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

QUESTION 1

Mr. Bob, a threat analyst, is performing analysis of competing hypotheses (ACH). He has reached to a stage where he is required to apply his analysis skills effectively to reject as many hypotheses and select the best hypotheses from the identified bunch of hypotheses, and this is done with the help of listed evidence. Then, he prepares a matrix where all the screened hypotheses are placed on the top, and the listed evidence for the hypotheses are placed at the bottom.

What stage of ACH is Bob currently in?

A. Diagnostics

B. Evidence

C. Inconsistency

D. Refinement

Correct Answer: A

QUESTION 2

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 3

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

QUESTION 4

An organization suffered many major attacks and lost critical information, such as employee records, and financial information. Therefore, the management decides to hire a threat analyst to extract the strategic threat intelligence that provides high-level information regarding current cyber-security posture, threats, details on the financial impact of various cyber-activities, and so on.

Which of the following sources will help the analyst to collect the required intelligence?

A. Active campaigns, attacks on other organizations, data feeds from external third parties

B. OSINT, CTI vendors, ISAO/ISACs

C. Campaign reports, malware, incident reports, attack group reports, human intelligence

D. Human, social media, chat rooms

Correct Answer: B

QUESTION 5

In which of the following forms of bulk data collection are large amounts of data first collected from multiple sources in multiple formats and then processed to achieve threat intelligence?

A. Structured form

B. Hybrid form

C. Production form

D. Unstructured form

Correct Answer: D