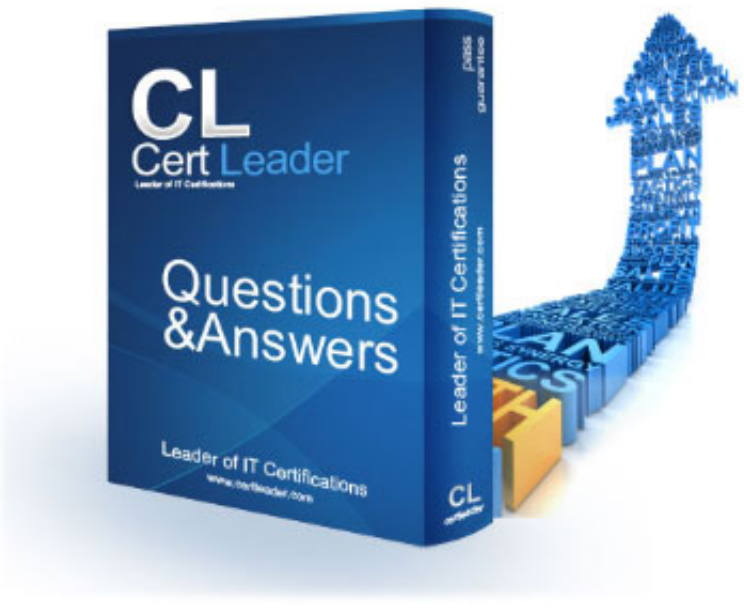
212-82 Dumps

Certified Cybersecurity Technician(C|CT)

https://www.certleader.com/212-82-dumps.html



NEW QUESTION 1
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 2
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 3
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 4
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 5
Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, 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. What is the social engineering technique Steve employed in the above scenario?

A. Quid pro quo
B. Diversion theft
C. Elicitation
D. Phishing

Answer: A

Explanation:
Quid pro quo is the social engineering technique that Johnson employed in the above scenario. 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. If you want to learn more about social engineering techniques, you can check out these resources:
? [1] A guide to different types of social engineering attacks and how to prevent
them: [https://www.csoonline.com/article/2124681/what-is-social-engineering.html]
? [2] A video that explains how quid pro quo works and how to avoid falling for it: [https://www.youtube.com/watch?v=3Yy0gZ9xw8g]
? [3] A quiz that tests your knowledge of social engineering techniques and scenarios: [https://www.proprofs.com/quiz-school/story.php?title=social- engineering-quiz]

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
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 9
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 10
Tristan, a professional penetration tester, was recruited by an organization to test its network infrastructure. The organization wanted to understand its current security posture and its strength in defending against external threats. For this purpose, the organization did not provide any information about their IT infrastructure to Tristan. Thus, Tristan initiated zero-knowledge attacks, with no information or assistance from the organization.
Which of the following types of penetration testing has Tristan initiated in the above scenario?

A. Black-box testing
B. White-box testing
C. Gray-box testing
D. Translucent-box testing

Answer: A

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

NEW QUESTION 10
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 14
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 17
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 19
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 23
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 25
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 27
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 32
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 37
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 38
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 43
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 47
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 48
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 51
Steve, a network engineer, was tasked with troubleshooting a network issue that is causing unexpected packet drops. For this purpose, he employed a network troubleshooting utility to capture the ICMP echo request packets sent to the server. He identified that certain packets are dropped at the gateway due to poor network connection.
Identify the network troubleshooting utility employed by Steve in the above scenario.

A. dnsenurn
B. arp
C. traceroute
D. ipconfig

Answer: C

Explanation:
Traceroute is the network troubleshooting utility employed by Steve in the above scenario. Traceroute is a utility that traces the route of packets from a source host to a destination host over a network. Traceroute sends ICMP echo request packets with increasing TTL (Time to Live) values and records the ICMP echo reply packets from each intermediate router or gateway along the path. Traceroute can help identify the network hops, latency, and packet loss between the source and destination hosts . Dnsenum is a utility that enumerates DNS information from a domain name or an IP address. Arp is a utility that displays and modifies the ARP (Address Resolution Protocol) cache of a host. Ipconfig is a utility that displays and configures the IP (Internet Protocol) settings of a host.

NEW QUESTION 52
Andre, a security professional, was tasked with segregating the employees' names, phone numbers, and credit card numbers before sharing the database with clients. For this purpose, he implemented a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#).
Which of the following techniques was employed by Andre in the above scenario?

A. Tokenization
B. Masking
C. Hashing
D. Bucketing

Answer: B

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

NEW QUESTION 56
Leilani, a network specialist at an organization, employed Wireshark for observing network traffic. Leilani navigated to the Wireshark menu icon that contains items to manipulate, display and apply filters, enable, or disable the dissection of protocols, and configure user- specified decodes.
Identify the Wireshark menu Leilani has navigated in the above scenario.

A. Statistics
B. Capture
C. Main toolbar
D. Analyze

Answer: B

Explanation:
Capture is the Wireshark menu that Leilani has navigated in the above scenario. Wireshark is a network analysis tool that captures and displays network traffic in real-time or from saved files. Wireshark has various menus that contain different items and options for manipulating, displaying, and analyzing network data. Capture is the Wireshark menu that contains items to start, stop, restart, or save a live capture of network traffic. Capture also contains items to configure capture filters, interfaces, options, and preferences . Statistics is the Wireshark menu that contains items to display various statistics and graphs of network traffic, such as packet lengths, protocols, endpoints, conversations, etc. Main toolbar is the Wireshark toolbar that contains icons for quick access to common functions, such as opening or saving files, starting or stopping a capture, applying display filters, etc. Analyze is the Wireshark menu that contains items to manipulate, display and apply filters, enable or disable the dissection of protocols, and configure user-specified decodes.

NEW QUESTION 57
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 61
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 63
Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?

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

Answer: B

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

NEW QUESTION 67
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 68
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 71
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 72
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 77
Ashton is working as a security specialist in SoftEight Tech. He was instructed by the management to strengthen the Internet access policy. For this purpose, he implemented a type of Internet access policy that forbids everything and imposes strict restrictions on all company computers, whether it is system or network usage.

Identify the type of Internet access policy implemented by Ashton in the above scenario.

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

Answer: A

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

NEW QUESTION 82
Stella purchased a smartwatch online using her debit card. After making payment for the product through the payment gateway, she received a transaction text message with a deducted and available balance from her bank.
Identify the information security element that ensures that Stella's transaction status is immediately reflected in her bank account in this scenario.

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

Answer: C

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

NEW QUESTION 86
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 212-82 Exam with Our Prep Materials Via below:

https://www.certleader.com/212-82-dumps.html