# EC-Council

## Exam Questions 212-82

Certified Cybersecurity Technician(C|CT)

**NEW QUESTION 1**
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 2**
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 3**
Grace, an online shopping freak, has purchased a smart TV using her debit card. During online payment, Grace's browser redirected her from ecommerce website to a third-party payment gateway, where she provided her debit card details and OTP received on her registered mobile phone. After completing the transaction, Grace navigated to her online bank account and verified the current balance in her savings account.
Identify the state of data when it is being processed between the ecommerce website and the payment gateway in the above scenario.

A. Data at rest
B. Data in inactive
C. Data in transit
D. Data in use

**Answer:** C

**Explanation:**
Data in transit is the state of data when it is being processed between the ecommerce website and the payment gateway in the above scenario. Data in transit is data that is moving from one location to another over a network, such as the internet, a LAN, or a WAN. Data in transit can be vulnerable to interception, modification, or theft by unauthorized parties, so it needs to be protected by encryption, authentication, and other security measures . Data at rest is data that is stored on a device or a media, such as a hard drive, a flash drive, or a cloud storage. Data in active is data that is currently being accessed or modified by an application or a user. Data in use is data that is loaded into the memory of a device or a system for processing or computation.

**NEW QUESTION 4**
Calvin spotted blazing flames originating from a physical file storage location in his organization because of a Short circuit. In response to the incident, he used a fire suppression system that helped curb the incident in the initial stage and prevented it from spreading over a large area. Which of the following firefighting systems did Calvin use in this scenario?

A. Fire detection system
B. Sprinkler system
C. Smoke detectors
D. Fire extinguisher

**Answer:** D

**Explanation:**
Fire extinguisher is the firefighting system that Calvin used in this scenario. A firefighting system is a system that detects and suppresses fire in a physical location or environment. A firefighting system can consist of various components, such as sensors, alarms, sprinklers, extinguishers, etc. A firefighting system can use various agents or substances to suppress fire, such as water, foam, gas, powder, etc. A fire extinguisher is a portable device that contains an agent or substance that can be sprayed or discharged onto a fire to extinguish it . A fire extinguisher can be used to curb fire in the initial stage and prevent it from spreading over a large area . In the scenario, Calvin spotted blazing flames originating from a physical file storage location in his organization because of a short circuit. In response to the incident, he used a fire suppression system that helped curb the incident in the initial stage and prevented it from spreading over a large area. This means that he used a fire extinguisher for this purpose. A fire detection system is a system that detects the presence of fire by sensing its characteristics, such as smoke, heat, flame, etc., and alerts the occupants or authorities about it . A sprinkler system is a system that consists of pipes and sprinkler heads that release water onto a fire when activated by heat
or smoke. A smoke detector is a device that senses smoke and emits an audible or visual signal to warn about fire.

**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**
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 8**
The incident handling and response (IH&R) team of an organization was handling a recent cyberattack on the organization's web server. Fernando, a member of the IH&P team, was tasked with eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future. For this purpose. Fernando applied the latest patches to the web server and installed the latest security mechanisms on it. Identify the IH&R step performed by Fernando in this scenario.

A. Notification
B. Containment
C. Recovery
D. Eradication

**Answer:** D

**Explanation:**
Eradication is the IH&R step performed by Fernando in this scenario. Eradication is a step in IH&R that involves eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future. Eradication can include applying patches, installing security mechanisms, removing malware, restoring backups, or reformatting systems.
References: [Eradication Step in IH&R]

**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**
The IH&R team in an organization was handling a recent malware attack on one of the hosts connected to the organization's network. Edwin, a member of the IH&R team, was involved in reinstating lost data from the backup media. Before performing this step, Edwin ensured that the backup does not have any traces of malware.
Identify the IH&R step performed by Edwin in the above scenario.

A. Eradication
B. Incident containment
C. Notification
D. Recovery

**Answer:** D

**Explanation:**
Recovery is the IH&R step performed by Edwin 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. Recovery is the IH&R step that involves restoring the normal operation of the system or network after eradicating the incident. Recovery can include reinstating lost data from the backup media, applying patches or updates, reconfiguring settings, testing functionality, etc. Recovery also involves ensuring that the backup does not have any traces of malware or compromise . 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 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. Notification is the IH&R step that involves informing relevant stakeholders, authorities, or customers about the incident and its impact.

