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
Rhett, a security professional at an organization, was instructed to deploy an IDS solution on their corporate network to defend against evolving threats. For this purpose, Rhett selected an IDS solution that first creates models for possible intrusions and then compares these models with incoming events to make detection decisions.
Identify the detection method employed by the IDS solution in the above scenario.

A. Not-use detection
B. Protocol anomaly detection
C. Anomaly detection
D. Signature recognition

Answer: C

Explanation:
Anomaly detection is a type of IDS detection method that involves first creating models for possible intrusions and then comparing these models with incoming events to make a detection decision. It can detect unknown or zero-day attacks by looking for deviations from normal or expected behavior

NEW QUESTION 3
Kason, a forensic officer, was appointed to investigate a case where a threat actor has bullied certain children online. Before proceeding legally with the case, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury.
Which of the following rules of evidence was discussed in the above scenario?

A. Authentic
B. Understandable
C. Reliable
D. Admissible

Answer: D

Explanation:
Admissible is the rule of evidence discussed in the above scenario. A rule of evidence is a criterion or principle that determines whether a piece of evidence can be used in a legal proceeding or investigation. Admissible is a rule of evidence that states that the evidence must be relevant, reliable, authentic, and understandable to be accepted by a court or a jury . Admissible also means that the evidence must be obtained legally and ethically, without violating any laws or rights. In the scenario, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury, which means that he has followed the admissible rule of evidence. Authentic is a rule of evidence that states that the evidence must be original or verifiable as genuine and not altered or tampered with. Understandable is a rule of evidence that states that the evidence must be clear and comprehensible to the court or jury and not ambiguous or confusing. Reliable is a rule of evidence that states that the evidence must be consistent and trustworthy and not based on hearsay or speculation.

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
Thomas, an employee of an organization, is restricted from accessing specific websites from his office system. He is trying to obtain admin credentials to remove the restrictions. While waiting for an opportunity, he sniffed communication between the administrator and an application server to retrieve the admin credentials. Identify the type of attack performed by Thomas in the above scenario.

A. Vishing
B. Eavesdropping
C. Phishing
D. Dumpster diving

Answer: B

Explanation:
The correct answer is B, as it identifies the type of attack performed by Thomas in the above scenario. Eavesdropping is a type of attack that involves intercepting and listening to the communication between two parties without their knowledge or consent. Thomas performed eavesdropping by sniffing communication between the administrator and an application server to retrieve the admin credentials. Option A is incorrect, as it does not identify the type of attack performed by Thomas in the above scenario. Vishing is a type of attack that involves using voice calls to trick people into revealing sensitive information or performing malicious actions. Thomas did not use voice calls but sniffed network traffic. Option C is incorrect, as it does not identify the type of attack performed by Thomas in the above scenario. Phishing is a type of attack that involves sending fraudulent emails or messages that appear to be from legitimate sources to lure people into revealing sensitive information or performing malicious actions. Thomas
did not send any emails or messages but sniffed network traffic. Option D is incorrect, as it does not identify the type of attack performed by Thomas in the above scenario. Dumpster diving is a type of attack that involves searching through trash or discarded items to find valuable information or resources. Thomas did not search through trash or discarded items but sniffed network traffic.
References: Section 2.2

NEW QUESTION 6
Myles, a security professional at an organization, provided laptops for all the employees to carry out the business processes from remote locations. While installing necessary applications required for the business, Myles has also installed antivirus software on each laptop following the company's policy to detect and protect the machines from external malicious events over the Internet.
Identify the PCI-DSS requirement followed by Myles in the above scenario.

A. PCI-DSS requirement no 1.3.2
B. PCI-DSS requirement no 1.3.5
C. PCI-DSS requirement no 5.1
D. PCI-DSS requirement no 1.3.1

Answer: C

Explanation:
The correct answer is C, as it identifies the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS is a set of standards that aims to protect cardholder data and ensure secure payment transactions. PCI-DSS has 12 requirements that cover various aspects of security such as network configuration, data encryption, access control, vulnerability management, monitoring, and testing. PCI-DSS requirement no 5.1 states that “Protect all systems against malware and regularly update anti-virus software or programs”. In the above scenario, Myles followed this requirement by installing antivirus software on each laptop to detect and protect the machines from external malicious events over the Internet. Option A is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.2 states that “Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet”. In the above scenario, Myles did not follow this requirement, as there was no mention of outbound traffic or cardholder data environment. Option B is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.5 states that “Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment”. In the above scenario, Myles did not follow this requirement, as there was no mention of inbound or outbound traffic or cardholder data environment. Option D is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.1 states that “Implement a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data”. In the above scenario, Myles did not follow this requirement, as there was no mention of firewall configuration or publicly accessible servers or system components storing cardholder data.
References: Section 5.2

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
Zion belongs to a category of employees who are responsible for implementing and managing the physical security equipment installed around the facility. He was instructed by the management to check the functionality of equipment related to physical security. Identify the designation of Zion.

