EC-Council

Exam Questions 212-82

Certified Cybersecurity Technician(C|CT)

NEW QUESTION 1
Sam, a software engineer, visited an organization to give a demonstration on a software tool that helps in business development. The administrator at the organization created a least privileged account on a system and allocated that system to Sam for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file in the system.
Which of the following types of accounts the organization has given to Sam in the above scenario?

A. Service account
B. Guest account
C. User account
D. Administrator account

Answer: B

Explanation:
The correct answer is B, as it identifies the type of account that the organization has given to Sam in the above scenario. A guest account is a type of account that allows temporary or limited access to a system or network for visitors or users who do not belong to the organization. A guest account typically has minimal privileges and permissions and can only access certain files or applications. In the above scenario, the organization has given Sam a guest account for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file in the system. Option A is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. A service account is a type of account that allows applications or services to run on a system or network under a specific identity. A service account typically has high privileges and permissions and can access various files or applications. In the above scenario, the organization has not given Sam a service account for the demonstration. Option C is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. A user account is a type of account that allows regular access to a system or network for employees or members of an organization. A user account typically has moderate privileges and permissions and can access various files or applications depending on their role. In the above scenario, the organization has not given Sam a user account for the demonstration. Option D is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. An administrator account is a type of account that allows full access to a system or network for administrators or managers of an organization. An administrator account typically has the highest privileges and permissions and can access and modify any files or applications. In the above scenario, the organization has not given Sam an administrator account for the demonstration.
References: , Section 4.1

NEW QUESTION 2
Tenda, a network specialist at an organization, was examining logged data using Windows Event Viewer to identify attempted or successful unauthorized activities. The logs analyzed by Tenda include events related to Windows security; specifically, log-on/log-off activities, resource access, and also information based on Windows system's audit policies.
Identify the type of event logs analyzed by Tenda in the above scenario.

A. Application event log
B. Setup event log
C. Security event log
D. System event log

Answer: C

Explanation:
Security event log is the type of event log analyzed by Tenda in the above scenario. Windows Event Viewer is a tool that displays logged data about various events that occur on a Windows system or network. Windows Event Viewer categorizes event logs into different types based on their source and purpose. Security event log is the type of event log that records events related to Windows security; specifically, log-on/log-off activities, resource access, and also information based on Windows system’s audit policies. Security event log can help identify attempted or successful unauthorized activities on a Windows system or network. Application event log is the type of event log that records events related to applications running on a Windows system, such as errors, warnings, or information messages. Setup event log is the type of event log that records events related to the installation or removal of software or hardware components on a Windows system. System event log is the type of event log that records events related to the operation of a Windows system or its components, such as drivers, services, processes, etc.

NEW QUESTION 3
Juan, a safety officer at an organization, installed a physical lock at the entrance of each floor. All employees in the organization were allotted a smart card embedded in their ID cards, which had to be swiped to unlock doors and Access any floor. Which of the following types of physical locks did Juan install In this scenario?

A. Mechanical locks
B. Digital locks
C. Combination locks
D. Electromagnetic locks

Answer: B

Explanation:
Digital locks are the types of physical locks that Juan installed in this scenario. A physical lock is a device that prevents or restricts access to a physical location or environment, such as a door, a cabinet, a drawer, etc. A physical lock can have different types based on its mechanism or technology. A digital lock is a type of physical lock that uses electronic or digital components, such as a keypad, a card reader, a fingerprint scanner, etc., to unlock or lock . A digital lock can be used to provide enhanced security and convenience to users, but it can also be vulnerable to hacking or tampering. In the scenario, Juan installed a physical lock at the entrance of each floor. All employees in the organization were allotted a smart card embedded in their ID cards, which had to be swiped to unlock doors and access any floor. This means that he installed digital locks for those doors. A mechanical lock is a type of physical lock that uses mechanical components, such as a key, a bolt, a latch, etc., to unlock or lock. A combination lock is a type of physical lock that uses a sequence of numbers or symbols, such as a dial, a wheel, or a keypad, to unlock or lock. An electromagnetic lock is a type of physical lock that uses an electromagnet and an armature plate to unlock or lock.

NEW QUESTION 4
Zayn, a network specialist at an organization, used Wireshark to perform network analysis. He selected a Wireshark menu that provided a summary ol captured packets, IO graphs, and flow graphs. Identify the Wireshark menu selected by Zayn in this scenario.

A. Status bar
B. Analyze
C. Statistics
D. Packet list panel

Answer: C

Explanation:
Statistics is the Wireshark menu selected by Zayn in this scenario. Statistics is a Wireshark menu that provides a summary of captured packets, IO graphs, and flow graphs. Statistics can be used to analyze various aspects of network traffic, such as protocols, endpoints, conversations, or packet lengths3.
References: Wireshark Statistics Menu

NEW QUESTION 5
Gideon, a forensic officer, was examining a victim's Linux system suspected to be involved in online criminal activities. Gideon navigated to a directory containing a log file that recorded information related to user login/logout. This information helped Gideon to determine the current login state of cyber criminals in the victim system, identify the Linux log file accessed by Gideon in this scenario.

