Free Questions for 212-82

Shared by Lester on 04-10-2024

For More Free Questions and Preparation Resources

Question 1

Rickson, a security professional at an organization, was instructed to establish short-range communication between devices within a range of 10 cm. For this purpose, he used a mobile connection method that employs electromagnetic induction to enable communication between devices. The mobile connection method selected by Rickson can also read RFID tags and establish Bluetooth connections with nearby devices to exchange information such as images and contact lists.

Which of the following mobile connection methods has Rickson used in above scenario?

Options:

A- NFC

B- Satcom

C- Cellular communication

D- ANT

Answer:

A

Explanation:

NFC (Near Field Communication) is the mobile connection method that Rickson has used in the above scenario. NFC is a short-range wireless communication technology that enables devices to exchange data within a range of 10 cm. NFC employs electromagnetic induction to create a radio frequency field between two devices. NFC can also read RFID tags and establish Bluetooth connections with nearby devices to exchange information such as images and contact lists . Satcom (Satellite Communication) is a mobile connection method that uses satellites orbiting the earth to provide communication services over long distances. Cellular communication is a mobile connection method that uses cellular networks to provide voice and data services over wireless devices. ANT is a low-power wireless communication technology that enables devices to create personal area networks and exchange data over short distances.

Question 2

Question Type: **MultipleChoice**

Matias, a network security administrator at an organization, was tasked with the implementation of secure wireless network encryption for their network. For this purpose, Matias employed a security solution that uses 256-bit Galois/Counter Mode Protocol (GCMP-256) to maintain the authenticity and confidentiality of data.

Identify the type of wireless encryption used by the security solution employed by Matias in the above scenario.

Options:

A- WPA2 encryption

B- WPA3 encryption

C- WEP encryption

D- WPA encryption

Answer:

B

Explanation:

WPA3 encryption is the type of wireless encryption used by the security solution employed by Matias in the above scenario. WPA3 encryption is the latest and most secure version of Wi-Fi Protected Access, a protocol that provides authentication and encryption for wireless networks. WPA3 encryption uses 256-bit Galois/Counter Mode Protocol (GCMP-256) to maintain the authenticity and confidentiality of data. WPA3 encryption also provides enhanced protection against offline dictionary attacks, forward secrecy, and secure public Wi-Fi access . WPA2 encryption is the previous version of Wi-Fi Protected Access, which uses Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) for data encryption. WEP encryption is an outdated and insecure version of Wi-Fi security, which uses RC4 stream cipher for data encryption. WPA encryption is an intermediate version of Wi-Fi security, which uses TKIP for data encryption.

Question 3

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?

Options:

A- WiMAX

B- RFID

C- Bluetooth

D- Wi-Fi

Answer:

B

Explanation:

RFID (Radio Frequency Identification) is the wireless technology that the software company has implemented in the above scenario.RFID uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects1112.WiMAX (Worldwide Interoperability for Microwave Access) is a wireless technology that provides high-speed broadband access over long distances13.Bluetooth is a wireless technology that enables short-range data communication between devices, such as phones, laptops, printers, etc.14.Wi-Fi (Wireless Fidelity) is a wireless technology that allows devices to connect to a local area network or the internet using radio waves

Question 4

Question Type: **MultipleChoice**

Walker, a security team member at an organization, was instructed to check if a deployed cloud service is working as expected. He performed an independent examination of cloud service controls to verify adherence to standards through a review of objective evidence. Further, Walker evaluated the services provided by the CSP regarding security controls, privacy impact, and performance.

Identify the role played by Walker in the above scenario.

Options:

A- Cloud auditor

B- Cloud provider

C- Cloud carrier

D- Cloud consumer

Answer:

A

Explanation:

A cloud auditor is a role played by Walker in the above scenario. A cloud auditor is a third party who examines controls of cloud computing service providers.Cloud auditor performs an audit to verify compliance with the standards and expressed his opinion through a report89.A cloud provider is an entity that provides cloud services, such as infrastructure, platform, or software, to cloud consumers10.A cloud carrier is an entity that provides connectivity and transport of cloud services between cloud providers and cloud consumers10.A cloud consumer is an entity that uses cloud services for its own purposes or on behalf of another entity

Question 5

Question Type: **MultipleChoice**

Nicolas, a computer science student, decided to create a guest OS on his laptop for different lab operations. He adopted a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS.

Which of the following virtualization approaches has Nicolas adopted in the above scenario?

Options:

A- Hardware-assisted virtualization

B- Full virtualization

C- Hybrid virtualization

D- OS-assisted virtualization

Answer:

A

Explanation:

Hardware-assisted virtualization is a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS.Hardware-assisted virtualization relies on special hardware features in the CPU and chipset to create and manage virtual machines efficiently and securely34.Full virtualization is a virtualization approach in which the guest

OS will not be aware that it is running in a virtualized environment, but the VMM will run in software and emulate all the hardware resources for each virtual machine5.Hybrid virtualization is a virtualization approach that combines hardware-assisted and full virtualization techniques to optimize performance and compatibility6.OS-assisted virtualization is a virtualization approach in which the guest OS will be modified to run in a virtualized environment and cooperate with the VMM to access the hardware resources

Question 6

Question Type: **MultipleChoice**

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?

