EC-Council

Exam Questions 212-82

Certified Cybersecurity Technician(C|CT)

NEW QUESTION 1
Jase. a security team member at an organization, was tasked with ensuring uninterrupted business operations under hazardous conditions. Thus, Jase implemented a deterrent control strategy to minimize the occurrence of threats, protect critical business areas, and mitigate the impact of threats. Which of the following business continuity and disaster recovery activities did Jase perform in this scenario?

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

Answer: A

Explanation:
Prevention is the business continuity and disaster recovery activity performed by Jase in this scenario. Prevention is an activity that involves implementing a deterrent control strategy to minimize the occurrence of threats, protect critical business areas, and mitigate the impact of threats. Prevention can include measures such as backup systems, firewalls, antivirus software, or physical security1. References: Prevention Activity in BCDR

NEW QUESTION 2
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.

A. Nearline backup
B. Cold backup
C. Hot backup
D. Warm backup

Answer: B

Explanation:
Cold backup is the backup technique utilized by Ryleigh in the above scenario. Cold backup is a backup technique that involves taking a full backup of data when the system or database is offline or shut down. Cold backup ensures that the data is consistent and not corrupted by any ongoing transactions or operations. Cold backup is usually performed on a fixed date or time when the service-level downtime is allowed or scheduled . Nearline backup is a backup technique that involves storing data on a medium that is not immediately accessible, but can be retrieved within a short time. Hot backup is a backup technique that involves taking a backup of data while the system or database is online or running. Warm backup is a backup technique that involves taking a backup of data while the system or database is partially online or running.

NEW QUESTION 3
in a security incident, the forensic investigation has isolated a suspicious file named "security_update.exe". You are asked to analyze the file in the Documents folder of the "Attacker Machine-1" to determine whether it is malicious. Analyze the suspicious file and identify the malware signature. (Practical Question)

A. Stuxnet
B. KLEZ
C. ZEUS
D. Conficker

Answer: A

Explanation:
Stuxnet is the malware signature of the suspicious file in the above scenario. Malware is malicious software that can harm or compromise the security or functionality of a system or network. Malware can include various types, such as viruses, worms, trojans, ransomware, spyware, etc. Malware signature is a unique pattern or characteristic that identifies a specific malware or malware family. Malware signature can be used to detect or analyze malware by comparing it with known malware signatures in databases or repositories. To analyze the suspicious file and identify the malware signature, one has to follow these steps:
? Navigate to Documents folder of Attacker Machine-1.
? Right-click on security_update.exe file and select Scan with VirusTotal option.
? Wait for VirusTotal to scan the file and display the results.
? Observe the detection ratio and details.
The detection ratio is 59/70, which means that 59 out of 70 antivirus engines detected the file as malicious. The details show that most antivirus engines detected the file as Stuxnet, which is a malware signature of a worm that targets industrial control systems (ICS). Stuxnet can be used to sabotage or damage ICS by modifying their code or behavior. Therefore, Stuxnet is the malware signature of the suspicious file. KLEZ is a malware signature of a worm that spreads via email and network shares. KLEZ can be used to infect or overwrite files, disable antivirus software, or display fake messages. ZEUS is a malware signature of a trojan that targets banking and financial systems. ZEUS can be used to steal or modify banking credentials, perform fraudulent transactions, or install other malware. Conficker is a malware signature of a worm that exploits a vulnerability in Windows operating systems. Conficker can be used to create a botnet, disable security services, or download other malware

NEW QUESTION 4
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 5
An IoT device that has been placed in a hospital for safety measures, it has sent an alert command to the server. The network traffic has been captured and stored in the Documents folder of the Attacker Machine-1. Analyze the loTdeviceTraffic.pcapng file and select the appropriate command that was sent by the IoT device over the network.