A. /va r/l og /mysq l
B. log
C. /va r/l og /wt m p
D. /ar/log/boot.iog
E. /var/log/httpd/

Answer: B

Explanation:
/var/log/wtmp is the Linux log file accessed by Gideon in this scenario.
/var/log/wtmp is a log file that records information related to user login/logout, such as username, terminal, IP address, and login time. /var/log/wtmp can be used to determine the current login state of users in a Linux system. /var/log/wtmp can be viewed using commands such as last, lastb, or utmpdump1. References: Linux Log Files

NEW QUESTION 6
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-po int communication
B. MAC authentication
C. Anti-DoS solution
D. Use of authorized RTU and PLC commands

Answer: D

Explanation:
The use of authorized RTU and PLC commands is the security control implemented by Hayes in the above scenario. RTU (Remote Terminal Unit) and PLC (Programmable Logic Controller) are devices that control and monitor industrial processes, such as power generation, water treatment, oil and gas production, etc. RTU and PLC commands are instructions that are sent from a master station to a slave station to perform certain actions or request certain data. The use of authorized RTU and PLC commands is a security control that fortifies the IDMZ (Industrial Demilitarized Zone) against cyber- attacks by ensuring that only valid and authenticated commands are executed by the RTU and PLC devices. Point-to-point communication is a communication method that establishes a direct connection between two endpoints. MAC authentication is an authentication method that verifies the MAC (Media Access Control) address of a device before granting access to a network. Anti-DoS solution is a security solution that protects a network from DoS (Denial-of-Service) attacks by filtering or blocking malicious traffic.

NEW QUESTION 7
Nancy, a security specialist, was instructed to identify issues related to unexpected shutdown and restarts on a Linux machine. To identify the incident cause, Nancy navigated to a directory on the Linux system and accessed a log file to troubleshoot problems related to improper shutdowns and unplanned restarts.
Identify the Linux log file accessed by Nancy in the above scenario.

A. /var/log/secure
B. /var/log/kern.log
C. /var/log/boot.log
D. /var/log/lighttpd/

Answer: C

Explanation:
/var/log/boot.log is the Linux log file accessed by Nancy in the above scenario. Linux is an open-source operating system that logs various events and activities on the system or network. Linux log files are stored in the /var/log directory, which contains different types of log files for different purposes. /var/log/boot.log is the type of log file that records events related to the booting process of the Linux system, such as loading drivers, services, modules, etc. /var/log/boot.log can help identify issues related to unexpected shutdowns and restarts on a Linux machine . /var/log/secure is the type of log file that records events related to security and authentication, such as logins, logouts, password changes, sudo commands, etc. /var/log/kern.log is the type of log file that records events related to the kernel, such as kernel messages, errors, warnings, etc. /var/log/lighttpd/ is the directory that contains log files related to the lighttpd web server, such as access logs, error logs, etc.

NEW QUESTION 8
Richard, a professional hacker, was hired by a marketer to gather sensitive data and information about the offline activities of users from location data. Richard employed a technique to determine the proximity of a user's mobile device to an exact location using CPS features. Using this technique. Richard placed a virtual barrier positioned at a static location to interact with mobile users crossing the barrier, identify the technique employed by Richard in this scenario.

A. Containerization
B. Over-the-air (OTA) updates
C. Full device encryption
D. Ceofencing

Answer: D

Explanation:
Geofencing is a technique that uses GPS features to determine the proximity of a user's mobile device to an exact location. Geofencing can be used to create a virtual barrier positioned at a static location to interact with mobile users crossing the barrier. Geofencing can be used for marketing, security, and tracking purposes2.
References: What is Geofencing?

NEW QUESTION 9
You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?

A. Reconnaissance
B. Command and control
C. Weaponization
D. Exploitation

Answer: C

Explanation:
Weaponization is the stage of the cyber kill chain that you are at in the above scenario. The cyber kill chain is a model that describes the phases of a cyberattack from the perspective of the attacker. The cyber kill chain consists of seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Reconnaissance is the stage of the cyber kill chain that involves gathering information about the target, such as IP addresses, domain names, vulnerabilities, etc. Weaponization is the stage of the cyber kill chain that involves creating a malicious payload or tool that can exploit the target's vulnerabilities. Weaponization can include creating a client-side backdoor to send it to the employees via email. Delivery is the stage of the cyber kill chain that involves transmitting or delivering the weaponized payload or tool to the target's system or network. Exploitation is the stage of the cyber kill chain that involves executing or triggering the weaponized payload or tool on the target's system or network.