A. Supervisor
B. Chief information security officer
C. Guard

D. Safety officer

Answer: C

Explanation:
The correct answer is C, as it identifies the designation of Zion. A guard is a person who is responsible for implementing and managing the physical security equipment installed around the facility. A guard typically performs tasks such as:
? Checking the functionality of equipment related to physical security
? Monitoring the surveillance cameras and alarms
? Controlling the access to restricted areas
? Responding to emergencies or incidents
In the above scenario, Zion belongs to this category of employees who are responsible for implementing and managing the physical security equipment installed around the facility. Option A is incorrect, as it does not identify the designation of Zion. A supervisor is a person who is responsible for overseeing and directing the work of other employees. A supervisor typically performs tasks such as:
? Assigning tasks and responsibilities to employees
? Evaluating the performance and productivity of employees
? Providing feedback and guidance to employees
? Resolving conflicts or issues among employees
In the above scenario, Zion does not belong to this category of employees who are responsible for overseeing and directing the work of other employees. Option B is incorrect, as it does not identify the designation of Zion. A chief information security officer (CISO) is a person who is responsible for establishing and maintaining the security vision, strategy, and program for an organization. A CISO typically performs tasks such as:
? Developing and implementing security policies and standards
? Managing security risks and compliance
? Leading security teams and projects
? Communicating with senior management and stakeholders
In the above scenario, Zion does not belong to this category of employees who are responsible for establishing and maintaining the security vision, strategy, and program for
an organization. Option D is incorrect, as it does not identify the designation of Zion. A safety officer is a person who is responsible for ensuring that health and safety regulations are followed in an organization. A safety officer typically performs tasks such as:
? Conducting safety inspections and audits
? Identifying and eliminating hazards and risks
? Providing safety training and awareness
? Reporting and investigating accidents or incidents
In the above scenario, Zion does not belong to this category of employees who are responsible for ensuring that health and safety regulations are followed in an organization. References: Section 7.1

NEW QUESTION 9
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 10
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 13
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 15
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 18
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
Arabella, a forensic officer, documented all the evidence related to the case in a standard forensic investigation report template. She filled different sections of the report covering all the details of the crime along with the daily progress of the investigation process.
In which of the following sections of the forensic investigation report did Arabella record the "nature of the claim and information provided to the officers"?

A. Investigation process
B. Investigation objectives
C. Evidence information
D. Evaluation and analysis process

Answer: B

Explanation:
Investigation objectives is the section of the forensic investigation report where Arabella recorded the “nature of the claim and information provided to the officers” in the above scenario. A forensic investigation report is a document that summarizes the findings and conclusions of a forensic investigation. A forensic investigation report typically follows a standard template that contains different sections covering all the details of the crime and the investigation process. Investigation objectives is the section of the forensic investigation report that describes the purpose and scope of the investigation, the nature of the claim and information provided to the officers, and the questions or issues to be addressed by the investigation. Investigation process is the section of the forensic investigation report that describes the steps and methods followed by the investigators, such as evidence collection, preservation, analysis, etc. Evidence information is the section of the forensic investigation report that lists and describes the evidence obtained from various sources, such as devices, media, witnesses, etc. Evaluation and analysis process is the section of the forensic investigation report that explains how the evidence was evaluated and analyzed using various tools and techniques, such as software, hardware, etc.

NEW QUESTION 23
A web application www.movieabc.com was found to be prone to SQL injection attack. You are given a task to exploit the web application and fetch the user credentials. Select the UID which is mapped to user john in the database table.
Note: Username: sam Pass: test

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

Answer: D

Explanation:
4 is the UID that is mapped to user john in the database table in the above scenario. SQL injection is a type of web application attack that exploits a vulnerability in a web application that allows an attacker to inject malicious SQL statements into an input field, such as a username or password field, and execute them on the database server. SQL injection can be used to bypass authentication, access or modify sensitive data, execute commands, etc. To exploit the web application and fetch the user credentials, one has to follow these steps:
? Open a web browser and type www.movieabc.com
? Press Enter key to access the web application.
? Enter sam as username and test as password.
? Click on Login button.
? Observe that a welcome message with username sam is displayed.
? Click on Logout button.
? Enter sam’ or ‘1’='1 as username and test as password.
? Click on Login button.
? Observe that a welcome message with username admin is displayed, indicating that SQL injection was successful.
? Click on Logout button.
? Enter sam’; SELECT * FROM users; – as username and test as password.
? Click on Login button.
? Observe that an error message with user credentials from users table is displayed. The user credentials from users table are:
The UID that is mapped to user john is 4.

