# EC-Council

## Exam Questions 212-82

Certified Cybersecurity Technician(C|CT)

**NEW QUESTION 1**
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 2**
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 3**
A software company is developing a new software product by following the best practices for secure application development. Dawson, a software analyst, is checking the performance of the application on the client's network to determine whether end users are facing any issues in accessing the application.
Which of the following tiers of a secure application development lifecycle involves checking the performance of the application?

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

**Answer:** B

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

**NEW QUESTION 4**
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 5**
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 6**

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

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

**Answer:** A

**Explanation:**

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


**NEW QUESTION 7**
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 8**
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 9**
Dany, a member of a forensic team, was actively involved in an online crime investigation process. Dany's main responsibilities included providing legal advice on conducting the investigation and addressing legal issues involved in the forensic investigation process. Identify the role played by Dany in the above scenario.

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 10**
A disgruntled employee has set up a RAT (Remote Access Trojan) server in one of the machines in the target network to steal sensitive corporate documents. The IP address of the target machine where the RAT is installed is 20.20.10.26. Initiate a remote connection to the target machine from the "Attacker Machine-1" using the Theef client. Locate the "Sensitive Corporate Documents" folder in the target machine's Documents directory and determine the number of files. Mint: Theef folder is located at Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Theef of the Attacker Machine1.

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

**Answer:** B

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

**NEW QUESTION 10**
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 11**
An IoT 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 14**
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 19**
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 21**
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 25**
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 27**
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 30**
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 35**
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 39**
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 42**
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 45**
Stephen, a security professional at an organization, was instructed to implement security measures that prevent corporate data leakage on employees' mobile devices. For this purpose, he employed a technique using which all personal and corporate data are isolated on an employee's mobile device. Using this technique, corporate applications do not have any control of or communication with the private applications or data of the employees.
Which of the following techniques has Stephen implemented in the above scenario?

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

**Answer:** C

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

**NEW QUESTION 50**
......

# 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

## 100% Actual & Verified — Instant Download, Please Click
[Order The 212-82 Practice Test Here](https://www.surepassexam.com/212-82-exam-dumps.html)