

# 212-82<sup>Q&As</sup>

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.leads4pass.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**

An FTP server has been hosted in one of the machines in the network. Using Cain and Abel the attacker was able to poison the machine and fetch the FTP credentials used by the admin. You're given a task to validate the credentials that were stolen using Cain and Abel and read the file flag.txt

- A. white@hat
- B. red@hat
- C. hat@red
- D. blue@hat

Correct Answer: C

---

**QUESTION 2**

Rickson, a security professional at an organization, was instructed to establish short-range communication between devices within a range of 10 cm. For this purpose, he used a mobile connection method that employs electromagnetic induction to enable communication between devices. The mobile connection method selected by Rickson can also read RFID tags and establish Bluetooth connections with nearby devices to exchange information such as images and contact lists.

Which of the following mobile connection methods has Rickson used in above scenario?

- A. NFC
- B. Satcom
- C. Cellular communication
- D. ANT

Correct Answer: A

---

**QUESTION 3**

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

Correct Answer: A

---

**QUESTION 4**

Kayden successfully cracked the final round of interview at an organization. After 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 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 company's message, and 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

---

**QUESTION 5**

Warren, a member of IHandR 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 IHandR step performed by Warren in the above scenario.

- A. Containment
- B. Recovery
- C. Eradication
- D. Incident triage

Correct Answer: A

---

**QUESTION 6**

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

---

#### QUESTION 7

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 type 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

---

#### QUESTION 8

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

Correct Answer: C

---

#### QUESTION 9

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

---

## QUESTION 10

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

Correct Answer: C

[212-82 PDF Dumps](#)

[212-82 Study Guide](#)

[212-82 Exam Questions](#)