NEW QUESTION 10
Martin, a network administrator at an organization, received breaching alerts for an application. He identified that a vulnerability in the application allowed attackers to enter malicious input. Martin evaluated the threat severity and extent of damage that could be caused by this vulnerability. He then escalated the issue to the security management team to determine appropriate mitigation strategies. In which of the following threat-modeling steps did Martin evaluate the severity level of the threat?

A. Identify vulnerabilities
B. Application overview
C. Risk and impact analysis
D. Decompose the application

Answer: C

Explanation:
Risk and impact analysis is the threat-modeling step in which Martin evaluated the severity level of the threat in the above scenario. Threat modeling is a process that involves identifying, analyzing, and mitigating threats and risks to a system or network. Threat modeling can be used to improve the security and resilience of a system or network by applying various methods or techniques, such as STRIDE, DREAD, PASTA, etc. Threat modeling consists of various steps or phases that perform different tasks or roles. Risk and impact analysis is a threat-modeling step that involves assessing the likelihood and consequences of threats and risks to a system or network . Risk and impact analysis can be used to evaluate the severity level of threats and risks and prioritize them for mitigation . In the scenario, Martin received breaching alerts for an application. He identified that a vulnerability in the application allowed attackers to enter malicious input. Martin evaluated the threat severity and extent of damage that could be caused by this vulnerability. He then escalated the issue to the security management team to determine appropriate mitigation strategies. This means that he performed risk and impact analysis for this purpose. Identify vulnerabilities is a threat-modeling step that involves finding and documenting the weaknesses or flaws in a system or network that can be exploited by threats or risks . Application overview is a threat-modeling step that involves defining and understanding the scope, architecture, components, and functionality of a system or network . Decompose the application is a threat-modeling step that involves breaking down a system or network into smaller and simpler elements, such as data flows, processes, assets, etc.

NEW QUESTION 10
Desmond, a forensic officer, was investigating a compromised machine involved in various online attacks. For this purpose. Desmond employed a forensic tool to extract and analyze computer-based evidence to retrieve information related to websites accessed from the victim machine. Identify the computer-created evidence retrieved by Desmond in this scenario.

A. Cookies
B. Documents
C. Address books
D. Compressed files

Answer: A

Explanation:
Cookies are the computer-created evidence retrieved by Desmond in this scenario. Cookies are small files that are stored on a user's computer by a web browser when the user visits a website. Cookies can contain information such as user preferences, login details, browsing history, or tracking data. Cookies can be used to extract and analyze computer-based evidence to retrieve information related to websites accessed from the victim machine2. References: Cookies

NEW QUESTION 14
Wilson, a security specialist in an organization, was instructed to enhance its cloud network security. To achieve this, Wilson deployed a network routing solution that established and managed communication between the on-premises consumer network and VPCs via a centralized unit. Identity the method used by Wilson to

achieve cloud network security in this scenario.

A. Virtual private cloud (VPC)
B. Public and private subnets
C. Transit gateways
D. VPC endpoint

Answer: C

Explanation:
Transit gateways are the method used by Wilson to achieve cloud network security in this scenario. Cloud network security is a branch of cybersecurity that focuses on protecting and securing the network infrastructure and traffic in a cloud environment. Cloud network security can involve various methods or techniques, such as encryption, firewall, VPN, IDS/IPS, etc. Transit gateways are a method of cloud network security that provide a network routing solution that establishes and manages communication between on-premises consumer networks and VPCs (Virtual Private Clouds) via a centralized unit . Transit gateways can be used to simplify and secure the connectivity between different networks or VPCs in a cloud environment . In the scenario, Wilson was instructed to enhance its cloud network security. To achieve this, Wilson deployed a network routing solution that established and managed communication between the on-premises consumer network and VPCs via a centralized unit. This means that he used transit gateways for this purpose. A virtual private cloud (VPC) is not a method of cloud network security, but a term that describes an isolated and private section of a public cloud that provides exclusive access to cloud resources to a single organization or entity . A VPC can be used to create and configure virtual networks in a cloud environment . Public and private subnets are not methods of cloud network security, but terms that describe segments of a VPC that have different levels of accessibility or visibility . A public subnet is a segment of a VPC that can be accessed from the internet or other networks . A private subnet is a segment of a VPC that cannot be accessed from the internet or other networks . A VPC endpoint is not a method of cloud network security, but a term that describes an interface that allows private connectivity between a VPC and other AWS (Amazon Web Services) services or resources.

NEW QUESTION 19
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.

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.

NEW QUESTION 20
Shawn, a forensic officer, was appointed to investigate a crime scene that had occurred at a coffee shop. As a part of investigation, Shawn collected the mobile device from the victim, which may contain potential evidence to identify the culprits.
Which of the following points must Shawn follow while preserving the digital evidence? (Choose three.)