**NEW QUESTION 11**
A software company is developing a new software product by following the best practices for secure application development. Dawson, a software analyst, is checking the performance of the application on the client's network to determine whether end users are facing any issues in accessing the application.
Which of the following tiers of a secure application development lifecycle involves checking the performance of the application?

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

**Answer:** B

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

**NEW QUESTION 13**
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 16**
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 19**
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 21**
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 22**
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 24**
Leo has walked to the nearest supermarket to purchase grocery. At the billing section, the billing executive scanned each product's machine-readable tag against a readable machine that automatically reads the product details, displays the prices of the individual product on the computer, and calculates the sum of those scanned items. Upon completion of scanning all the products, Leo has to pay the bill.
Identify the type of short-range wireless communication technology that the billing executive has used in the above scenario.

A. Radio-frequency identification (RFID)
B. Near-field communication (NFC)
C. QUIC
D. QR codes and barcodes

**Answer:** A

**Explanation:**
Radio-frequency identification (RFID) is the type of short-range wireless communication technology that the billing executive has used in the above scenario. RFID uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects . RFID tags are machine-readable tags that store information about the products, such as name, price, expiry date, etc. RFID readers are readable machines that scan the RFID tags and display the product details on the computer . RFID technology is widely used in supermarkets, warehouses, libraries, and other places where inventory management and tracking are required .

**NEW QUESTION 25**
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 26**
Kayden successfully cracked the final round of interviews at an organization. After a few days, he received his offer letter through an official company email address. The email stated that the selected candidate should respond within a specified time. Kayden accepted the opportunity and provided an e-signature on the offer letter, then replied to the same email address. The company validated the e-signature and added his details to their database. Here, Kayden could not deny the company's message, and the company could not deny Kayden's signature.
Which of the following information security elements was described in the above scenario?

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

**Answer:** B

**Explanation:**
The correct answer is B, as it describes the information security element that was described in the above scenario. Non-repudiation is an information security element that ensures that a party cannot deny sending or receiving a message or performing an action. In the above scenario, non-repudiation was described, as Kayden could not deny company’s message, and company could not deny Kayden’s signature. Option A is incorrect, as it does not describe the information security element that was described in the above scenario. Availability is an information security element that ensures that authorized users can access and use information and resources when needed. In the above scenario, availability was not described, as there was no mention of access or use of information and resources. Option C is incorrect, as it does not describe the information security element that was described in the above scenario. Integrity is an information security element that ensures that information and resources are accurate and complete and have not been modified by unauthorized parties. In the above scenario, integrity was not described, as there was no mention of accuracy or completeness of information and resources. Option D is incorrect, as it does not describe the information security element that was described in the above scenario. Confidentiality is an information security element that ensures that information and resources are protected from unauthorized access and disclosure. In the above scenario, confidentiality was not described, as there was no mention of protection or disclosure of information and resources.
References: , Section 3.1

**NEW QUESTION 31**
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 34**
Riley sent a secret message to Louis. Before sending the message, Riley digitally signed the message using his private key. Louis received the message, verified the digital signature using the corresponding key to ensure that the message was not tampered during transit.
Which of the following keys did Louis use to verify the digital signature in the above scenario?

A. Riley's public key
B. Louis's public key
C. Riley's private key
D. Louis's private key

**Answer:** A

**Explanation:**
Riley’s public key is the key that Louis used to verify the digital signature in the above scenario. A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document. A digital signature is created by applying a hash function to the message or document and then encrypting the hash value with the sender’s private key. A digital signature can be verified by decrypting the hash value with the sender’s public key and comparing it with the hash value of the original message or document . Riley’s public key is the key that corresponds to Riley’s private key, which he used to sign the message. Louis’s public key is the key that corresponds to Louis’s private key, which he may use to encrypt or decrypt messages with Riley. Louis’s private key is the key that only Louis knows and can use to sign or decrypt messages. Riley’s private key is the key that only Riley knows and can use to sign or encrypt messages.

