KillTest

High Quality. Better Service

Practice Questions

https://www.killtest.com

Free updates for one year

Exam : **CPTIA**

Title : CREST Practitioner Threat Intelligence Analyst

Version : DEMO

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.
References:
ENISA (European Union Agency for Cybersecurity) Threat Landscape Report
Verizon Data Breach Investigations Report

2.Which of the following tools helps incident responders effectively contain a potential cloud security incident and gather required forensic evidence?
A. Alert Logic
B. Cloud Passage Quarantine
C. Qualys Cloud Platform
D. Cloud Passage Halo
Answer: D
Explanation:
Cloud Passage Halo is a security platform designed to provide comprehensive visibility and protection for cloud environments, making it an effective tool for incident responders dealing with potential cloud security incidents. It offers capabilities for detecting, responding to, and containing threats across public, private, and hybrid cloud environments. With features like automated security policies, compliance monitoring, and threat detection, Cloud Passage Halo enables incident responders to quickly contain incidents and gather the required forensic evidence to investigate the scope and impact of a breach or security issue. Tools like Alert Logic and Qualys Cloud Platform also provide security and compliance solutions for cloud environments, but Cloud Passage Halo is specifically recognized for its robust incident response and containment capabilities. References: The Incident Handler (CREST CPTIA) certification materials and courses discuss various tools and technologies that support cloud security incident response, including the role of platforms like Cloud Passage Halo in effective incident

management.

3.Eric is an incident responder and is working on developing incident-handling plans and procedures. As part of this process, he is performing an analysis on the organizational network to generate a report and develop policies based on the acquired results.
Which of the following tools will help him in analyzing his network and the related traffic?
A. Whois
B. Burp Suite
C. FaceNiff
D. Wireshark
Answer: D
Explanation:
Wireshark is a widely used network protocol analyzer that helps in capturing and interactively browsing the traffic on a network. It is an essential tool for incident responders like Eric who are developing incident-handling plans and procedures. By analyzing network traffic, Wireshark allows users to see what is happening on their network at a microscopic level, making it invaluable for troubleshooting network problems, analyzing security incidents, and understanding network behavior. Whois is used for querying databases that store registered users or assignees of an Internet resource. Burp Suite is a tool for testing web application security, and FaceNiff is used for session hijacking within a WiFi network, which makes Wireshark the best choice for analyzing network traffic.
References: CREST materials often reference Wireshark as a fundamental tool for network analysis, crucial for incident handlers in the analysis phase of incident response.

4.Sam received an alert through an email monitoring tool indicating that their company was targeted by a phishing attack. After analyzing the incident, Sam identified that most of the targets of the attack are high-profile executives of the company.
What type of phishing attack is this?
A. Pharming
B. Whaling
C. Puddle phishing
D. Spear phishing
Answer: B
Explanation:
Whaling is a specific type of phishing attack that targets high-profile executives or individuals within an organization, often with the intent to steal sensitive information or gain access to their accounts for financial fraud. The term "whaling" is used because it targets the "big fish" of an organization. Given that Sam identified the targets of the attack as high-profile executives, the described scenario is indicative of a whaling attack.
References: The CREST CPTIA curriculum includes a section on different types of phishing attacks, including whaling, emphasizing the strategies attackers use to target individuals based on their roles within an organization.

5.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
Answer: D
Explanation:
The Blueliv Threat Exchange Network is a collaborative platform designed for sharing and receiving threat intelligence among security professionals and organizations. It provides real-time information on global threats, helping participants to enhance their security posture by leveraging shared intelligence. The platform facilitates the exchange of information related to cybersecurity threats, including indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs) of threat actors, and other relevant data. This makes it an ideal choice for Kim, who is looking to gather and share threat information to develop security policies for his organization. In contrast, Cuckoo Sandbox is a malware analysis system, OmniPeek is a network analyzer, and PortDroid is a network analysis application, none of which are primarily designed for intelligence sharing.
References:
Blueliv's official documentation and resources
"Building an Intelligence-Led Security Program," by Allan Liska