*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 2*

You are implementing some security services in an organization, such as smart cards, biometrics, access control lists, firewalls, intrusion detection systems, and clipping levels. Which of the following categories of implementation of the access control includes all these security services?

A. Administrative access control

B. Logical access control

C. Physical access control

D. Preventive access control

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 2*

You work as a Network Administrator for Net World Inc. You are required to configure a VLAN for the company. Which of the following devices will you use to physically connect the computers in the VLAN? Each correct answer represents a complete solution. Choose two.

A. Switch

B. Router

C. Bridge

D. Hub E. Repeater

Suggested Answer: *BA*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 2*

Which of the following protocols work at the Network layer of the OSI model?

A. Routing Information Protocol (RIP)

B. File Transfer Protocol (FTP)

C. Simple Network Management Protocol (SNMP)

D. Internet Group Management Protocol (IGMP)

Suggested Answer: *AD*

d1fa141 1 year, 5 months ago

Nonsense. IGMP operates at layer 3. Check Google.

upvoted 1 times

n00r1 1 year, 6 months ago

The protocol that works at the Network layer (Layer 3) of the OSI model is:

A. Routing Information Protocol (RIP)

RIP is a routing protocol that operates at the Network layer, specifically designed for routing within an IP network. The other options, FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), and IGMP (Internet Group Management Protocol), operate at higher layers of the OSI model.

upvoted 1 times

Question #24 *Topic 2*

Which of the following are used to suppress paper or wood fires? Each correct answer represents a complete solution. Choose two.

A. Soda acid

B. Kerosene

C. Water

D. CO2

Suggested Answer: *CA*

Currently there are no comments in this discussion, be the first to comment!