Eccouncil

(212-82)

Certified Cybersecurity Technician

Total: **125 Questions**

Link:

MYEXAM.FR

defense method required by the PCI-DSS to manage malware threats.

References:

1. https://www.pcisecuritystandards.org/documents/PCI_DSS_v4-0.pdf
2. https://www.pcisecuritystandards.org/pci_security/
3. https://www.iso.org/isoiec-27001-information-security.html

Question: 5

Ashton is working as a security specialist in SoftEight Tech. He was instructed by the management to strengthen the Internet access policy. For this purpose, he implemented a type of Internet access policy that forbids everything and imposes strict restrictions on all company computers, whether it is system or network usage. Identify the type of Internet access policy implemented by Ashton in the above scenario.

A.Paranoid policy
B.Prudent policy
C.Permissive policy
D.Promiscuous policy

Answer: A

Explanation:

A. Paranoid policy is the correct answer as it represents an Internet access strategy that implements strict restrictions by forbidding all access unless explicitly permitted.

In cybersecurity governance, particularly concerning Internet access, a paranoid policy is characterized by an overarching cautiousness—reminiscent of a zero-trust framework. This model assumes that threats could originate from both external and internal sources, leading to a configuration where all transactions and system interactions are scrutinized stringently. It effectively minimizes digital attack surfaces and thus helps safeguard sensitive data by allowing access only when the criteria are met, thereby enhancing overall security posture.

Evaluation of Incorrect Options:

B. **Prudent policy** is a balanced strategy involving moderate restrictions that allow some freedoms while still providing protection. Unlike the paranoid policy, it does not impose a blanket ban on all access, making it less stringent.

C. **Permissive policy** fosters a more open environment, enabling users to access various systems and networks with minimal restrictions. This type is inherently opposed to Ashton's strategy, as it prioritizes usability over security.

D. **Promiscuous policy** suggests a non-selective access approach, potentially allowing unrestricted interactions with network resources. This policy type may inadvertently invite security breaches, contradicting the defensive aims of Ashton's implementation focused on preemptively mitigating risks.

Authoritative References:

https://www.nist.gov/publications
https://www.isaca.org/resources
https://www.sans.org/white-papers

Answer: B

Explanation:

B. RADIUS is the correct answer as it is a widely used protocol for centralized authentication, authorization, and accounting (AAA) for network access.

RADIUS (Remote Authentication Dial-In User Service) operates at the transport layer (Layer 4) of the OSI model, facilitating communication between clients and servers in a client-server architecture. It provides a framework for secure access to systems and networks, allowing for centralized management of authentication, whereby users can be authenticated based on credentials stored on a central server, significantly enhancing security in multi-user environments. Moreover, RADIUS supports various authentication methods, including PAP, CHAP, and EAP, which are crucial for flexibility in modern cybersecurity applications.

Evaluation of incorrect options:

A. SNMPv3: Simple Network Management Protocol version 3 focuses on network management and monitoring rather than authentication, authorization, or accounting, making it unsuitable for the described scenario. Its purpose primarily revolves around the management of devices on IP networks.

C. POP3S: Post Office Protocol version 3 Secure is designed specifically for retrieving emails from a server, emphasizing data confidentiality during the transmission of emails rather than providing AAA functionalities required for network access.

D. IMAPS: Internet Message Access Protocol Secure, similar to POP3S, is intended for email retrieval and management with encryption, rather than dealing with authentication, authorization, or accounting at the network access level. Its focus is on secure mail access rather than broader network security considerations that RADIUS addresses.

In summary, RADIUS is designed for the AAA framework essential for securing remote access in an enterprise environment, while the other protocols serve entirely different functions.

References:

https://datatracker.ietf.org/doc/html/rfc2865
https://csrc.nist.gov/publications/detail/sp/800-150/final
https://www.fortinet.com/resources/cyberglossary/radius-protocol

Question: 9

Malachi, a security professional, implemented a firewall in his organization to trace incoming and outgoing traffic. He deployed a firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate.
Identify the firewall technology implemented by Malachi in the above scenario.

A. Next generation firewall (NGFW)
B. Circuit-level gateways
C. Network address translation (NAT)
D. Packet filtering

Answer: B

Explanation:

qualify as high-interaction, where attackers could interact freely and extensively.

References:

1. https://www.sans.org/white-papers/34596/
2. https://resources.infosecinstitute.com/topic/honeypots-and-honeynets-a-comprehensive-overview/
3. https://www.cisecurity.org/white-papers/honeypots-and-honeynets/

Question: 13

An MNC hired Brandon, a network defender, to establish secured VPN communication between the company's remote offices. For this purpose, Brandon employed a VPN topology where all the remote offices communicate with the corporate office but communication between the remote offices is denied.
Identify the VPN topology employed by Brandon in the above scenario.