**NEW QUESTION 36**
Elliott, a security professional, was tasked with implementing and deploying firewalls in the corporate network of an organization. After planning and deploying firewalls in the network,
Elliott monitored the firewall logs to detect evolving threats And attacks; this helped in ensuring firewall security and addressing network issues beforehand.
in which of the following phases of firewall implementation and deployment did Elliott monitor the firewall logs?

A. Deploying
B. Managing and maintaining
C. Testing
D. Configuring

**Answer:** B

**Explanation:**
Managing and maintaining is the phase of firewall implementation and deployment in which Elliott monitored the firewall logs in the above scenario. A firewall is a system or device that controls and filters the incoming and outgoing traffic between different networks or systems based on predefined rules or policies. A firewall can be used to protect a network or system from unauthorized access, use, disclosure, modification, or destruction . Firewall implementation and deployment is a process that involves planning, installing, configuring, testing, managing, and maintaining firewalls in a network or system . Managing and maintaining is the phase of firewall implementation and deployment that involves monitoring and reviewing the performance and effectiveness of firewalls over time. Managing and maintaining can include tasks such as updating firewall rules or policies, analyzing firewall logs , detecting evolving threats or attacks , ensuring firewall security , addressing network issues , etc. In the scenario, Elliott was tasked with implementing and deploying firewalls in the corporate network of an organization. After planning and deploying firewalls in the network, Elliott monitored the firewall logs to detect evolving threats and attacks; this helped in ensuring firewall security and addressing network issues beforehand. This means that he performed managing and maintaining phase for this purpose. Deploying is the phase of firewall implementation and deployment that involves installing and activating firewalls in the network or system according to the plan. Testing is the phase of firewall implementation and deployment that involves verifying and validating the functionality and security of firewalls before putting them into operation. Configuring is the phase of firewall implementation and deployment that involves setting up and customizing firewalls according to the requirements and specifications.

**NEW QUESTION 40**
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 42**
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 43**
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 46**
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 50**
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 51**
Omar, an encryption specialist in an organization, was tasked with protecting low- complexity applications such as RFID tags, sensor-based applications, and other IbT- based applications. For this purpose, he employed an algorithm for all lower-powered devices that used less power and resources without compromising device security.
identify the algorithm employed by Omar in this scenario.

A. Quantum cryptography
B. Elliptic curve cryptography
C. Lightweight cryptography
D. Homomorphic encryption

**Answer:** C

**Explanation:**
Lightweight cryptography is an algorithm that is designed for low-complexity applications such as RFID tags, sensor-based applications, and other IoT-based applications. Lightweight cryptography uses less power and resources without compromising device security. Lightweight cryptography can be implemented using symmetric-key algorithms, asymmetric-key algorithms, or hash functions1. References: Lightweight Cryptography

**NEW QUESTION 54**
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 56**
Nicolas, a computer science student, decided to create a guest OS on his laptop for different lab operations. He adopted a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS.
Which of the following virtualization approaches has Nicolas adopted in the above scenario?

A. Hardware-assisted virtualization
B. Full virtualization
C. Hybrid virtualization
D. OS-assisted virtualization

**Answer:** A

**Explanation:**
Hardware-assisted virtualization is a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS. Hardware-assisted virtualization relies on special hardware features in the CPU and chipset to create and manage virtual machines efficiently and securely34. Full virtualization is a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment, but the VMM will run in software and emulate all the hardware resources for each virtual machine5. Hybrid virtualization is a virtualization approach that combines hardware-assisted and full virtualization techniques to optimize performance and compatibility6. OS-assisted virtualization is a virtualization approach in which the guest OS will be modified to run in a virtualized environment and cooperate with the VMM to access the hardware resources

**NEW QUESTION 57**
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 60**

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 64**
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 68**
Camden, a network specialist in an organization, monitored the behavior of the organizational network using SIFM from a control room. The SIEM detected suspicious activity and sent an alert to the camera. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers.
Which of the following SIEM functions allowed Camden to view suspicious behavior and make correct decisions during a security incident?

