



312-85^{Q&As}

Certified Threat Intelligence Analyst

Pass EC-COUNCIL 312-85 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/312-85.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 threat analyst obtains an intelligence related to a threat, where the data is sent in the form of a connection request from a remote host to the server. From this data, he obtains only the IP address of the source and destination but no contextual information. While processing this data, he obtains contextual information stating that multiple connection requests from different geo-locations are received by the server within a short time span, and as a result, the server is stressed and gradually its performance has reduced. He further performed analysis on the information based on the past and present experience and concludes the attack experienced by the client organization.

Which of the following attacks is performed on the client organization?

- A. DHCP attacks
- B. MAC spoofing attack
- C. Distributed Denial-of-Service (DDoS) attack
- D. Bandwidth attack

Correct Answer: C

QUESTION 2

Jame, a professional hacker, is trying to hack the confidential information of a target organization. He identified the vulnerabilities in the target system and created a tailored deliverable malicious payload using an exploit and a backdoor to send it to the victim.

Which of the following phases of cyber kill chain methodology is Jame executing?

- A. Reconnaissance
- B. Installation
- C. Weaponization
- D. Exploitation

Correct Answer: C

QUESTION 3

Michael, a threat analyst, works in an organization named TechTop, was asked to conduct a cyber-threat intelligence analysis. After obtaining information regarding threats, he has started analyzing the information and understanding the nature of the threats.

What stage of the cyber-threat intelligence is Michael currently in?

- A. Unknown unknowns
- B. Unknowns unknown



C. Known unknowns

D. Known knowns

Correct Answer: C

QUESTION 4

Alice, an analyst, shared information with security operation managers and network operations center (NOC) staff for protecting the organizational resources against various threats. Information shared by Alice was highly technical and include threat actor TTPs, malware campaigns, tools used by threat actors, and so on.

Which of the following types of threat intelligence was shared by Alice?

A. Strategic threat intelligence

B. Tactical threat intelligence

C. Technical threat intelligence

D. Operational threat intelligence

Correct Answer: C

QUESTION 5

Tim is working as an analyst in an ABC organization. His organization had been facing many challenges in converting the raw threat intelligence data into meaningful contextual information. After inspection, he found that it was due to noise obtained from misrepresentation of data from huge data collections. Hence, it is important to clean the data before performing data analysis using techniques such as data reduction. He needs to choose an appropriate threat intelligence framework that automatically performs data collection, filtering, and analysis for his organization.

Which of the following threat intelligence frameworks should he choose to perform such task?

A. HighCharts

B. SIGVERIF

C. Threat grid

D. TC complete

Correct Answer: D

[312-85 PDF Dumps](#)

[312-85 VCE Dumps](#)

[312-85 Exam Questions](#)