A. Point-to-Point VPN topology
B. Star topology
C. Hub-and-Spoke VPN topology
D. Full-mesh VPN topology

Answer: B

Explanation:

B is correct because the Hub-and-Spoke VPN topology allows communication solely between the remote offices and a central corporate office, restricting inter-office communication.

The Hub-and-Spoke topology functions by establishing a single central connection point (the hub) for all remote locations (spokes), ensuring efficient management and enhanced security by controlling the traffic flow. This tightly regulated structure minimizes vulnerabilities that could arise from peer-to-peer connections among remote offices, thus fortifying the network against potential threats. The hub acts as an intermediary, facilitating traffic between spokes but preventing direct communication between them, effectively securing data transmission.

Evaluation of Other Options

A. **Point-to-Point VPN Topology**: This setup involves direct connections between two endpoints only, meaning it does not support multiple remote office connections efficiently. Consequently, it fails to illustrate the centralized communication structure required by the MNC in question.

C. **Hub-and-Spoke VPN Topology**: While this is technically the correct answer, it's crucial to note that this option reflects the defined structure where the corporate office is the hub, allowing for remote office connectivity solely through the hub without direct communication among offices. This option is partially correct because it aligns with the scenario described, but option B is explicitly labeled as correct due to its definition in the question.

D. **Full-Mesh VPN Topology**: In this configuration, every remote office connects to every other remote office, promoting direct inter-office communication. This model contradicts the requirements of the MNC scenario where such communications are to be denied; hence, it's not suitable for their needs.

References

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/vpn_config/configuration/15-mt/vpn-secure.html
https://www.paloaltonetworks.com/resources/what-is-a-vpn

The scenario illustrates a failure to secure all communication channels, leading to an exploitable weakness where critical information could be accessed illegitimately. This reflects inadequate consideration for holistic security measures throughout the application's architecture. By not addressing the weakest link, the application exposes itself to attacks that could have been mitigated through rigorous security protocols.

Evaluation of Incorrect Options:

B. **Do not trust user input**: This principle relates to input validation and sanitization. While essential, this specific scenario focuses more on communication flaws rather than user input vulnerabilities directly. Consequently, it is less relevant in this context.

C. **Exception handling**: This principle concerns managing errors gracefully to prevent information leakage or application crashes. However, the primary issue in the scenario is a flaw in end-point communication, not necessarily an error management problem, making this choice less applicable.

D. **Fault tolerance**: This principle refers to a system's ability to remain operational despite failures. While important for overall reliability, the hacker's exploitation centers around a fundamental security oversight rather than an operational failure, making this choice not directly pertinent to the scenario.

References:

https://www.owasp.org/index.php/Secure_Application_Architecture
https://csrc.nist.gov/publications/detail/sp/800-161/final
https://www.sans.org/white-papers/39662/

Question: 18

A software company is developing a new software product by following the best practices for secure application development. Dawson, a software analyst, is checking the performance of the application on the client's network to determine whether end users are facing any issues in accessing the application.
Which of the following tiers of a secure application development lifecycle involves checking the performance of the application?

A. Development
B. Testing
C. Quality assurance (QA)
D. Staging

Answer: C

Explanation:

Answer C is correct because the Quality Assurance (QA) tier is specifically focused on evaluating both the performance and overall functionality of an application before it goes live.

In the secure application development lifecycle, each tier serves a distinct purpose. The Development stage primarily concentrates on coding and functional design but does not emphasize performance testing. The Testing tier is generally where functional and security tests occur, but it is not exclusively focused on evaluating performance metrics under real-world conditions.

The Quality Assurance (QA) phase encompasses comprehensive assessment procedures that include performance evaluation as part of ensuring the final product meets predefined standards. This involves checking for speed, reliability, and responsiveness in the application, which directly impacts user experience. The QA team's goal is to simulate production conditions to identify and mitigate any performance bottlenecks.

https://www.nist.gov/publications/recommendations-cloud-computing-auditing-and-compliance

Question: 21

A software company has implemented a wireless technology to track the employees' attendance by recording their in and out timings. Each employee in the company will have an entry card that is embedded with a tag. Whenever an employee enters the office premises, he/she is required to swipe the card at the entrance. The wireless technology uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects.
Which of the following technologies has the software company implemented in the above scenario?