A. Never record the screen display of the device
B. Turn the device ON if it is OFF
C. Do not leave the device as it is if it is ON
D. Make sure that the device is charged

Answer: BCD

Explanation:
Turn the device ON if it is OFF, do not leave the device as it is if it is ON, and make sure that the device is charged are some of the points that Shawn must follow while preserving the digital evidence in the above scenario. Digital evidence is any information or data stored or transmitted in digital form that can be used in a legal proceeding or investigation. Digital evidence can be found on various devices, such as computers, mobile phones, tablets, etc. Preserving digital evidence is a crucial step in forensic investigation that involves protecting and maintaining the integrity and authenticity of digital evidence from any alteration or damage.
Some of the points that Shawn must follow while preserving digital evidence are:
? Turn the device ON if it is OFF: If the device is OFF, Shawn must turn it ON to prevent any data loss or encryption that may occur when the device is powered off. Shawn must also document any password or PIN required to unlock or access the device.
? Do not leave the device as it is if it is ON: If the device is ON, Shawn must not leave it as it is or use it for any purpose other than preserving digital evidence. Shawn must also disable any network connections or communication features on the device, such as Wi-Fi, Bluetooth, cellular data, etc., to prevent any remote access or deletion of data by unauthorized parties.
? Make sure that the device is charged: Shawn must ensure that the device has enough battery power to prevent any data loss or corruption that may occur due to sudden shutdown or low battery. Shawn must also use a write blocker or a Faraday bag to isolate the device from any external interference or signals.
Never record the screen display of the device is not a point that Shawn must follow while preserving digital evidence. On contrary, Shawn should record or photograph the screen display of the device to capture any relevant information or messages that may appear on the screen. Recording or photographing the screen display of the device can also help document any changes or actions performed on the device during preservation.

NEW QUESTION 22
Paul, a computer user, has shared information with his colleague using an online application. The online application used by Paul has been incorporated with the latest encryption mechanism. This mechanism encrypts data by using a sequence of photons that have a spinning trait while traveling from one end to another, and these photons keep changing their shapes during their course through filters: vertical, horizontal, forward slash, and backslash.
Identify the encryption mechanism demonstrated in the above scenario.

A. Quantum cryptography

B. Homomorphic encryption
C. Rivest Shamir Adleman encryption
D. Elliptic curve cryptography

Answer: A

Explanation:
Quantum cryptography is the encryption mechanism demonstrated in the above scenario. Quantum cryptography is a branch of cryptography that uses quantum physics to secure data transmission and communication. Quantum cryptography encrypts data by using a sequence of photons that have a spinning trait, called polarization, while traveling from one end to another. These photons keep changing their shapes, called states, during their course through filters: vertical, horizontal, forward slash, and backslash. Quantum cryptography ensures that any attempt to intercept or tamper with the data will alter the quantum states of the photons and be detected by the sender and receiver . Homomorphic encryption is a type of encryption that allows computations to be performed on encrypted data without decrypting it first. Rivest Shamir Adleman (RSA) encryption is a type of asymmetric encryption that uses two keys, public and private, to encrypt and decrypt data. Elliptic curve cryptography (ECC) is a type of asymmetric encryption that uses mathematical curves to generate keys and perform encryption and decryption.

NEW QUESTION 25
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.

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.

NEW QUESTION 29
Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

A. HIPPA/PHl
B. Pll
C. PCIDSS
D. ISO 2002

Answer: A

Explanation:
HIPPA/PHI is the regulation that is mostly violated in the above scenario. HIPPA (Health Insurance Portability and Accountability Act) is a US federal law that sets standards for protecting the privacy and security of health information. PHI (Protected Health Information) is any information that relates to the health or health care of an individual and that can identify the individual, such as name, address, medical records, etc. HIPPA/PHI requires covered entities, such as health care providers, health plans, or health care clearinghouses, and their business associates, to safeguard PHI from unauthorized access, use, or disclosure . In the scenario, the medical company experienced a major cyber security breach that exposed the personal medical records of many patients on the internet, which violates HIPPA/PHI regulations. PII (Personally Identifiable Information) is any information that can be used to identify a specific individual, such as name, address, social security number, etc. PII is not specific to health information and can be regulated by various laws, such as GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), etc. PCI DSS (Payment Card Industry Data Security Standard) is a set of standards that applies to entities that store, process, or transmit payment card information, such as merchants, service providers, or payment processors. PCI DSS requires them to protect cardholder data from unauthorized access, use, or disclosure. ISO 2002 (International Organization for Standardization 2002) is not a regulation, but a standard for information security management systems that provides guidelines and best practices for organizations to manage their information security risks.

NEW QUESTION 32
An attacker with malicious intent used SYN flooding technique to disrupt the network and gain advantage over the network to bypass the Firewall. You are working with a security architect to design security standards and plan for your organization. The network traffic was captured by the SOC team and was provided to you to perform a detailed analysis. Study the Synflood.pcapng file and determine the source IP address.
Note: Synflood.pcapng file is present in the Documents folder of Attacker-1 machine.