Options:

A- Development

B- Testing

C- Quality assurance (QA)

D- Staging

Answer:

B

Explanation:

The testing tier of a secure application development lifecycle involves checking the performance of the application on the client's network to determine whether end users are facing any issues in accessing the application. Testing is a crucial phase of software development that ensures the quality, functionality, reliability, and security of the application.Testing can be done manually or automatically using various tools and techniques, such as unit testing, integration testing, system testing, regression testing, performance testing, usability testing, security testing, and acceptance testing

Question 7

Question Type: **MultipleChoice**

Miguel, a professional hacker, targeted an organization to gain illegitimate access to its critical information. He identified a flaw in the end-point communication that can disclose the target application's data.

Which of the following secure application design principles was not met by the application in the above scenario?

Options:

A- Secure the weakest link

B- Do not trust user input

C- Exception handling

D- Fault tolerance

Answer:

C

Explanation:

Exception handling is a secure application design principle that states that the application should handle errors and exceptions gracefully and securely, without exposing sensitive information or compromising the system's functionality. Exception handling can help prevent attackers from exploiting errors or exceptions to gain access to data or resources or cause denial-of-service attacks. In the scenario, Miguel identified a flaw in the end-point communication that can disclose the target application's data, which means that the application did not meet the exception handling principle.

Question 8

Tristan, a professional penetration tester, was recruited by an organization to test its network infrastructure. The organization wanted to understand its current security posture and its strength in defending against external threats. For this purpose, the organization did not provide any information about their IT infrastructure to Tristan. Thus, Tristan initiated zero-knowledge attacks, with no information or assistance from the organization.

Which of the following types of penetration testing has Tristan initiated in the above scenario?

Options:

A- Black-box testing

B- White-box testing

C- Gray-box testing

D- Translucent-box testing

Answer:

A

Explanation:

Black-box testing is a type of penetration testing where the tester has no prior knowledge of the target system or network and initiates zero-knowledge attacks, with no information or assistance from the organization. Black-box testing simulates the perspective of an external attacker who tries to find and exploit vulnerabilities without any insider information. Black-box testing can help identify unknown or hidden vulnerabilities that may not be detected by other types of testing. However, black-box testing can also be time-consuming, costly, and incomplete, as it depends on the tester's skills and tools.

Question 9

Question Type: **MultipleChoice**

An organization hired a network operations center (NOC) team to protect its IT infrastructure from external attacks. The organization utilized a type of threat intelligence to protect its resources from evolving threats. The threat intelligence helped the NOC team understand how attackers are expected to perform an attack on the organization, identify the information leakage, and determine the attack goals as well as attack vectors.

Identify the type of threat intelligence consumed by the organization in the above scenario.

Options:

A- Operational threat intelligence

B- Strategic threat intelligence

C- Technical threat intelligence

D- Tactical threat intelligence

Answer:

C

Explanation:

Technical threat intelligence is a type of threat intelligence that provides information about the technical details of specific attacks, such as indicators of compromise (IOCs), malware signatures, attack vectors, and vulnerabilities. Technical threat intelligence helps the NOC team understand how attackers are expected to perform an attack on the organization, identify the information leakage, and determine the attack goals as well as attack vectors. Technical threat intelligence is often consumed by security analysts, incident responders, and penetration testers who need to analyze and respond to active or potential threats.

Question 10

Question Type: **MultipleChoice**

Mark, a security analyst, was tasked with performing threat hunting to detect imminent threats in an organization's network. He generated a hypothesis based on the observations in the initial step and started the threat-hunting process using existing data collected from DNS and proxy logs.

Identify the type of threat-hunting method employed by Mark in the above scenario.

Options:

A- Entity-driven hunting

B- TTP-driven hunting

C- Data-driven hunting

D- Hybrid hunting

Answer:

C

Explanation:

A data-driven hunting method is a type of threat hunting method that employs existing data collected from various sources, such as DNS and proxy logs, to generate and test hypotheses about potential threats. This method relies on data analysis and machine learning techniques to identify patterns and anomalies that indicate malicious activity. A data-driven hunting method can help discover unknown or emerging threats that may evade traditional detection methods. An entity-driven hunting method is a type of threat hunting method

that focuses on specific entities, such as users, devices, or domains, that are suspected or known to be involved in malicious activity. A TTP-driven hunting method is a type of threat hunting method that leverages threat intelligence and knowledge of adversary tactics, techniques, and procedures (TTPs) to formulate and test hypotheses about potential threats. A hybrid hunting method is a type of threat hunting method that combines different approaches, such as data-driven, entity-driven, and TTP-driven methods, to achieve more comprehensive and effective results.