A. Tempe_Low
B. Low_Tempe
C. Temp_High
D. High_Tempe

Answer: C

Explanation:
Temp_High is the command that was sent by the IoT device over the network in the above scenario. An IoT (Internet of Things) device is a device that can connect to the internet and communicate with other devices or systems over a network. An IoT device can send or receive commands or data for various purposes, such as monitoring, controlling, or automating processes. To analyze the IoT device traffic file and determine the command that was sent by the IoT device over the network, one has to follow these steps:
? Navigate to the Documents folder of Attacker-1 machine.
? Double-click on loTdeviceTraffic.pcapng file to open it with Wireshark.
? Click on Analyze menu and select Display Filters option.
? Enter udp.port == 5000 as filter expression and click on Apply button.
? Observe the packets filtered by the expression.
? Click on packet number 4 and expand User Datagram Protocol section in packet details pane.
? Observe the data field under User Datagram Protocol section.
The data field under User Datagram Protocol section is 54:65:6d:70:5f:48:69:67:68 , which is hexadecimal representation of Temp_High , which is the command that was sent by the IoT device over the network.

NEW QUESTION 6
A text file containing sensitive information about the organization has been leaked and modified to bring down the reputation of the organization. As a safety measure, the organization did contain the MD5 hash of the original file. The file which has been leaked is retained for examining the integrity. A file named "Sensitiveinfo.txt" along with OriginalFileHash.txt has been stored in a folder named Hash in Documents of Attacker Machine-1. Compare the hash value of the original file with the leaked file and state whether the file has been modified or not by selecting yes or no.

A. No
B. Yes

Answer: B

Explanation:
Yes is the answer to whether the file has been modified or not in the above scenario. A hash is a fixed-length string that is generated by applying a mathematical function, called a hash function, to a piece of data, such as a file or a message. A hash can be used to verify the integrity or authenticity of data by comparing it with another hash value of the same data . A hash value is unique and any change in the data will result in a different hash value . To compare the hash value of the original file with the leaked file and state whether the file has been modified or not, one has to follow these steps:
? Navigate to Hash folder in Documents of Attacker-1 machine.
? Open OriginalFileHash.txt file with a text editor.
? Note down the MD5 hash value of the original file as 8f14e45fceea167a5a36dedd4bea2543
? Open Command Prompt and change directory to Hash folder using cd command.
? Type certutil -hashfile Sensitiveinfo.txt MD5 and press Enter key to generate MD5 hash value of leaked file.
? Note down the MD5 hash value of leaked file as 9f14e45fceea167a5a36dedd4bea2543
? Compare both MD5 hash values.
The MD5 hash values are different , which means that the file has been modified.

NEW QUESTION 7
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 8
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 9
Cairo, an incident responder. was handling an incident observed in an organizational network. After performing all IH&R steps, Cairo initiated post-incident activities. He determined all types of losses caused by the incident by identifying And evaluating all affected devices, networks, applications, and software. Identify the post-incident activity performed by Cairo in this scenario.

A. Incident impact assessment
B. Close the investigation
C. Review and revise policies
D. Incident disclosure

Answer: A

Explanation:
Incident impact assessment is the post-incident activity performed by Cairo in this scenario. Incident impact assessment is a post-incident activity that involves determining all types of losses caused by the incident by identifying and evaluating all affected devices, networks, applications, and software. Incident impact assessment can include measuring financial losses, reputational damages, operational disruptions, legal liabilities, or regulatory penalties1. References: Incident Impact Assessment

NEW QUESTION 10
Finley, a security professional at an organization, was tasked with monitoring the organizational network behavior through the SIEM dashboard. While monitoring, Finley noticed suspicious activities in the network; thus, he captured and analyzed a single network packet to determine whether the signature included malicious patterns. Identify the attack signature analysis technique employed by Finley in this scenario.

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

Answer: D

Explanation:
Content-based signature analysis is the attack signature analysis technique employed by Finley in this scenario. Content-based signature analysis is a technique that captures and analyzes a single network packet to determine whether the signature included malicious patterns. Content-based signature analysis can be used to detect known attacks, such as buffer overflows, SQL injections, or cross-site scripting2. References: Content-Based Signature Analysis

NEW QUESTION 10
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 15
RAT has been setup in one of the machines connected to the network to steal the important Sensitive corporate docs located on Desktop of the server, further investigation revealed the IP address of the server 20.20.10.26. Initiate a remote connection using thief client and determine the number of files present in the folder.
Hint: Thief folder is located at: Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1.