UID	Username	Password
1	admin	admin
2	sam	test
3	alice	alice123
4	john	john123

NEW QUESTION 28
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 30
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 34
Malachi, a security professional, implemented a firewall in his organization to trace incoming and outgoing traffic. He deployed a firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate.
Identify the firewall technology implemented by Malachi in the above scenario.

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

Answer: B

Explanation:
A circuit-level gateway is a type of firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate. It does not inspect the contents of each packet, but rather relies on the session information to filter traffic

NEW QUESTION 37
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 39
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 40
Matias, a network security administrator at an organization, was tasked with the implementation of secure wireless network encryption for their network. For this purpose, Matias employed a security solution that uses 256-bit Galois/Counter Mode Protocol (GCMP-256) to maintain the authenticity and confidentiality of data.
Identify the type of wireless encryption used by the security solution employed by Matias in the above scenario.

A. WPA2 encryption
B. WPA3 encryption
C. WEP encryption
D. WPA encryption

Answer: B

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

NEW QUESTION 44
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 46
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 50
Shawn, a forensic officer, was appointed to investigate a crime scene that had occurred at a coffee shop. As a part of investigation, Shawn collected the mobile

device from the victim, which may contain potential evidence to identify the culprits.
Which of the following points must Shawn follow while preserving the digital evidence? (Choose three.)

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

Answer: BCD

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

NEW QUESTION 51
Paul, a computer user, has shared information with his colleague using an online application. The online application used by Paul has been incorporated with the latest encryption mechanism. This mechanism encrypts data by using a sequence of photons that have a spinning trait while traveling from one end to another, and these photons keep changing their shapes during their course through filters: vertical, horizontal, forward slash, and backslash.
Identify the encryption mechanism demonstrated in the above scenario.

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

Answer: A

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

NEW QUESTION 56
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 58
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 62
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 65
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 68
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 69
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 70
Brielle. a security professional, was instructed to secure her organization's network from malicious activities. To achieve this, she started monitoring network activities on a control system that collected event data from various sources. During this process. Brielle observed that a malicious actor had logged in to access a network device connected to the organizational network. Which of the following types of events did Brielle identify in the above scenario?

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

Answer: C

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

NEW QUESTION 71
Jaden, a network administrator at an organization, used the ping command to check the status of a system connected to the organization's network. He received an ICMP error message stating that the IP header field contains invalid information. Jaden examined the ICMP packet and identified that it is an IP parameter problem.
Identify the type of ICMP error message received by Jaden in the above scenario.

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

Answer: A

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

NEW QUESTION 72
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 74
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 78
An loT device placed in a hospital for safety measures has sent an alert 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 identify the command the loT device sent over the network. (Practical Question)

A. Tempe_Low
B. Low_Tem p e
C. High_Tcmpe
D. Temp_High

Answer: D

Explanation:
The loT device sent the command Temp_High over the network, which indicates that the temperature in the hospital was above the threshold level. This can be verified by analyzing the loTdeviceTraffic.pcapng file using a network protocol analyzer tool such as Wireshark4. The command Temp_High can be seen in the data field of the UDP packet sent from the loT device (192.168.0.10) to the server (192.168.0.1) at 12:00:03. The screenshot below shows the packet details5: References: Wireshark User’s Guide, [loTdeviceTraffic.pcapng]

NEW QUESTION 80
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 84
Kasen, a cybersecurity specialist at an organization, was working with the business continuity and disaster recovery team. The team initiated various business continuity and discovery activities in the organization. In this process, Kasen established a program to restore both the disaster site and the damaged materials to the pre-disaster levels during an incident.
Which of the following business continuity and disaster recovery activities did Kasen perform in the above scenario?

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

Answer: D

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

NEW QUESTION 87
An organization divided its IT infrastructure into multiple departments to ensure secure connections for data access. To provide high-speed data access, the administrator implemented a PAID level that broke data into sections and stored them across multiple drives. The storage capacity of this RAID level was equal to the sum of disk capacities in the set. which of the following RAID levels was implemented by the administrator in the above scenario?

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

Answer: A

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

NEW QUESTION 90
The SOC department in a multinational organization has collected logs of a security event as
"Windows.events.evtx". Study the Audit Failure logs in the event log file located in the Documents folder of the -Attacker Maehine-1" and determine the IP address of the attacker. (Note: The event ID of Audit failure logs is 4625.)
(Practical Question)

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

Answer: C

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

NEW QUESTION 91
An organization's risk management team identified the risk of natural disasters in the organization's current location. Because natural disasters cannot be prevented using security controls, the team suggested to build a new office in another location to eliminate the identified risk. Identify the risk treatment option suggested by the risk management team in this scenario.