A. 20.20.10.180
B. 20.20.10.19
C. 20.20.10.60
D. 20.20.10.59

Answer: B

Explanation:
20.20.10.19 is the source IP address of the SYN flooding attack in the above scenario. SYN flooding is a type of denial-of-service (DoS) attack that exploits the TCP (Transmission Control Protocol) three-way handshake process to disrupt the network and gain advantage over the network to bypass the firewall. SYN flooding sends a large number of SYN packets with spoofed source IP addresses to a target server, causing it to allocate resources and wait for the corresponding ACK packets that never arrive. This exhausts the server’s resources and prevents it from accepting legitimate requests . To determine the source IP address of the SYN flooding attack, one has to follow these steps:
? Navigate to the Documents folder of Attacker-1 machine.

? Double-click on Synflood.pcapng file to open it with Wireshark.
? Click on Statistics menu and select Conversations option.
? Click on TCP tab and sort the list by Bytes column in descending order.
? Observe the IP address that has sent the most bytes to 20.20.10.26 (target server).
The IP address that has sent the most bytes to 20.20.10.26 is 20.20.10.19 , which is the source IP address of the SYN flooding attack.

NEW QUESTION 35
Lorenzo, a security professional in an MNC, was instructed to establish centralized authentication, authorization, and accounting for remote-access servers. For this purpose, he implemented a protocol that is based on the client-server model and works at the transport layer of the OSI model.
Identify the remote authentication protocol employed by Lorenzo in the above scenario.

A. SNMPv3
B. RADIUS
C. POP3S
D. IMAPS

Answer: B

Explanation:
The correct answer is B, as it identifies the remote authentication protocol employed by Lorenzo in the above scenario. RADIUS (Remote Authentication Dial-In User Service) is a protocol that provides centralized authentication, authorization, and accounting (AAA) for remote-access servers such as VPNs (Virtual Private Networks), wireless networks, or dial-up connections. RADIUS is based on the client-server model and works at the transport layer of the OSI model. RADIUS uses UDP (User Datagram Protocol) as its transport protocol and encrypts only user passwords in its messages. In the above scenario, Lorenzo implemented RADIUS to provide centralized AAA for remote-access servers. Option A is incorrect, as it does not identify the remote authentication protocol employed by Lorenzo in the above scenario. SNMPv3 (Simple Network Management Protocol version 3) is a protocol that provides network management and monitoring for network devices such as routers, switches, servers, or printers. SNMPv3 is based on the manager-agent model and works at the application layer of the OSI model. SNMPv3 uses UDP as its transport protocol and encrypts all its messages with AES (Advanced Encryption Standard) or DES (Data Encryption Standard). In the above scenario, Lorenzo did not implement SNMPv3 to provide network management and monitoring for network devices. Option C is incorrect, as it does not identify the remote authentication protocol employed by Lorenzo in the above scenario. POP3S (Post Office Protocol version 3 Secure) is a protocol that provides secure email access and retrieval for email clients from email servers. POP3S is based on the client-server model and works at the application layer of the OSI model. POP3S uses TCP (Transmission Control Protocol) as its transport protocol and encrypts all its messages with SSL (Secure Sockets Layer) or TLS (Transport Layer Security). In the above scenario, Lorenzo did not implement POP3S to provide secure email access and retrieval for email clients from email servers. Option D is incorrect, as it does not identify the remote authentication protocol employed by Lorenzo in the above scenario. IMAPS (Internet Message Access Protocol Secure) is a protocol that provides secure email access and management for email clients from email servers. IMAPS is based on the client-server model and works at the application layer of the OSI model. IMAPS uses TCP as its transport protocol and encrypts all its messages with SSL or TLS. In the above scenario, Lorenzo did not implement IMAPS to provide secure email access and management for email clients from email servers.
References: , Section 8.2

NEW QUESTION 36
Brielle. a security professional, was instructed to secure her organization's network from malicious activities. To achieve this, she started monitoring network activities on a control system that collected event data from various sources. During this process. Brielle observed that a malicious actor had logged in to access a network device connected to the organizational network. Which of the following types of events did Brielle identify in the above scenario?

A. Failure audit
B. Error
C. Success audit
D. Warning

Answer: C

Explanation:
Success audit is the type of event that Brielle identified in the above scenario. Success audit is a type of event that records successful attempts to access a network device or resource. Success audit can be used to monitor authorized activities on a network, but it can also indicate unauthorized activities by malicious actors who have compromised credentials or bypassed security controls4.
References: Success Audit Event

NEW QUESTION 38
Jaden, a network administrator at an organization, used the ping command to check the status of a system connected to the organization's network. He received an ICMP error message stating that the IP header field contains invalid information. Jaden examined the ICMP packet and identified that it is an IP parameter problem.
Identify the type of ICMP error message received by Jaden in the above scenario.