A. 2
B. 4
C. 3
D. 5

Answer: C

Explanation:
3 is the number of files present in the folder in the above scenario. A RAT (Remote Access Trojan) is a type of malware that allows an attacker to remotely access and control a compromised system or network. A RAT can be used to steal sensitive data, spy on user activity, execute commands, install other malware, etc. To initiate a remote connection using thief client, one has to follow these steps:
? Navigate to the thief folder located at Z:\CCT-Tools\CCT Module 01 Information
Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1.
? Double-click on thief.exe file to launch thief client.
? Enter 20.20.10.26 as IP address of server.
? Enter 1234 as port number.
? Click on Connect button.
? After establishing connection with server, click on Browse button.
? Navigate to Desktop folder on server.
? Count number of files present in folder. The number of files present in folder is 3, which are:
? Sensitive corporate docs.docx
? Sensitive corporate docs.pdf
? Sensitive corporate docs.txt

NEW QUESTION 19
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 21
Elliott, a security professional, was appointed to test a newly developed application deployed over an organizational network using a Bastion host. Elliott initiated the process by configuring the nonreusable bastion host. He then tested the newly developed application to identify the presence of security flaws that were not yet known; further, he executed services that were not secure. identify the type of bastion host configured by Elliott in the above scenario.

A. External services hosts
B. Victim machines
C. One-box firewalls
D. Non-routing dual-homed hosts

Answer: D

Explanation:
Non-routing dual-homed hosts are the type of bastion hosts configured by Elliott in the above scenario. A bastion host is a system or device that is exposed to the public internet and acts as a gateway or a proxy for other systems or networks behind it. A bastion host can be used to provide an additional layer of security and protection for internal systems or networks from external threats and attacks . A bastion host can have different types based on its configuration or functionality. A non-routing dual-homed host is a type of bastion host that has two network interfaces: one connected to the public internet and one connected to the internal network. A non-routing dual-homed host does not allow any direct communication between the two networks and only allows specific services or applications to pass through it . A non-routing dual-homed host can be used to isolate and secure internal systems or networks from external access . In the scenario, Elliott was appointed to test a newly developed application deployed over an organizational network using a bastion host. Elliott initiated the process by configuring the non-reusable bastion host. He then tested the newly developed application to identify the presence of security flaws that were not yet known; further, he executed services that were not secure. This means that he configured a non-routing dual-homed host for this purpose. An external services host is a type of bastion host that provides external services, such as web, email, FTP, etc., to the public internet while protecting internal systems or networks from direct access . A victim machine is not a type of bastion host, but a term that describes a system or device that has been compromised or infected by an attacker or malware . A one-box firewall is not a type of bastion host, but a term that describes a firewall that performs both packet filtering and application proxy functions in one device .

NEW QUESTION 24
A startup firm contains various devices connected to a wireless network across the floor. An AP with Internet connectivity is placed in a corner to allow wireless communication between devices. To support new devices connected to the network beyond the APS range, an administrator used a network device that extended the signals of the wireless AP and transmitted it to uncovered area, identify the network component employed by the administrator to extend signals in this scenario.

A. Wireless repeater
B. Wireless bridge
C. wireless modem
D. Wireless router

Answer: A

Explanation:
Wireless repeater is the network component employed by the administrator to extend signals in this scenario. A wireless network is a type of network that uses radio waves or infrared signals to transmit data between devices without using cables or wires. A wireless network can consist of various components, such as wireless access points (APs), wireless routers, wireless adapters, wireless bridges, wireless repeaters, etc. A wireless repeater is a network component that extends the range or coverage of a wireless signal by receiving it from an AP or another repeater and retransmitting it to another area . A wireless repeater can be used to support new devices connected to the network beyond the AP's range . In the scenario, a startup firm contains various devices connected to a wireless network across the floor. An AP with internet connectivity is placed in a corner to allow wireless communication between devices. To support new devices connected to the network beyond the AP's range, an administrator used a network component that extended the signals of the wireless AP and transmitted it to the uncovered area. This means that he used a wireless repeater for this purpose. A wireless bridge is a network component that connects two or more wired or wireless networks or segments together . A wireless bridge can be used to expand the network or share resources between networks . A wireless modem is a network component that modulates and demodulates wireless signals to enable data transmission over a network . A wireless modem can be used to provide internet access to devices via a cellular network or a satellite network . A wireless router is a network component that performs the functions of both a wireless AP and a router . A wireless router can be used to create a wireless network and connect it to another network, such as the internet

NEW QUESTION 25
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?