A. Application log monitoring
B. Log Retention
C. Dashboard
D. Data aggregation

**Answer:** C

**Explanation:**
Dashboard is the SIEM function that allowed Camden to view suspicious behavior and make correct decisions during a security incident. SIEM (Security Information and Event Management) is a system or software that collects, analyzes, and correlates security data from various sources, such as logs, alerts, events, etc., and provides a centralized view and management of the security posture of a network or system. SIEM can be used to detect, prevent, or respond to security incidents or threats. SIEM consists of various functions or components that perform different tasks or roles. Dashboard is a SIEM function that provides a graphical user interface (GUI) that displays various security metrics, indicators, alerts, reports, etc., in an organized and interactive manner. Dashboard can be used to view suspicious behavior and make correct decisions during a security incident. In the scenario, Camden monitored the behavior of the organizational network using SIEM from a control room. The SIEM detected suspicious activity and sent an alert to Camden. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers. This means that he used the dashboard function of SIEM for this purpose. Application log monitoring is a SIEM function that collects and analyzes application logs, which are records of events or activities that occur within an application or software. Log retention is an SIEM function that stores and preserves logs for a certain period of time or

indefinitely for future reference or analysis. Data aggregation is an SIEM function that combines and normalizes data from different sources into a common format or structure.

**NEW QUESTION 73**
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 76**
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 80**
A company decided to implement the cloud infrastructure within its corporate firewall 10 secure sensitive data from external access. The company invested heavily in creating a cloud architecture within its premises to manage full control over its corporate data. Which of the following types of cloud deployment models did the company implement in this scenario?

A. Multi cloud
B. Public cloud
C. Private cloud
D. Community cloud

**Answer:** C

**Explanation:**
Private cloud is the type of cloud deployment model that the company implemented in this scenario. Cloud computing is a model that provides on-demand access to shared and scalable computing resources, such as servers, storage, networks, applications, etc., over the internet or a network. Cloud computing can have different types based on its service or deployment model. A cloud deployment model defines how and where the cloud infrastructure and services are hosted and accessed . A cloud deployment model can have different types, such as public cloud, private cloud, hybrid cloud, community cloud, etc. A private cloud is a type of cloud deployment model that provides exclusive access to cloud infrastructure and services to a single organization or entity . A private cloud can be hosted within or outside the organization’s premises and managed by the organization or a third-party provider . A private cloud can be used to secure sensitive data from

external access and maintain full control over the corporate data . In the scenario, the company decided to implement the cloud infrastructure within its corporate firewall to secure sensitive data from external access. The company invested heavily in creating a cloud architecture within its premises to manage full control over its corporate data. This means that the company implemented a private cloud for this purpose. A multi- cloud is not a type of cloud deployment model, but a term that describes a strategy that uses multiple public or private clouds from different providers for different purposes or functions . A public cloud is a type of cloud deployment model that provides open access to cloud infrastructure and services to multiple organizations or entities over the internet . A public cloud can be hosted and managed by a third-party provider that owns and operates the cloud infrastructure and services . A community cloud is a type of cloud deployment model that provides shared access to cloud infrastructure and services to multiple organizations or entities that have common interests or goals

**NEW QUESTION 84**
Identify a machine in the network with 5SH service enabled. Initiate an SSH Connection to the machine, find the file, ttag.txt. in the machine, and enter the tile's content as the answer. The credentials tor SSH login are sam/adm(admin@123. {Practical Question)

A. sam@bob
B. bob2@sam
C. sam2@bob
D. bobt@sam

**Answer:** D

**Explanation:**
bob1@sam is the file’s content as the answer. To find the machine with SSH service enabled, one can use a network scanning tool such as Nmap to scan the network for port 22, which is the default port for SSH. For example, the command nmap -p 22 192.168.0.0/24 will scan the network range 192.168.0.0/24 for port 22 and display the results2. To initiate an SSH connection to the machine, one can use a command-line tool such as ssh or an SSH client such as PuTTY to connect to the machine using the credentials sam/admin@123. For example, the command ssh sam@192.168.0.10 will connect to the machine with IP address 192.168.0.10 using the username sam and prompt for the password admin@1233. To find the file flag.txt in the machine, one can use a file searching tool such as find or locate to search for the file name in the machine’s file system. For example, the command find / -name flag.txt will search for the file flag.txt from the root directory (/) and display its location4. To enter the file’s content as the answer, one can use a file viewing tool such as cat or less to display the content of the file flag.txt. For example, the command cat /home/sam/flag.txt will display the content of the file flag.txt located in /home/sam/ directory5. The screenshot below shows an example of performing these steps: ![Screenshot of performing these steps] References: Nmap Tutorial, SSH Tutorial, Find Command Tutorial, Cat Command Tutorial, [Screenshot of performing these steps]

**NEW QUESTION 89**
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 93**
Grace, an online shopping enthusiast, purchased a smart TV using her debit card. During online payment. Grace's browser redirected her from the e-commerce website to a third- party payment gateway, where she provided her debit card details and the OTP received on her registered mobile phone. After completing the transaction, Grace logged Into her online bank account and verified the current balance in her savings account, identify the state of data being processed between the e-commerce website and payment gateway in the above scenario.