A. Type =12
B. Type = 8
C. Type = 5
D. Type = 3

Answer: A

Explanation:
Type = 12 is the type of ICMP error message received by Jaden in the above scenario. ICMP (Internet Control Message Protocol) is a protocol that sends error and control messages between network devices. ICMP error messages are categorized by types and codes, which indicate the cause and nature of the error. Type = 12 is the type of ICMP error message that indicates an IP parameter problem, which means that the IP header field contains invalid information . Type = 8 is the type of ICMP message that indicates an echo request, which is used to test the connectivity and reachability of a destination host. Type = 5 is the type of ICMP error message that indicates a redirect, which means that a better route to the destination host is available. Type = 3 is the type of ICMP error message that indicates a destination unreachable, which means that the destination host or network cannot be reached.

NEW QUESTION 39
You are Harris working for a web development company. You have been assigned to perform a task for vulnerability assessment on the given IP address

20.20.10.26. Select the vulnerability that may affect the website according to the severity factor.
Hint: Greenbone web credentials: admin/password

A. TCP timestamps
B. Anonymous FTP Login Reporting
C. FTP Unencrypted Cleartext Login
D. UDP timestamps

Answer: C

Explanation:
FTP Unencrypted Cleartext Login is the vulnerability that may affect the website according to the severity factor in the above scenario. A vulnerability is a weakness or flaw in a system or network that can be exploited by an attacker to compromise its security or functionality. A vulnerability assessment is a process that involves identifying, analyzing, and evaluating vulnerabilities in a system or network using various tools and techniques. Greenbone is a tool that can perform vulnerability assessment on various targets using various tests and scans. To perform a vulnerability assessment on the given IP address 20.20.10.26, one has to follow these steps:
? Open a web browser and type 20.20.10.26:9392
? Press Enter key to access the Greenbone web interface.
? Enter admin as username and password as password.
? Click on Login button.
? Click on Scans menu and select Tasks option.
? Click on Start Scan icon next to IP Address Scan task.
? Wait for the scan to complete and click on Report icon next to IP Address Scan task.
? Observe the vulnerabilities found by the scan.
The vulnerabilities found by the scan are:

Name	Severity
TCP timestamps	Low
Anonymous FTP Login Reporting	Low
FTP Unencrypted Cleartext Login	Medium
UDP timestamps	Low

The vulnerability that may affect the website according to the severity factor is FTP Unencrypted Cleartext Login, which has a medium severity level. FTP Unencrypted Cleartext Login is a vulnerability that allows an attacker to intercept or sniff FTP login credentials that are sent in cleartext over an unencrypted connection. An attacker can use these credentials to access or modify files or data on the FTP server. TCP timestamps and UDP timestamps are vulnerabilities that allow an attacker to estimate the uptime of a system or network by analyzing the timestamp values in TCP or UDP packets. Anonymous FTP Login Reporting is a vulnerability that allows an attacker to access an FTP server anonymously without providing any username or password.

NEW QUESTION 43
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?

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.

NEW QUESTION 44
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:
Masking is the technique that Andre employed in the above scenario. Masking is a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#). Masking can help protect sensitive data from unauthorized access or disclosure, while preserving the format and structure of the original data . Tokenization is a deidentification technique that can replace the critical information in database fields with random tokens that have no meaning or relation to the original data. Hashing is a deidentification technique that can transform the critical information in database fields into fixed-length strings using a mathematical function. Bucketing is a deidentification technique that can group the critical information in database fields into ranges or categories based on certain criteria.

NEW QUESTION 49
Kasen, a cybersecurity specialist at an organization, was working with the business continuity and disaster recovery team. The team initiated various business continuity and discovery activities in the organization. In this process, Kasen established a program to restore both the disaster site and the damaged materials to the pre-disaster levels during an incident.
Which of the following business continuity and disaster recovery activities did Kasen perform in the above scenario?

A. Prevention
B. Resumption
C. Response
D. Recovery

Answer: D

Explanation:
Recovery is the business continuity and disaster recovery activity that Kasen performed in the above scenario. Business continuity and disaster recovery (BCDR) is a process that involves planning, preparing, and implementing various activities to ensure the continuity of critical business functions and the recovery of essential resources in the event of a disaster or disruption. BCDR activities can be categorized into four phases: prevention, response, resumption, and recovery . Prevention is the BCDR phase that involves identifying and mitigating potential risks and threats that can cause a disaster or disruption. Response is the BCDR phase that involves activating the BCDR plan and executing the immediate actions to protect people, assets, and operations during a disaster or disruption. Resumption is the BCDR phase that involves restoring the minimum level of services and functions required to resume normal business operations after a disaster or disruption. Recovery is the BCDR phase that involves restoring both the disaster site and the damaged materials to the pre-disaster levels during an incident.

NEW QUESTION 52
Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?