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.

NEW QUESTION 29
An FTP server has been hosted in one of the machines in the network. Using Cain and Abel the attacker was able to poison the machine and fetch the FTP credentials used by the admin. You're given a task to validate the credentials that were stolen using Cain and Abel and read the file flag.txt

A. white@hat
B. red@hat
C. hat@red
D. blue@hat

Answer: C

Explanation:
hat@red is the FTP credential that was stolen using Cain and Abel in the above scenario. FTP (File Transfer Protocol) is a protocol that allows transferring files between a client and a server over a network. FTP requires a username and a password to authenticate the client and grant access to the server . Cain and Abel is a tool that can perform various network attacks, such as ARP poisoning, password cracking, sniffing, etc. Cain and Abel can poison the machine and fetch the FTP credentials used by the admin by intercepting and analyzing the network traffic . To validate the credentials that were stolen using Cain and Abel and read the file flag.txt, one has to follow these steps:
? Navigate to the Documents folder of Attacker-1 machine.
? Double-click on Cain.exe file to launch Cain and Abel tool.
? Click on Sniffer tab.
? Click on Start/Stop Sniffer icon.
? Click on Configure icon.
? Select the network adapter and click on OK button.
? Click on + icon to add hosts to scan.
? Select All hosts in my subnet option and click on OK button.
? Wait for the hosts to appear in the list.
? Right-click on 20.20.10.26 (FTP server) and select Resolve Host Name option.
? Note down the host name as ftpserver.movieabc.com
? Click on Passwords tab.
? Click on + icon to add items to list.
? Select Network Passwords option.
? Select FTP option from Protocol drop-down list.
? Click on OK button.
? Wait for the FTP credentials to appear in the list.
? Note down the username as hat and the password as red
? Open a web browser and type ftp://hat:red@ftpserver.movieabc.com

? Press Enter key to access the FTP server using the stolen credentials.
? Navigate to flag.txt file and open it.
? Read the file content.

NEW QUESTION 31
Jordan, a network administrator in an organization, was instructed to identify network- related issues and improve network performance. While troubleshooting the network, he received a message indicating that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host, which of the following network issues did Jordan find in this scenario?

A. Time exceeded message
B. Destination unreachable message
C. Unreachable networks
D. Network cable is unplugged

Answer: B

Explanation:
Destination unreachable message is the network issue that Jordan found in this scenario. Destination unreachable message is a type of ICMP message that indicates that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host. Destination unreachable message can be caused by various reasons, such as incorrect routing, firewall blocking, or host configuration problems1.
References: Destination Unreachable Message

NEW QUESTION 36
Karter, a security professional, deployed a honeypot on the organization's network for luring attackers who attempt to breach the network. For this purpose, he configured a type of honeypot that simulates a real OS as well as the applications and services of a target network. Furthermore, the honeypot deployed by Karter only responds to pre-configured commands.
Identify the type of Honeypot deployed by Karter in the above scenario.

A. Low-interaction honeypot
B. Pure honeypot
C. Medium-interaction honeypot
D. High-interaction honeypot

Answer: A

Explanation:
A low-interaction honeypot is a type of honeypot that simulates a real OS as well as the applications and services of a target network, but only responds to pre-configured commands. It is designed to capture basic information about the attacker, such as their IP address, tools, and techniques. A low-interaction honeypot is easier to deploy and maintain than a high-interaction honeypot, which fully emulates a real system and allows the attacker to interact with it. A pure honeypot is a real system that is intentionally vulnerable and exposed to attackers. A medium-interaction honeypot is a type of honeypot that offers more functionality and interactivity than a low-interaction honeypot, but less than a high-interaction honeypot.

