ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Eccouncil

Code: 312-85

Exam: Certified Threat Intelligence Analyst

https://www.examsnest.com/exam/312-85/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 5.0

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

Answer: D

Explanation:
Daniel's activities align with those typically associated with organized hackers. Organized hackers or cybercriminals work in groups with the primary goal of financial gain through illegal activities such as stealing and selling data. These groups often target large amounts of data, including personal and financial information, which they can monetize by selling on the black market or dark web. Unlike industrial spies who focus on corporate espionage or state-sponsored hackers who are backed by nation-states for political or military objectives, organized hackers are motivated by profit. Insider threats, on the other hand, come from within the organization and might not always be motivated by financial gain. The actions described in the scenario—targeting personal and financial information for sale—best fit the modus operandi of organized cybercriminal groups.
Reference:
ENISA (European Union Agency for Cybersecurity) Threat Landscape Report
Verizon Data Breach Investigations Report

Question: 2

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

Answer: D

Explanation:
Fast-Flux DNS is a technique used by attackers to hide phishing and malware distribution sites behind an ever-changing network of compromised hosts acting as proxies. It involves rapidly changing the association of domain names with multiple IP addresses, making the detection and shutdown of malicious sites more difficult. This technique contrasts with DNS zone transfers, which involve the replication of DNS data across DNS servers, or Dynamic DNS, which typically involves the automatic updating of DNS records for dynamic IP addresses, but not necessarily for malicious purposes. DNS interrogation involves querying DNS servers to retrieve information about domain names, but it does not involve hiding malicious content. Fast-Flux DNS specifically refers to the rapid changes in DNS records to obfuscate the source of the malicious activity, aligning with the scenario described.
Reference:
SANS Institute InfoSec Reading Room
ICANN (Internet Corporation for Assigned Names and Numbers) Security and Stability Advisory Committee

Question: 3

Kathy wants to ensure that she shares threat intelligence containing sensitive information with the appropriate audience. Hence, she used traffic light protocol (TLP).
Which TLP color would you signify that information should be shared only within a particular community?

A. Red
B. White
C. Green
D. Amber

Answer: D

Explanation:
In the Traffic Light Protocol (TLP), the color amber signifies that the information should be limited to those who have a need-to-know within the specified community or organization, and not further disseminated without permission. TLP Red indicates information that should not be disclosed outside of the originating organization. TLP Green indicates information that is limited to the community but can be disseminated within the community without restriction. TLP White, or TLP Clear, indicates information that can be shared freely with no restrictions. Therefore, for information meant to be shared within a particular community with some restrictions on further dissemination, TLP Amber is the appropriate designation.
Reference:
FIRST (Forum of Incident Response and Security Teams) Traffic Light Protocol (TLP) Guidelines
CISA (Cybersecurity and Infrastructure Security Agency) TLP Guidelines

Question: 4

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

Answer: A

Explanation:
The "related:" Google search operator is used to find websites that are similar or related to a specified URL. In the context provided, Moses wants to identify fake websites that may be posing as or are similar to his organization's official site. By using the "related:" operator followed by his organization's URL, Google will return a list of websites that Google considers to be similar to the specified site. This can help Moses identify potential impersonating websites that could be used for phishing or other malicious activities. The "info:", "link:", and "cache:" operators serve different purposes; "info:" provides information about the specified webpage, "link:" used to be used to find pages linking to a specific URL (but is now deprecated), and "cache:" shows the cached version of the specified webpage.
Reference:
Google Search Operators Guide by Moz
Google Advanced Search Help Documentation

Question: 5

A team of threat intelligence analysts is performing threat analysis on malware, and each of them has come up with their own theory and evidence to support their theory on a given malware.
Now, to identify the most consistent theory out of all the theories, which of the following analytic processes must threat intelligence manager use?

A. Threat modelling
B. Application decomposition and analysis (ADA)
C. Analysis of competing hypotheses (ACH)
D. Automated technical analysis

Answer: C

Explanation:
Analysis of Competing Hypotheses (ACH) is an analytic process designed to help an analyst or a team of analysts evaluate multiple competing hypotheses on an issue fairly and objectively. ACH assists in identifying and analyzing the evidence for and against each hypothesis, ultimately aiding in determining the most likely explanation. In the scenario where a team of threat intelligence analysts has various

theories on a particular malware, ACH would be the most appropriate method to assess these competing theories systematically. ACH involves listing all possible hypotheses, collecting data and evidence, and assessing the evidence's consistency with each hypothesis. This process helps in minimizing cognitive biases and making a more informed decision on the most consistent theory.
Reference:
Richards J. Heuer Jr., "Psychology of Intelligence Analysis," Central Intelligence Agency
"A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," Central Intelligence Agency

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Eccouncil

Code: 312-85

Exam: Certified Threat Intelligence Analyst

https://www.examsnest.com/exam/312-85/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation