212-82^{Q&As}

212-82^{Q&As}

Certified Cybersecurity Technician(C|CT)

Pass EC-COUNCIL 212-82 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/212-82.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

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

A. Incident impact assessment

B. Close the investigation

C. Review and revise policies

D. Incident disclosure

Correct Answer: A

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

QUESTION 2

Shawn, a forensic officer, was appointed to investigate a crime scene that had occurred at a coffee shop. As a part of investigation, Shawn collected the mobile device from the victim, which may contain potential evidence to identify the culprits.

Which of the following points must Shawn follow while preserving the digital evidence? (Choose three.)

A. Never record the screen display of the device

B. Turn the device ON if it is OFF

C. Do not leave the device as it is if it is ON

D. Make sure that the device is charged

Correct Answer: BCD

Explanation: Turn the device ON if it is OFF, do not leave the device as it is if it is ON, and make sure that the device is charged are some of the points that Shawn must follow while preserving the digital evidence in the above scenario. Digital evidence is any information or data stored or transmitted in digital form that can be used in a legal proceeding or investigation. Digital evidence can be found on various devices, such as computers, mobile phones, tablets, etc. Preserving digital evidence is a crucial step in forensic investigation that involves protecting and maintaining the integrity and authenticity of digital evidence from any alteration or damage. Some of the points that Shawn must follow while preserving digital evidence are: Turn the device ON if it is OFF: If the device is OFF, Shawn must turn it ON to prevent any data loss or encryption that may occur when the device is powered off. Shawn must also document any password or PIN required to unlock or access the device. Do not leave the device as it is if it is ON: If the device is ON, Shawn must not leave it as it is or use it for any purpose other than preserving digital evidence. Shawn must also disable any network connections or communication features on the device, such as Wi-Fi, Bluetooth, cellular data, etc., to prevent any remote access or deletion of data by unauthorized parties. Make sure that the device is charged: Shawn must

ensure that the device has enough battery power to prevent any data loss or corruption that may occur due to sudden shutdown or low battery. Shawn must also use a write blocker or a Faraday bag to isolate the device from any external interference or signals. Never record the screen display of the device is not a point that Shawn must follow while preserving digital evidence. On contrary, Shawn should record or photograph the screen display of the device to capture any relevant information or messages that may appear on the screen. Recording or photographing the screen display of the device can also help document any changes or actions performed on the device during preservation.

QUESTION 3

Matias, a network security administrator at an organization, was tasked with the implementation of secure wireless network encryption for their network. For this purpose, Matias employed a security solution that uses 256-bit Galois/Counter Mode Protocol (GCMP-256) to maintain the authenticity and confidentiality of data.

Identify the type of wireless encryption used by the security solution employed by Matias in the above scenario.

A. WPA2 encryption

B. WPA3 encryption

C. WEP encryption

D. WPA encryption

Correct Answer: B

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

QUESTION 4

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

Correct 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.

QUESTION 5

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

A. Third-party account

B. Croup-based account

C. Shared account

D. Application account

Correct Answer: B

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

QUESTION 6

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

Correct 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.

QUESTION 7

Ruben, a crime investigator, wants to retrieve all the deleted files and folders in the suspected media without affecting the original files. For this purpose, he uses a method that involves the creation of a cloned copy of the entire media and prevents the contamination of the original media.

Identify the method utilized by Ruben in the above scenario.

A. Sparse acquisition

B. Bit-stream imaging

C. Drive decryption

D. Logical acquisition

Correct Answer: B

Explanation: Bit-stream imaging is the method utilized by Ruben in the above scenario. Bit-stream imaging is a method that involves creating a cloned copy of the entire media and prevents the contamination of the original media. Bit-stream imaging copies all the data on the media, including deleted files and folders, hidden partitions, slack space, etc., at a bit level. Bit-stream imaging preserves the integrity and authenticity of the digital evidence and allows further analysis without affecting the original media. Sparse acquisition is a method that involves creating a partial copy of the media by skipping empty sectors or blocks. Drive decryption is a method that involves decrypting an encrypted drive or partition using a password or a key. Logical acquisition is a method that involves creating a copy of the logical files and folders on the media using file system commands.