NEW QUESTION 40
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 45
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.

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

NEW QUESTION 50
Richards, a security specialist at an organization, was monitoring an IDS system. While monitoring, he suddenly received an alert of an ongoing intrusion attempt on the organization's network. He immediately averted the malicious actions by implementing the necessary measures.
Identify the type of alert generated by the IDS system in the above scenario.

A. True positive
B. True negative
C. False negative
D. False positive

Answer: A

Explanation:
A true positive alert is generated by an IDS system when it correctly identifies an ongoing intrusion attempt on the network and sends an alert to the security professional. This is the desired outcome of an IDS system, as it indicates that the system is working effectively and accurately

NEW QUESTION 51
Cassius, a security professional, works for the risk management team in an organization. The team is responsible for performing various activities involved in the risk management process. In this process, Cassius was instructed to select and implement appropriate controls on the identified risks in order to address the risks based on their severity level.
Which of the following risk management phases was Cassius instructed to perform in the above scenario?

A. Risk analysis
B. Risk treatment
C. Risk prioritization
D. Risk identification

Answer: B

Explanation:
Risk treatment is the risk management phase that Cassius was instructed to perform in the above scenario. Risk management is a process that involves identifying, analyzing, evaluating, treating, monitoring, and reviewing risks that can affect an organization’s objectives, assets, or operations. Risk management phases can be summarized as follows: risk identification, risk analysis, risk prioritization, risk treatment, and risk monitoring . Risk identification is the risk management phase that involves identifying and documenting potential sources, causes, events, and impacts of risks. Risk analysis is the risk management phase that involves assessing and quantifying the likelihood and consequences of risks. Risk prioritization is the risk management phase that involves ranking risks based on their severity level and determining which risks need immediate attention or action. Risk treatment is the risk management phase that involves selecting and implementing appropriate controls or strategies to address risks based on their severity level . Risk treatment can include avoiding, transferring, reducing, or accepting risks. Risk monitoring is the risk management phase that involves tracking and reviewing the performance and effectiveness of risk controls or strategies over time.

NEW QUESTION 52
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 55
Kaison. a forensic officer, was investigating a compromised system used for various online attacks. Kaison initiated the data acquisition process and extracted the data from the systems DVD-ROM. Which of the following types of data did Kaison acquire in the above scenario?

A. Archival media
B. Kernel statistics
C. ARP cache
D. Processor cache

Answer: A

Explanation:

Archival media is the type of data that Kaison acquired in the above scenario. Archival media is a type of data that is stored on removable media such as DVD-ROMs, CD-ROMs, tapes, or flash drives. Archival media can be used to backup or transfer data from one system to another. Archival media can be acquired using forensic tools that can read and copy the data from the media4. References: Archival Media

NEW QUESTION 60
Dany, a member of a forensic team, was actively involved in an online crime investigation process. Dany's main responsibilities included providing legal advice on conducting the investigation and addressing legal issues involved in the forensic investigation process. Identify the role played by Dany in the above scenario.

A. Attorney
B. Incident analyzer
C. Expert witness
D. Incident responder

Answer: A

Explanation:
Attorney is the role played by Dany in the above scenario. Attorney is a member of a forensic team who provides legal advice on conducting the investigation and addresses legal issues involved in the forensic investigation process. Attorney can help with obtaining search warrants, preserving evidence, complying with laws and regulations, and presenting cases in court3. References: Attorney Role in Forensic Investigation

NEW QUESTION 65
A disgruntled employee has set up a RAT (Remote Access Trojan) server in one of the machines in the target network to steal sensitive corporate documents. The IP address of the target machine where the RAT is installed is 20.20.10.26. Initiate a remote connection to the target machine from the "Attacker Machine-1" using the Theef client. Locate the "Sensitive Corporate Documents" folder in the target machine's Documents directory and determine the number of files. Mint: Theef folder is located at Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Theef of the Attacker Machine1.