A. Data in inactive
B. Data in transit
C. Data in use
D. Data at rest

**Answer:** B

**Explanation:**
Data in transit is the state of data being processed between the e-commerce website and payment gateway in the above scenario. Data in transit is the data that is moving from one location to another over a network, such as the internet. Data in transit can be vulnerable to interception, modification, or theft by unauthorized parties. Therefore, data in transit should be protected using encryption, authentication, and secure protocols2. References: Data in Transit

**NEW QUESTION 97**
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 99**
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 100**
Ayden works from home on his company's laptop. During working hours, he received an antivirus software update notification on his laptop. Ayden clicked on the update button; however, the system restricted the update and displayed a message stating that the update could only be performed by authorized personnel.
Which of the following PCI-DSS requirements is demonstrated In this scenario?

A. PCI-DSS requirement no 53
B. PCI-DSS requirement no 1.3.1
C. PCI-DSS requirement no 5.1
D. PCI-DSS requirement no 1.3.2

**Answer:** A

**Explanation:**
PCI-DSS requirement no 5.3 is the PCI-DSS requirement that is demonstrated in this scenario. 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. PCI-DSS consists of 12 requirements that are grouped into six categories: build and maintain a secure network and systems, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy. PCI-DSS requirement no 5.3 is part of the category “maintain a vulnerability management program” and states that antivirus mechanisms must be actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. In the scenario, Ayden works from home on his company’s laptop. During working hours, he received an antivirus software update notification on his laptop. Ayden clicked on the update button; however, the system restricted the update and displayed a message stating that the update could only be performed by authorized personnel. This means that his company’s laptop has an antivirus mechanism that is actively running and cannot be disabled or altered by users, which demonstrates PCI-DSS requirement no 5.3.

**NEW QUESTION 104**
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**
As a cybersecurity technician, you were assigned to analyze the file system of a Linux image captured from a device that has been attacked recently. Study the

forensic image 'Evidenced.img" in the Documents folder of the "Attacker Machine-1" and identify a user from the image file. (Practical Question)

A. smith
B. attacker
C. roger
D. john

**Answer:** B

**Explanation:**
The attacker is a user from the image file in the above scenario. A file system is a method or structure that organizes and stores files and data on a storage device, such as a hard disk, a flash drive, etc. A file system can have different types based on its format or features, such as FAT, NTFS, ext4, etc. A file system can be analyzed to extract various information, such as file names, sizes, dates, contents, etc. A Linux image is an image file that contains a copy or a snapshot of a Linux-based file system . A Linux image can be analyzed to extract various information about a Linux-based system or device . To analyze the file system of a Linux image captured from a device that has been attacked recently and identify a user from the image file, one has to follow these steps:
? Navigate to Documents folder of Attacker Machine-1.
? Right-click on Evidenced.img file and select Mount option.
? Wait for the image file to be mounted and assigned a drive letter.
? Open File Explorer and navigate to the mounted drive.
? Open etc folder and open passwd file with a text editor.
? Observe the user accounts listed in the file. The user accounts listed in the file are:
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www- data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100: systemd-network:x: systemd-resolve:x: systemd-bus-proxy:x: syslog:x: _apt:x: messagebus:x: uuidd:x: lightdm:x: whoopsie:x: avahi-autoipd:x: avahi:x: dnsmasq:x: colord:x: speech-dispatcher:x: hplip:x: kernoops:x: saned:x: nm-openvpn:x: nm- openconnect:x: pulse:x: rtkit:x: sshd:x: attacker::1000
The user account that is not a system or service account is attacker, which is a user from the image file.

**NEW QUESTION 112**
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 115**
.....

# 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