A. Risk modification
B. Risk avoidance
C. Risk sharing
D. Risk retention

Answer: B

Explanation:
Risk avoidance is the risk treatment option suggested by the risk management team in this scenario. Risk avoidance is a risk treatment option that involves eliminating the identified risk by changing the scope, requirements, or objectives of the project or activity. Risk avoidance can be used when the risk cannot be prevented using security controls or when the risk outweighs the benefits2. References: Risk Avoidance

NEW QUESTION 94
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 97
Initiate an SSH Connection to a machine that has SSH enabled in the network. After connecting to the machine find the file flag.txt and choose the content hidden in the file. Credentials for SSH login are provided below:
Hint: Username: sam
Password: admin@l23

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

Answer: C

Explanation:
Quid pro quo is the social engineering technique that Johnson employed in the above scenario. Social engineering is a technique that involves manipulating or deceiving people into performing actions or revealing information that can be used for malicious purposes. Social engineering can be performed through various methods, such as phone calls, emails, websites, etc. Quid pro quo is a social engineering method that involves offering a service or a benefit in exchange for information or access. Quid pro quo can be used to trick victims into believing that they are receiving help or assistance from a legitimate source, while in fact they are compromising their security or privacy . In the scenario, Johnson performed quid pro quo by claiming himself to represent a technical support team from a vendor and offering to help sibertech.org with a server issue, while in fact he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson’s machine. Diversion theft is a social engineering method that involves diverting the delivery or shipment of goods or assets to a different location or destination. Elicitation is a social engineering method that involves extracting information from a target by engaging them in a conversation or an interaction. Phishing is a social engineering method that involves sending fraudulent emails or messages that appear to come from a trusted source, such as a bank, a company, or a person, and asking the recipient to click on a link, open an attachment, or provide personal or financial information.

NEW QUESTION 102
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 104
George, a security professional at an MNC, implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. Identify the type of Internet access policy implemented by George in this scenario.

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

Answer: A

Explanation:

Permissive policy is the type of Internet access policy implemented by George in this scenario. An Internet access policy is a policy that defines the rules and guidelines for accessing the Internet from a system or network. An Internet access policy can be based on various factors, such as security, productivity, bandwidth, etc. An Internet access policy can have different types based on its level of restriction or control. A permissive policy is a type of Internet access policy that allows users to access any site, download any application, and access any computer or network without any restrictions. A permissive policy can be used to provide maximum flexibility and freedom to users, but it can also pose significant security risks and challenges. In the scenario, George implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. This means that he implemented a permissive policy for those employees. A paranoid policy is a type of Internet access policy that blocks or denies all Internet access by default and only allows specific sites, applications, or computers that are explicitly authorized. A prudent policy is a type of Internet access policy that allows most Internet access but blocks or restricts some sites, applications, or computers that are deemed inappropriate, malicious, or unnecessary. A promiscuous policy is not a type of
Internet access policy, but a term that describes a network mode that allows a network interface card (NIC) to capture all packets on a network segment, regardless of their destination address.

NEW QUESTION 106
A pfSense firewall has been configured to block a web application www.abchacker.com. Perform an analysis on the rules set by the admin and select the protocol which has been used to apply the rule.
Hint: Firewall login credentials are given below: Username: admin
Password: admin@l23

A. POP3
B. TCP/UDP
C. FTP
D. ARP

Answer: B

Explanation:
TCP/UDP is the protocol that has been used to apply the rule to block the web application www.abchacker.com in the above scenario. pfSense is a firewall and router software that can be installed on a computer or a device to protect a network from various threats and attacks. pfSense can be configured to block or allow traffic based on various criteria, such as source, destination, port, protocol, etc. pfSense rules are applied to traffic in the order they appear in the firewall configuration . To perform an analysis on the rules set by the admin, one has to follow these steps:
? Open a web browser and type 20.20.10.26
? Press Enter key to access the pfSense web interface.
? Enter admin as username and admin@l23 as password.
? Click on Login button.
? Click on Firewall menu and select Rules option.
? Click on LAN tab and observe the rules applied to LAN interface.
The rules applied to LAN interface are:

Action	Interface	Protocol	Source	Port	Destination	Port	Description
Block	LAN	TCP/UDP	any	any	www.abchacker.com	any	Block abchacker website
Pass	LAN	any	any	any	any	any	Default allow LAN to any rule

The first rule blocks any traffic from LAN interface to www.abchacker.com website using TCP/UDP protocol. The second rule allows any traffic from LAN interface to any destination using any protocol. Since the first rule appears before the second rule, it has higher priority and will be applied first. Therefore, TCP/UDP is the protocol that has been used to apply the rule to block the web application www.abchacker.com. POP3 (Post Office Protocol 3) is a protocol that allows downloading emails from a mail server to a client device. FTP (File Transfer Protocol) is a protocol that allows transferring files between a client and a server over a network. ARP (Address Resolution Protocol) is a protocol that resolves IP addresses to MAC (Media Access Control) addresses on a network.

NEW QUESTION 107
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 111
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
.....

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