A. 2
B. 4
C. 5
D. 3

Answer: B

Explanation:
The number of files in the “Sensitive Corporate Documents” folder is 4. This can be verified by initiating a remote connection to the target machine from the “Attacker Machine-1” using Theef client. Theef is a Remote Access Trojan (RAT) that allows an attacker to remotely control a victim’s machine and perform various malicious activities. To connect to the target machine using Theef client, one can follow these steps:
Launch Theef client from Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Theef on the “Attacker Machine-1”.
Enter the IP address of the target machine (20.20.10.26) and click on Connect.
Wait for a few seconds until a connection is established and a message box appears saying “Connection Successful”.
Click on OK to close the message box and access the remote desktop of the target machine.
Navigate to the Documents directory and locate the “Sensitive Corporate Documents” folder.
Open the folder and count the number of files in it. The screenshot below shows an example of performing these steps: References: [Theef Client Tutorial], [Screenshot of Theef client showing remote desktop and folder]

NEW QUESTION 66
Giovanni, a system administrator, was tasked with configuring permissions for employees working on a new project. Hit organization used active directories (ADs) to grant/deny permissions to resources Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. Identify the type of account created by Giovanni in this scenario.

A. Third-party account
B. Croup-based account
C. Shared account
D. Application account

Answer: B

Explanation:
Group-based account is the type of account created by Giovanni in this scenario. An account is a set of credentials, such as a username and a password, that allows a user to access a system or network. An account can have different types based on its purpose or usage. A group-based account is a type of account that allows multiple users to access a system or network with the same credentials and permissions. A group-based account can be used to simplify the management of users and resources by assigning them to groups based on their roles or functions. In the scenario, Giovanni was tasked with configuring permissions for employees working on a new project. His organization used active directories (ADs) to grant/deny permissions to resources. Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. This means that he created a group-based account for those employees.
A third-party account is a type of account that allows an external entity or service to access a system or network with limited permissions or scope. A shared account is a type of account that allows multiple users to access a system or network with the same credentials but different permissions. An application account is a type of account that allows an application or software to access a system or network with specific permissions or functions.

NEW QUESTION 70
You have been assigned to perform a vulnerability assessment of a web server located at IP address 20.20.10.26. Identify the vulnerability with a severity score of &A. You can use the OpenVAS vulnerability scanner, available with the Parrot Security machine, with credentials admin/password for this challenge. (Practical Question)

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

Answer: A

Explanation:
TCP Timestamps is the vulnerability with a severity score of 8.0. This can be verified by performing a vulnerability assessment of the web server located at IP address 20.20.10.26 using the OpenVAS vulnerability scanner, available with the Parrot Security machine, with credentials admin/password. To perform the vulnerability assessment, one can follow these steps:
Launch the Parrot Security machine and open a terminal.
Enter the command sudo openvas-start to start the OpenVAS service and wait for a few minutes until it is ready.
Open a web browser and navigate to https://127.0.0.1:9392 to access the OpenVAS web interface.
Enter the credentials admin/password to log in to OpenVAS.
Click on Scans -> Tasks from the left menu and then click on the blue icon with a star to create a new task.
Enter a name and a comment for the task, such as “Web Server Scan”. Select “Full and fast” as the scan config from the drop-down menu. Click on the icon with a star next to Target to create a new target. Enter a name and a comment for the target, such as “Web Server”. Enter 20.20.10.26 as the host in the text box and click on Save.
Select “Web Server” as the target from the drop-down menu and click on Save.
Click on the green icon with a play button next to the task name to start the scan and wait for it to finish.
Click on the task name to view the scan report and click on Results from the left menu to see the list of vulnerabilities found.
Sort the list by Severity in descending order and look for the vulnerability with a severity score of 8.0. The screenshot below shows an example of performing these steps: The vulnerability with a severity score of 8.0 is TCP Timestamps, which is an option in TCP packets that can be used to measure round-trip time and improve performance, but it can also reveal information about the system’s uptime, clock skew, or TCP sequence numbers, which can be used by attackers to launch various attacks, such as idle scanning, OS fingerprinting, or TCP hijacking1. The vulnerability report provides more details about this vulnerability, such as its description, impact, solution, references, and CVSS score2. References: Screenshot of OpenVAS showing TCP Timestamps vulnerability, TCP Timestamps Vulnerability, Vulnerability Report

NEW QUESTION 75
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 78
In an organization, all the servers and database systems are guarded in a sealed room with a single-entry point. The entrance is protected with a physical lock system that requires typing a sequence of numbers and letters by using a rotating dial that intermingles with several other rotating discs.
Which of the following types of physical locks is used by the organization in the above scenario?

