Incident Handler's Journal

Date: Apr 23, 2024	**Entry:** #1
Description	Documenting a security incident This incident occurred in the two phases: 1. **Detection and Analysis**: The scenario explains how the organization first noticed the ransomware attack. For the analysis, the organization reached out to multiple companies for technical help. 2. **Containment, Eradication, and Recovery**: The scenario describes the measures the organization took to control the incident. They turned off their computer systems, but because they couldn't handle the cleanup and recovery by themselves, they asked other organizations for help.
Tool(s) used	None
The 5 W's	● **Who**: An organized group of unethical hackers ● **What**: A ransomware security incident ● **Where**: At a health care company ● **When**: Tuesday 9:00 a.m. ● **Why**: The incident occurred when unethical hackers accessed the company's systems through a phishing attack. Once inside, they deployed ransomware that encrypted important files. The attackers seemed to be financially motivated, as they left a ransom note demanding a large sum of money for the decryption key.
Additional notes	1. What steps can the healthcare company take to prevent a similar incident in the future? 2. Should the company pay the ransom to obtain the decryption key?

Date: July 25	**Entry:**

2024	#2
Description	Analyzing a packet file.
Tool(s) used	For this task, I utilized Wireshark to examine a packet capture file. Wireshark is a network protocol analyzer with a graphical user interface. Its value in cybersecurity lies in its ability to capture and analyze network traffic, aiding security analysts in detecting and investigating malicious activity.
The 5 W's	● **Who**: N/A ● **What**: N/A ● **Where**: N/A ● **When**: N/A ● **Why**: N/A
Additional notes	Having never used Wireshark before, I was eager to start this exercise and analyze a packet capture file. The interface initially seemed quite overwhelming, but I can understand why it’s considered such a powerful tool for understanding network traffic.

Date: July 25 2024	**Entry:** #3
Description	Capturing a packet.
Tool(s) used	For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that operates through the command line. Like Wireshark, tcpdump is valuable in cybersecurity because it enables security analysts to capture, filter, and analyze network traffic.
The 5 W's	● **Who**: N/A ● **What**: N/A ● **Where**: N/A ● **When**: N/A ● **Why**: N/A
Additional notes	I'm still learning to use the command-line interface, so capturing and filtering

	network traffic was challenging for me. I faced difficulties a few times due to incorrect command usage. However, by carefully following instructions and retrying some steps, I successfully completed the activity and managed to capture network traffic.

Date: July 27 2024	**Entry:** #4
Description	Investigate a suspicious hash
Tool(s) used	For this task, I utilized VirusTotal, an investigative tool that scans files and URLs for malicious content such as viruses, worms, and trojans. It's invaluable for quickly checking if indicators like websites or files have been flagged as malicious by the cybersecurity community. In this instance, I used VirusTotal to analyze a file hash that had been marked as malicious. This incident occurred during the Detection and Analysis phase. In this scenario, I acted as a security analyst in a Security Operations Center (SOC), tasked with investigating a suspicious file hash. After our security systems initially flagged the suspicious file, I proceeded with in-depth analysis and investigation to determine the nature and severity of the potential threat.
The 5 W's	● **Who**: An unidentified malicious actor. ● **What**: An email sent to an employee contained a malicious file attachment identified by the SHA-256 file hash 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. ● **Where**: The employee's computer at a financial services company **When**: At 1:20 p.m., an alert was sent to the organization's SOC when the intrusion detection system flagged the file ● **Why**: An employee downloaded and ran a malicious file attachment received via email.

Additional notes	What measures can be taken to prevent such incidents in the future? Should we focus on enhancing security awareness training to ensure employees exercise caution when interacting with email attachments?

Reflections/Notes:

1. **Were there any specific activities that were challenging for you? Why or why not?**

I found using tcpdump in the activity quite challenging. Since I'm still new to command-line tools, learning tcpdump's syntax was difficult for me. Initially, I felt frustrated because I wasn't achieving the expected results. However, I persevered, repeated the task, and identified my mistakes. This experience taught me the importance of carefully reading instructions and methodically working through each step.

2. **Has your understanding of incident detection and response changed after taking this course?**

Since completing this course, my comprehension of incident detection and response has significantly deepened. Initially, I had a basic grasp of these concepts but lacked awareness of their intricacies. As I advanced through the course, I gained insights into the entire incident lifecycle, the critical roles of plans, processes, and personnel, as well as the tools utilized in these procedures. Overall, I now feel more knowledgeable and equipped to handle incident detection and response effectively.

3. **Was there a specific tool or concept that you enjoyed the most? Why?**

I had a great experience exploring network traffic analysis and using network protocol analyzer tools for the first time. It was both challenging and exhilarating to delve into this new area of study. I found the ability to capture and analyze network traffic in real-time fascinating. This experience has sparked my interest to delve deeper into this topic, and I aspire to enhance my proficiency with network protocol analyzer tools in the future.