QUESTION 8

Anderson, a security engineer, was Instructed to monitor all incoming and outgoing traffic on the organization\\'s network to identify any suspicious traffic. For this purpose, he employed an analysis technique using which he analyzed packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit.

Identify the type of attack signature analysis performed by Anderson in the above scenario.

A. Context-based signature analysis

B. Atomic-signature-based analysis

C. Composite-signature-based analysis

D. Content-based signature analysis

Correct Answer: D

Explanation: Content-based signature analysis is the type of attack signature analysis performed by Anderson in the above scenario. Content-based signature analysis is a technique that analyzes packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit. Content-based signature analysis can help detect attacks that manipulate packet headers to evade detection or exploit vulnerabilities . Context-based signature analysis is a technique that analyzes packet payloads such as application data or commands to check whether they match any known attack patterns or signatures. Atomic-signature-based analysis is a technique that analyzes individual packets to check whether they match any known attack patterns or signatures. Composite-signature-based analysis is a technique that analyzes multiple packets or sessions to check whether they match any known attack patterns or signatures.

QUESTION 9

Arabella, a forensic officer, documented all the evidence related to the case in a standard forensic investigation report template. She filled different sections of the report covering all the details of the crime along with the daily progress of the investigation process.

In which of the following sections of the forensic investigation report did Arabella record the "nature of the claim and information provided to the officers"?

A. Investigation process

B. Investigation objectives

C. Evidence information

D. Evaluation and analysis process

Correct Answer: B

Explanation: Investigation objectives is the section of the forensic investigation report where Arabella recorded the "nature of the claim and information provided to the officers" in the above scenario. A forensic investigation report is a document that summarizes the findings and conclusions of a forensic investigation. A forensic investigation report typically follows a standard template that contains different sections covering all the details of the crime and the investigation process. Investigation objectives is the section of the forensic investigation report that describes the purpose and scope of the investigation, the nature of the claim and information provided to the officers, and the questions or issues to be addressed by the investigation. Investigation process is the section of the forensic investigation report that describes the steps and methods followed by the investigators, such as evidence collection, preservation, analysis, etc. Evidence information is the section of the forensic investigation report that lists and

describes the evidence obtained from various sources, such as devices, media, witnesses, etc. Evaluation and analysis process is the section of the forensic investigation report that explains how the evidence was evaluated and analyzed using various tools and techniques, such as software, hardware, etc.

QUESTION 10

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

Correct 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

QUESTION 11

Sam, a software engineer, visited an organization to give a demonstration on a software tool that helps in business development. The administrator at the organization created a least privileged account on a system and allocated that system to Sam for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file in the system.

Which of the following types of accounts the organization has given to Sam in the above scenario?

A. Service account

B. Guest account

C. User account

D. Administrator account

Correct Answer: B

Explanation: The correct answer is B, as it identifies the type of account that the organization has given to Sam in the above scenario. A guest account is a type of account that allows temporary or limited access to a system or network for visitors or users who do not belong to the organization. A guest account typically has minimal privileges and permissions and can only access certain files or applications. In the above scenario, the organization has given Sam a guest account for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file in the system. Option A is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. A service account is a type of account that allows applications or services to run on a system or network under a specific identity. A service account typically has high privileges and permissions and can access various files or applications. In the above scenario, the organization has not given Sam a service account for the demonstration. Option C is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. A user account is a type of account that allows regular access to a system or network for employees or members of an organization. A user account typically has moderate privileges and permissions and can access various files or applications depending on their role. In the above scenario, the organization has not given Sam a user account for the demonstration. Option D is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. An administrator account is a type of account that allows full access to a system or network for administrators or managers of an organization. An administrator account typically has the highest privileges and permissions and can access and modify any files or applications. In the above scenario, the organization has not given Sam an administrator account for the demonstration. References: , Section 4.1

QUESTION 12

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

Correct 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.

QUESTION 13

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

Correct Answer: D

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

QUESTION 14

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

Correct 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.

QUESTION 15

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

Correct 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