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

Answer: B

Explanation:
It identifies the type of physical lock used by the organization in the above scenario. A physical lock is a device that prevents unauthorized access to a door, gate, cabinet, or other enclosure by using a mechanism that requires a key, code, or biometric factor to open or close it. There are different types of physical locks, such

as:
? Combination lock: This type of lock requires typing a sequence of numbers and letters by using a rotating dial that intermingles with several other rotating discs. This type of lock is suitable for securing safes, lockers, or cabinets that store valuable items or documents.
? Digital lock: This type of lock requires entering a numeric or alphanumeric code by using a keypad or touchscreen. This type of lock is suitable for securing doors or gates that require frequent access or multiple users.
? Mechanical lock: This type of lock requires inserting and turning a metal key that matches the shape and size of the lock. This type of lock is suitable for securing doors or gates that require simple and reliable access or single users.
? Electromagnetic lock: This type of lock requires applying an electric current to a magnet that attracts a metal plate attached to the door or gate. This type of lock is suitable for securing doors or gates that require remote control or integration with other security systems.
In the above scenario, the organization used a combination lock that requires typing a sequence of numbers and letters by using a rotating dial that intermingles with several other rotating discs. Option A is incorrect, as it does not identify the type of physical lock used by the organization in the above scenario. A digital lock requires entering a numeric or alphanumeric code by using a keypad or touchscreen. In the above scenario, the organization did not use a digital lock, but a combination lock. Option C is incorrect, as it does not identify the type of physical lock used by the organization in the above scenario. A mechanical lock requires inserting and turning a metal key that matches the shape and size of the lock. In the above scenario, the organization did not use a mechanical lock, but a combination lock. Option D is incorrect, as it does not identify the type of physical lock used by the organization in the above scenario. An electromagnetic lock requires applying an electric current to a magnet that attracts a metal plate attached to the door or gate. In the above scenario, the organization did not use an electromagnetic lock, but a combination lock. References: , Section 7.2

NEW QUESTION 82
Alex, a certified security professional, works for both aggressor and defender teams. His team's main responsibility involves enhancing protection and boosting the security standards of the organization. Identify Alex's team in this scenario.

A. White team
B. Purple learn
C. Blue team
D. Red team

Answer: B

Explanation:
Purple team is the team that Alex works for in this scenario. A team is a group of people that work together to achieve a common goal or objective. A team can have different types based on its role or function in an organization or a project. A purple team is a type of team that works for both aggressor and defender teams. A purple team can be used to enhance protection and boost the security standards of an organization by performing various tasks, such as testing, evaluating, improving, or integrating the security
measures implemented by the defender team or exploited by the aggressor team. In the scenario, Alex is a certified security professional who works for both aggressor and defender teams. His team’s main responsibility involves enhancing protection and boosting the security standards of the organization. This means that he works for a purple team. A white team is a type of team that acts as an observer or an arbitrator between the aggressor and defender teams. A white team can be used to monitor, evaluate, or adjudicate the performance or outcome of the aggressor and defender teams by providing feedback, guidance, or rules. A blue team is a type of team that acts as a defender or a protector of an organization’s network or system. A blue team can be used to prevent, detect, or respond to attacks from external or internal threats by implementing various security measures, such as firewalls, antivirus, encryption, etc. A red team is a type of team that acts as an attacker or an adversary of an organization’s network or system. A red team can be used to simulate realistic attacks from external or internal threats by exploiting various vulnerabilities, weaknesses, or gaps in the organization’s security posture.

