Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 8-24-23	**Entry:** #1
Description	Documenting a Ransomware Incident This documentation incorporated elements of the following phases of the Incident Response Lifecycle: **Detection and Analysis**, and **Containment, Eradication, and Recovery**. The ransomware was detected after the email attachments were opened, and in order to prevent it from spreading further in the network, all the rest of the endpoints were shut down.
Tool(s) used	N/A
The 5 W's	On Tuesday, at around 9:00 A.M., an organized cybercrime group known for targeting businesses in the healthcare industry used a spear phishing campaign to gain access to a small healthcare clinic’s network. The fraudulent emails they sent contained attachments that installed malware on employees’ computers once they were downloaded. Afterwards, the employees noticed that they were unable to access important files, like patient medical records, and that the cybercriminals demanded that a large ransom be paid in order to restore access to the files.
Additional notes	Even though the appropriate measures for containment were implemented, the clinic had to rely on many other organizations to assist in returning to normal business operations.

Date: 8-26-23	**Entry:** #2
Description	Investigating a Suspicious File Hash This investigation occurred during the **Detection and Analysis** phase of the Incident Response Lifecycle. Similar to the first entry, malware was detected after clicking an email attachment, and after the incident, the file's hash value was sent to the SOC team for further analysis.
Tool(s) used	Members of the SOC team uploaded the suspicious hash to VirusTotal, an online database that analyzes files, hashes, website URLs, domains, and even IP addresses for malicious content. 82% of the security vendors confirmed that trojan horses, backdoors, and other types of malware existed in the file. According to a MITRE ATT&CK report on the VirusTotal database, the threat actor crafted the malware to evade detection and steal user input.
The 5 W's	From 1:11 P.M. to 1:15 P.M., there was an incident at a financial services company that involved a malicious file. An employee received an email from an unknown threat actor that included a downloadable file attachment. Instead of quarantining the email and reporting it to the administrative office, he proceeded to open the attached file, triggering an install of unauthorized executable files on his computer.
Additional notes	The Pyramid of Pain was used to list indicators of compromise associated with the file hash.

Date: 8-28-23	**Entry:** #3
Description	Demonstration of Suricata As part of the **Preparation** phase of the Incident Response Lifecycle, the organization conducted a three-hour demonstration of the open-source IDS Suricata and its functions.
Tool(s) used	The first part of the Suricata demo involved the examination of a custom rule file. Next, the rule was triggered to analyze a sample packet capture file and print the alert to the fast.log file. The demo concluded with the analysis of Suricata's standard log output file, eve.json, with the use of the "jq" command to process the log file's content and filter specific data.
The 5 W's	N/A
Additional notes	Suricata is not limited to simply detecting intrusions; it can also be configured to run in IPS mode to prevent certain intrusions, or it can be run in NSM mode to monitor many different types of traffic in real time.