



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.passapply.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

A text file containing sensitive information about the organization has been leaked and modified to bring down the reputation of the organization. As a safety measure, the organization did contain the MD5 hash of the original file. The file which has been leaked is retained for examining the integrity. A file named "Sensitiveinfo.txt" along with OriginalFileHash.txt has been stored in a folder named Hash in Documents of Attacker Machine-1. Compare the hash value of the original file with the leaked file and state whether the file has been modified or not by selecting yes or no.

- A. No
- B. Yes

Correct Answer: B

Explanation: Yes is the answer to whether the file has been modified or not in the above scenario. A hash is a fixed-length string that is generated by applying a mathematical function, called a hash function, to a piece of data, such as a file or a message. A hash can be used to verify the integrity or authenticity of data by comparing it with another hash value of the same data. A hash value is unique and any change in the data will result in a different hash value. To compare the hash value of the original file with the leaked file and state whether the file has been modified or not, one has to follow these steps: Navigate to Hash folder in Documents of Attacker-1 machine. Open OriginalFileHash.txt file with a text editor. Note down the MD5 hash value of the original file as 8f14e45fceeaa167a5a36dedd4bea2543. Open Command Prompt and change directory to Hash folder using cd command. Type certutil -hashfile Sensitiveinfo.txt MD5 and press Enter key to generate MD5 hash value of leaked file. Note down the MD5 hash value of leaked file as 9f14e45fceeaa167a5a36dedd4bea2543. Compare both MD5 hash values. The MD5 hash values are different, which means that the file has been modified.

QUESTION 2

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

Correct 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.

QUESTION 3

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

Correct 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.

QUESTION 4

Jase, a security team member at an organization, was tasked with ensuring uninterrupted business operations under hazardous conditions. Thus, Jase implemented a deterrent control strategy to minimize the occurrence of threats, protect critical business areas, and mitigate the impact of threats. Which of the following business continuity and disaster recovery activities did Jase perform in this scenario?

- A. Prevention
- B. Response
- C. Restoration
- D. Recovery

Correct Answer: A

Explanation: Prevention is the business continuity and disaster recovery activity performed by Jase in this scenario. Prevention is an activity that involves implementing a deterrent control strategy to minimize the occurrence of threats, protect critical business areas, and mitigate the impact of threats. Prevention can include measures such as backup systems, firewalls, antivirus software, or physical security. References: Prevention Activity in BCDR



QUESTION 5

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

[Latest 212-82 Dumps](#)

[212-82 Exam Questions](#)

[212-82 Braindumps](#)