312-85<sup>Q&As</sup>

312-85<sup>Q&As</sup>

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.passapply.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

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

Which of the following characteristics of APT refers to numerous attempts done by the attacker to gain entry to the target\\'s network?

A. Risk tolerance

B. Timeliness

C. Attack origination points

D. Multiphased

Correct Answer: C

## QUESTION 3

Kim, an analyst, is looking for an intelligence-sharing platform to gather and share threat information from a variety of sources. He wants to use this information to develop security policies to enhance the overall security posture of his organization.

Which of the following sharing platforms should be used by Kim?

A. Cuckoo sandbox

B. OmniPeek

C. PortDroid network analysis

D. Blueliv threat exchange network

Correct Answer: D

## QUESTION 4

An attacker instructs bots to use camouflage mechanism to hide his phishing and malware delivery locations in the rapidly changing network of compromised bots. In this particular technique, a single domain name consists of multiple IP addresses.

Which of the following technique is used by the attacker?

A. DNS zone transfer

B. Dynamic DNS

C. DNS interrogation

D. Fast-Flux DNS

Correct Answer: D

## QUESTION 5

Moses, a threat intelligence analyst at InfoTec Inc., wants to find crucial information about the potential threats the organization is facing by using advanced Google search operators. He wants to identify whether any fake websites are hosted at the similar to the organization\\'s URL.

Which of the following Google search queries should Moses use?

A. related: www.infothech.org

B. info: www.infothech.org

C. link: www.infothech.org

D. cache: www.infothech.org

Correct Answer: A

Latest 312-85 Dumps                312-85 Exam Questions                312-85 Braindumps