



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

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 IoTdeviceTraffic.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

Correct Answer: C

QUESTION 2

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

QUESTION 3

The IHandR 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 IHandR 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 IHandR step performed by Edwin in the above scenario.

- A. Eradication
- B. Incident containment
- C. Notification
- D. Recovery

Correct Answer: D

QUESTION 4



A threat intelligence feed data file has been acquired and stored in the Documents folder of Attacker Machine-1 (File Name: Threatfeed.txt). You are a cybersecurity technician working for an ABC organization. Your organization has assigned you a task to analyze the data and submit a report on the threat landscape. Select the IP address linked with <http://securityabc.s21sec.com>.

- A. 5.9.200.200
- B. 5.9.200.150
- C. 5.9.110.120
- D. 5.9.188.148

Correct Answer: D

QUESTION 5

Tenda, a network specialist at an organization, was examining logged data using Windows Event Viewer to identify attempted or successful unauthorized activities. The logs analyzed by Tenda include events related to Windows security; specifically, log-on/log-off activities, resource access, and also information based on Windows system's audit policies.

Identify the type of event logs analyzed by Tenda in the above scenario.

- A. Application event log
- B. Setup event log
- C. Security event log
- D. System event log

Correct Answer: C

[212-82 PDF Dumps](#)

[212-82 VCE Dumps](#)

[212-82 Practice Test](#)