A. Desynchronization
B. Obfuscating
C. Session splicing
D. Urgency flag

Answer: B

Explanation:
Obfuscating is the technique used by Kevin to evade the IDS system in the above scenario. Obfuscating is a technique that involves encoding or modifying packets or data with various methods or characters to make them unreadable or unrecognizable by an IDS (Intrusion Detection System). Obfuscating can be used to bypass or evade an IDS system that relies on signatures or patterns to detect malicious activities. Obfuscating can include encoding packets with Unicode characters, which are characters that can represent various languages and symbols. The IDS system cannot recognize the packet, but the target web server can decode them and execute them normally. Desynchronization is a technique that involves creating discrepancies or inconsistencies between the state of a connection as seen by an IDS system and the state of a connection as seen by the end hosts. Desynchronization can be used to bypass or evade an IDS system that relies on stateful inspection to track and analyze connections. Desynchronization can include sending packets with invalid sequence numbers, which are numbers that indicate the order of packets in a connection. Session splicing is a technique that involves splitting or dividing packets or data into smaller fragments or segments to make them harder to detect by an IDS system. Session splicing can be used to bypass or evade an IDS system that relies on packet size or content to detect malicious activities. Session splicing can include sending packets with small MTU (Maximum Transmission Unit) values, which are values that indicate the maximum size of packets that can be transmitted over a network. An urgency flag is a flag in the TCP (Transmission Control Protocol) header that indicates that the data in the packet is urgent and should be processed immediately by the receiver. An urgency flag is not a technique to evade an IDS system, but it can be used to trigger an IDS system to generate an alert or a response.

NEW QUESTION 54
An organization divided its IT infrastructure into multiple departments to ensure secure connections for data access. To provide high-speed data access, the administrator implemented a PAID level that broke data into sections and stored them across multiple drives. The storage capacity of this RAID level was equal to the sum of disk capacities in the set. which of the following RAID levels was implemented by the administrator in the above scenario?

A. RAID Level 0
B. RAID Level 3
C. RAID Level 5
D. RAID Level 1

Answer: A

Explanation:
RAID Level 0 is the RAID level that was implemented by the administrator in the above scenario. RAID Level 0 is also known as striping, which breaks data into sections and stores them across multiple drives. RAID Level 0 provides high-speed data access and increases performance, but it does not provide any redundancy or fault tolerance. The storage capacity of RAID Level 0 is equal to the sum of disk capacities in the set3. References: RAID Level 0

NEW QUESTION 55
Ruben, a crime investigator, wants to retrieve all the deleted files and folders in the suspected media without affecting the original files. For this purpose, he uses a method that involves the creation of a cloned copy of the entire media and prevents the contamination of the original media.
Identify the method utilized by Ruben in the above scenario.

A. Sparse acquisition
B. Bit-stream imaging
C. Drive decryption
D. Logical acquisition

Answer: B

Explanation:

Bit-stream imaging is the method utilized by Ruben in the above scenario.
Bit-stream imaging is a method that involves creating a cloned copy of the entire media and prevents the contamination of the original media. Bit-stream imaging copies all the data on the media, including deleted files and folders, hidden partitions, slack space, etc., at a bit level. Bit-stream imaging preserves the integrity and authenticity of the digital evidence and allows further analysis without affecting the original media. Sparse acquisition is a method that involves creating a partial copy of the media by skipping empty sectors or blocks. Drive decryption is a method that involves decrypting an encrypted drive or partition using a password or a key. Logical acquisition is a method that involves creating a copy of the logical files and folders on the media using file system commands.

NEW QUESTION 59
The SOC department in a multinational organization has collected logs of a security event as "Windows.events.evtx". Study the Audit Failure logs in the event log file located in the Documents folder of the -Attacker Maehine-1" and determine the IP address of the attacker. (Note: The event ID of Audit failure logs is 4625.)
(Practical Question)

A. 10.10.1.12
B. 10.10.1.10
C. 10.10.1.16
D. 10.10.1.19

Answer: C

Explanation:
The IP address of the attacker is 10.10.1.16. This can be verified by analyzing the Windows.events.evtx file using a tool such as Event Viewer or Log Parser. The file contains several Audit Failure logs with event ID 4625, which indicate failed logon attempts to the system. The logs show that the source network address of the failed logon attempts is 10.10.1.16, which is the IP address of the attacker3. The screenshot below shows an example of viewing one of the logs using Event Viewer4: References: Audit Failure Log, [Windows.events.evtx], [Screenshot of Event Viewer showing Audit Failure log]

NEW QUESTION 62
Charlie, a security professional in an organization, noticed unauthorized access and eavesdropping on the WLAN. To thwart such attempts, Charlie employed an encryption mechanism that used the RC4 algorithm to encrypt information in the data link layer. Identify the type of wireless encryption employed by Charlie in the above scenario.