NEW QUESTION 84
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 89
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 92
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 93
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 98
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: C

Explanation:
A hub-and-spoke VPN topology is a type of VPN topology where all the remote offices communicate with the corporate office, but communication between the remote offices is denied. The corporate office acts as the hub, and the remote offices act as the spokes. This topology reduces the number of VPN tunnels required and simplifies the management of VPN policies. A point-to-point VPN topology is a type of VPN topology where two endpoints establish a direct VPN connection. A star topology is a type of VPN topology where one endpoint acts as the central node and connects to multiple other endpoints. A full-mesh VPN topology is a type of VPN topology where every endpoint connects to every other endpoint.

NEW QUESTION 99
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:
The correct answer is A, as it identifies the type of Internet access policy implemented by Ashton in the above scenario. An Internet access policy is a set of rules and guidelines that defines how an organization's employees or members can use the Internet and what types of websites or services they can access. There are different types of Internet access policies, such as:
? Paranoid policy: This type of policy forbids everything and imposes strict restrictions on all company computers, whether it is system or network usage. This policy is suitable for organizations that deal with highly sensitive or classified information and have a high level of security and compliance requirements.
? Prudent policy: This type of policy allows some things and blocks others and imposes moderate restrictions on company computers, depending on the role and responsibility of the user. This policy is suitable for organizations that deal with confidential or proprietary information and have a medium level of security and compliance requirements.
? Permissive policy: This type of policy allows most things and blocks few and imposes minimal restrictions on company computers, as long as the user does not violate any laws or regulations. This policy is suitable for organizations that deal with public or general information and have a low level of security and compliance requirements.
? Promiscuous policy: This type of policy allows everything and blocks nothing and imposes no restrictions on company computers, regardless of the user's role or responsibility. This policy is suitable for organizations that have no security or compliance requirements and trust their employees or members to use the Internet responsibly.
In the above scenario, Ashton implemented a paranoid policy that forbids everything and imposes strict restrictions on all company computers, whether it is system or network usage. Option B is incorrect, as it does not identify the type of Internet access policy implemented by Ashton in the above scenario. A prudent policy allows some things and blocks others and imposes moderate restrictions on company computers, depending on the role and responsibility of the user. In the above scenario, Ashton did not implement a prudent policy, but a paranoid policy. Option C is incorrect, as it does not identify the type of Internet access policy implemented by Ashton in the above scenario. A permissive policy allows most things and blocks few and imposes minimal restrictions on company computers, as long as the user does not violate any laws or regulations. In the above scenario, Ashton did not implement a permissive policy, but a paranoid policy. Option D is incorrect, as it does not identify the type of Internet access policy implemented by Ashton in the above scenario. A promiscuous policy allows everything and blocks nothing and imposes no restrictions on company computers, regardless of the user's role or responsibility. In the above scenario, Ashton did not implement a promiscuous policy, but a paranoid policy.
References: , Section 6.2

NEW QUESTION 100
Stella purchased a smartwatch online using her debit card. After making payment for the product through the payment gateway, she received a transaction text message with a deducted and available balance from her bank.
Identify the information security element that ensures that Stella's transaction status is immediately reflected in her bank account in this scenario.

A. Non-repudiation
B. Integrity
C. Availability
D. Confidentiality

Answer: C

Explanation:
Availability is the information security element that ensures that Stella's transaction status is immediately reflected in her bank account in this scenario. Information security is the practice of protecting information and information systems from unauthorized access, use, disclosure, modification, or destruction. Information security can be based on three fundamental principles: confidentiality, integrity, and availability. Confidentiality is the principle that ensures that information is accessible only to authorized parties and not disclosed to unauthorized parties. Integrity is the principle that ensures that information is accurate, complete, and consistent and not altered or corrupted by unauthorized parties. Availability is the principle that ensures that information and information systems are accessible and usable by authorized parties when needed. In the scenario, Stella purchased a smartwatch online using her debit card. After making payment for the product through the payment gateway, she received a transaction text message with a deducted and available balance from her bank. This means that her transaction status was immediately reflected in her bank account, which indicates that availability was ensured by her bank's information system.

NEW QUESTION 103
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 107
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 108
.....

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