A. WiMAX
B. RFID
C. Bluetooth
D. Wi-Fi

Answer: B

Explanation:

The technology implemented by the software company is RFID (Radio-Frequency Identification).

RFID enables automatic identification and tracking of tags embedded in objects through radio-frequency electromagnetic waves, making it suitable for attendance tracking by reading employee cards at entry points. The system can efficiently capture data, ensures contactless operation, and supports rapid processing without requiring direct line-of-sight, which is consistent with the described functionality.

Evaluation of Other Options:

A. WiMAX: This technology primarily provides high-speed wireless data transmission over large areas and is not designed for short-range identification purposes. It is unsuitable for the attendance tracking system described, which involves short-range card swiping rather than broad internet access. WiMAX Overview

C. Bluetooth: While Bluetooth allows for wireless communication over short distances, its primary use case centers around personal device connectivity rather than unique identification and tracking applications. Additionally, Bluetooth requires pairing and may not support the rapid identification needed in the attendance tracking scenario. Bluetooth Technology

D. Wi-Fi: Wi-Fi is designed for high-speed internet access and local area networking, not for the dedicated tracking of individual objects or attendance entry systems. Its functionality does not align with the specific requirements of tag-based identification as characterized in the scenario. Wi-Fi Alliance

In summary, RFID is the only technology that matches the operational requirements outlined, emphasizing efficient, automated tracking through embedded tags, while the other options do not align with the specific needs of the attendance tracking system.

References:

RFID Journal
IEEE RFID 2022
NI RFID Fundamentals

Answer: D

Explanation:

D. QR codes and barcodes are correct as they directly enable the scanning and automatic identification of products during the billing process.

Reasoning:QR codes and barcodes are widely employed in retail environments to streamline transactions. They serve as graphical representations of data encoded in a manner that can be easily scanned by a machine-readable device. When the billing executive scans products, the barcode or QR code is read by a barcode scanner, which translates the encoded data into product information, including pricing and inventory controls. This method enhances operational efficiency and reduces human error significantly during checkout processes.

Evaluation of Other Options:

A. Radio-frequency identification (RFID): While RFID technology also facilitates automatic identification through radio waves, it requires specialized tags and scanners, as opposed to the straightforward visual scanning of barcodes. In this scenario, no RFID tags or readers are mentioned.

B. Near-field communication (NFC): NFC is similar to RFID but is specifically designed for contactless payments and requires very short-range interaction. The process described in the scenario involves scanning barcodes, not NFC capabilities. There's no indication of payment being processed via NFC, thus making it incorrect.

C. QUIC: This protocol is irrelevant within the context of physical product scanning. QUIC focuses on improving web transport layer protocols and does not apply to the transactional process being examined.

Authoritative References:

https://www.gs1.org/standards/barcode-technology
https://www.rfidjournal.com/what-is-rfid
https://www.nfc-forum.org/what-is-nfc/

Question: 26

Hayes, a security professional, was tasked with the implementation of security controls for an industrial network at the Purdue level 3.5 (IDMZ). Hayes verified all the possible attack vectors on the IDMZ level and deployed a security control that fortifies the IDMZ against cyber-attacks.
Identify the security control implemented by Hayes in the above scenario.

A. Point-to-point communication
B. MAC authentication
C. Anti-DoS solution
D. Use of authorized RTU and PLC commands

Answer: C

Explanation:

C is correct because an Anti-DoS solution effectively mitigates risks associated with denial-of-service attacks, which are particularly threatening to industrial networks.

In cybersecurity, especially in complex systems like those operating at the Purdue model level 3.5, the

Question: 30

Andre, a security professional, was tasked with segregating the employees' names, phone numbers, and credit card numbers before sharing the database with clients. For this purpose, he implemented a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#).
Which of the following techniques was employed by Andre in the above scenario?

A. Tokenization
B. Masking
C. Hashing
D. Bucketing

Answer: B

Explanation:

B is correct because masking effectively conceals sensitive data by replacing it with non-sensitive equivalents, such as asterisks or hashes, while preserving the data structure.

Masking is a vital data protection strategy that allows for the use of required data fields in a functional capacity without exposing sensitive information. In this case, Andre's strategy focuses on maintaining confidentiality of employees' critical details, thereby allowing their utility without actual disclosure. This selective visibility aligns with regulatory compliance and data protection requirements.

Critical Evaluation of Other Options:

A. **Tokenization**: This procedure involves replacing sensitive data with non-sensitive equivalents called tokens, which can be mapped back to the original data. Unlike masking, tokenization preserves the original data's integrity and allows for reversible mapping, which is not the aim in Andre's approach where the visibility is entirely eliminated.