A. TKIP
B. WEP
C. AES
D. CCMP

Answer: B

Explanation:
WEP is the type of wireless encryption employed by Charlie in the above scenario. Wireless encryption is a technique that involves encoding or scrambling the data transmitted over a wireless network to prevent unauthorized access or interception. Wireless encryption can use various algorithms or protocols to encrypt and decrypt the data, such as WEP, WPA, WPA2, etc. WEP (Wired Equivalent Privacy) is a type of wireless encryption that uses the RC4 algorithm to encrypt information in the data link layer
. WEP can be used to provide basic security and privacy for wireless networks, but it can also be easily cracked or compromised by various attacks . In the scenario, Charlie, a security professional in an organization, noticed unauthorized access and eavesdropping on the WLAN (Wireless Local Area Network). To thwart such attempts, Charlie employed an encryption mechanism that used the RC4 algorithm to encrypt information in the data link layer. This means that he employed WEP for this purpose. TKIP (Temporal Key Integrity Protocol) is a type of wireless encryption that uses the RC4 algorithm to encrypt information in the data link layer with dynamic keys . TKIP can be used to provide enhanced security and compatibility for wireless networks, but it can also be vulnerable to certain attacks . AES (Advanced Encryption Standard) is a type of wireless encryption that uses the Rijndael algorithm to encrypt information in the data link layer with fixed keys . AES can be used to provide strong security and performance for wireless networks, but it can also require more processing power and resources . CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is a type of wireless encryption that uses the AES algorithm to encrypt information in the data link layer with dynamic keys .
CCMP can be used to provide robust security and reliability for wireless networks, but it can also require more processing power and resources

NEW QUESTION 66
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.

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.

NEW QUESTION 67
A software team at an MNC was involved in a project aimed at developing software that could detect the oxygen levels of a person without physical contact, a helpful solution for pandemic situations. For this purpose, the team used a wireless technology that could digitally transfer data between two devices within a short range of up to 5 m and only worked in the absence of physical blockage or obstacle between the two devices, identify the technology employed by the software

team in the above scenario.

A. Infrared
B. USB
C. CPS
D. Satcom

Answer: A

Explanation:

Infrared is a wireless technology that can digitally transfer data between two devices within a short range of up to 5 m and only works in the absence of physical blockage or obstacle between the two devices. Infrared is commonly used for remote controls, wireless keyboards, and medical devices.
References: Infrared Technology

NEW QUESTION 69
Warren, a member of IH&R team at an organization, was tasked with handling a malware attack launched on one of servers connected to the organization's network. He immediately implemented appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization.
Identify the IH&R step performed by Warren in the above scenario.

A. Containment
B. Recovery
C. Eradication
D. Incident triage

Answer: A

Explanation:
Containment is the IH&R step performed by Warren in the above scenario. IH&R (Incident Handling and Response) is a process that involves identifying, analyzing, containing, eradicating, recovering from, and reporting on security incidents that affect an organization's network or system. Containment is the IH&R step that involves implementing appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization . Containment can be done by isolating the affected system or network, blocking malicious traffic or communication, disabling or removing malicious accounts or processes, etc. Recovery is the IH&R step that involves restoring the normal operation of the system or network after eradicating the incident. Eradication is the IH&R step that involves removing all traces of the incident from the system or network, such as malware, backdoors, compromised files, etc. Incident triage is the IH&R step that involves prioritizing incidents based on their severity, impact, and urgency.

NEW QUESTION 70
Stephen, a security professional at an organization, was instructed to implement security measures that prevent corporate data leakage on employees' mobile devices. For this purpose, he employed a technique using which all personal and corporate data are isolated on an employee's mobile device. Using this technique, corporate applications do not have any control of or communication with the private applications or data of the employees.
Which of the following techniques has Stephen implemented in the above scenario?

A. Full device encryption
B. Geofencing
C. Containerization
D. OTA updates

Answer: C

Explanation:
Containerization is the technique that Stephen has implemented in the above scenario. Containerization is a technique that isolates personal and corporate data on an employee's mobile device. Containerization creates separate encrypted containers or partitions on the device, where corporate applications and data are stored and managed. Containerization prevents corporate data leakage on employees' mobile devices by restricting access, sharing, copying, or transferring of data between containers. Containerization also allows remote wiping of corporate data in case of device loss or theft
. Full device encryption is a technique that encrypts all the data on a mobile device using a password or a key. Geofencing is a technique that uses GPS or RFID to define geographical boundaries and trigger actions based on the location of a mobile device. OTA (Over-the-Air) updates are updates that are delivered wirelessly to mobile devices without requiring physical connection to a computer.

NEW QUESTION 74
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

212-82 Practice Exam Features:

* 212-82 Questions and Answers Updated Frequently

* 212-82 Practice Questions Verified by Expert Senior Certified Staff

* 212-82 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 212-82 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year