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.leads4pass.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

Daniel is a professional hacker whose aim is to attack a system to steal data and money for profit. He performs hacking to obtain confidential data such as social security numbers, personally identifiable information (PII) of an employee, and credit card information. After obtaining confidential data, he further sells the information on the black market to make money.

Daniel comes under which of the following types of threat actor.

A. Industrial spies

B. State-sponsored hackers

C. Insider threat

D. Organized hackers

Correct Answer: D

QUESTION 2

A network administrator working in an ABC organization collected log files generated by a traffic monitoring system, which may not seem to have useful information, but after performing proper analysis by him, the same information can be used to detect an attack in the network.

Which of the following categories of threat information has he collected?

A. Advisories

B. Strategic reports

C. Detection indicators

D. Low-level data

Correct Answer: C

QUESTION 3

Enrage Tech Company hired Enrique, a security analyst, for performing threat intelligence analysis. While performing data collection process, he used a counterintelligence mechanism where a recursive DNS server is employed to perform interserver DNS communication and when a request is generated from any name server to the recursive DNS server, the recursive DNS servers log the responses that are received. Then it replicates the logged data and stores the data in the central database. Using these logs, he analyzed the malicious attempts that took place over DNS infrastructure.

Which of the following cyber counterintelligence (CCI) gathering technique has Enrique used for data collection?

A. Data collection through passive DNS monitoring

B. Data collection through DNS interrogation

C. Data collection through DNS zone transfer

D. Data collection through dynamic DNS (DDNS)

Correct Answer: B

QUESTION 4

Cybersol Technologies initiated a cyber-threat intelligence program with a team of threat intelligence analysts. During the process, the analysts started converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods.

In which of the following phases of the threat intelligence lifecycle is the threat intelligence team currently working?

A. Dissemination and integration

B. Planning and direction

C. Processing and exploitation

D. Analysis and production

Correct Answer: A

QUESTION 5

Tyrion, a professional hacker, is targeting an organization to steal confidential information. He wants to perform website footprinting to obtain the following information, which is hidden in the web page header. Connection status and content type Accept-ranges and last-modified information X-powered-by information Web server in use and its version Which of the following tools should the Tyrion use to view header content?

A. Hydra

B. AutoShun

C. Vanguard enforcer

D. Burp suite

Correct Answer: D

312-85 VCE Dumps   312-85 Study Guide   312-85 Braindumps