C. **Hashing**: Hashing generates a unique fixed-size string from input data through one-way transformation. While it provides a level of obscurity, it does not allow data recovery or restoration of the original information —contradicting the need for data usability that masking offers.

D. **Bucketing**: This technique categorizes data into groups or 'buckets' based on certain attributes, which does not fundamentally alter or conceal individual data points but merely organizes them. Thus, it lacks the protective element inherent to masking.

For those looking to delve deeper into these concepts, here are some authoritative references:

https://www.ibm.com/docs/en/was-liberty/latest?topic=security-data-masking
https://www.owasp.org/index.php/Data_Masking_Cheat_Sheet
https://www.csoonline.com/article/3533790/understanding-data-masking-uses-and-benefits.html

Question: 31

Ryleigh, a system administrator, was instructed to perform a full back up of organizational data on a regular basis. For this purpose, she used a backup technique on a fixed date when the employees are not accessing the system i.e., when a service-level down time is allowed a full backup is taken.
Identify the backup technique utilized by Ryleigh in the above scenario.

case, the identification of packet drops at the gateway aligns with the primary function of traceroute, which is to analyze the path a packet takes and where it may be disrupted.

Evaluation of options:

A. dnsenurn: This option is incorrect as 'dnsenurn' seems to be a typographical error or a non-standard term. The relevant utility is DNS-related, primarily querying domain name systems, which does not assist in identifying packet drops.
B. arp: The Address Resolution Protocol (ARP) is used for mapping IP addresses to MAC addresses on a local network. It does not track packet loss through the network; rather, it resolves network layer addresses at the data link layer, making it inappropriate for diagnosing packet drops.
D. ipconfig: This tool is used for configuring IP parameters and viewing the system's network interfaces, but it does not trace the route taken by packets or identify points of failure. Therefore, it lacks the capability to analyze packet loss across the network path.

Given the critical role of traceroute in network diagnostics, its deployment by Steve is justified as the most effective method for uncovering the location of packet loss in this scenario.

References:

https://www.cloudflare.com/learning/network-layer/what-is-traceroute/
https://www.networkworld.com/article/3280161/how-traceroute-works.html
https://www.geeksforgeeks.org/traceroute-in-computer-network/

Question: 34

Anderson, a security engineer, was Instructed to monitor all incoming and outgoing traffic on the organization's network to identify any suspicious traffic. For this purpose, he employed an analysis technique using which he analyzed packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit.
Identify the type of attack signature analysis performed by Anderson in the above scenario.

A. Context-based signature analysis
B. Atomic-signature-based analysis
C. Composite-signature-based analysis
D. Content-based signature analysis

Answer: A

Explanation:

A is correct because context-based signature analysis focuses on evaluating various fields in packet headers to assess the integrity and behavior of network traffic.

Context-based signature analysis allows security engineers to detect anomalies by examining header fields such as IP options and fragmentation flags. This method is particularly effective for identifying tampered packets, as it considers the operational context of network traffic and correlates expected behaviors with observed anomalies. Thus, when Anderson employs this technique, he is using the inherent context of packet transmission to discern malicious activities.

Critical Evaluation of Other Options:

B. **Atomic-signature-based analysis**: This approach identifies attacks using single characteristics or properties of packets independently. It lacks the holistic view essential for identifying complex attack

D. Incident triage

Answer: A

Explanation:

A. Containment is correct because Warren took immediate action to restrict the malware's spread within the organization's network.

Justification:
Containment is a crucial step in incident handling, aimed at limiting the scope and impact of an active threat. By implementing measures to stop the infection from propagating to other assets, Warren effectively prioritized the organization's immediate safety and operational integrity. This step is essential in preventing further exploitation and protecting critical systems, thus minimizing operational disruption and financial loss.

Critique of Other Options:

B. Recovery: This step involves restoring systems to normal operations after an incident has been resolved. Since Warren focused on immediate containment rather than restoration, this option is inaccurate.

C. Eradication: This step entails completely removing the threat from the environment. Although an eventual goal, Warren's immediate actions were not directed at eradication but rather at halting the threat's spread. Thus, this option does not align with his initial response.

D. Incident triage: This phase involves assessing the incident's severity and categorizing it for response. While triage is essential, it precedes containment. Warren's actions indicated he was well past the initial assessment phase, focusing instead on immediate containment measures.

References:

https://www.cisecurity.org/white-papers/cyber-incident-response-policy-template/
https://www.nist.gov/publications/nist-special-publication-800-61-revision-2-computer-security-incident-handling-guide
https://www.sans.org/white-papers/40153/