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: March 10, 2025	**Entry:** #1
Description	Documenting a ransomware attack
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An organized group of unethical hackers ● **What** happened? Due to ransomware encryption, Employees could not access medical records and other files. The attackers issued a ransom demand for the decryption key. ● **When** did the incident occur? Tuesday at approximately 9:00 a.m ● **Where** did the incident happen? A small U.S. healthcare clinic ● **Why** did the incident happen? Attackers gained access via phishing emails containing malicious attachments. The malware is executed, encrypting files and locking employees out of critical systems.
Additional notes	Should the company pay the ransom to obtain the decryption key? What steps can the healthcare company take to avoid similar attacks in the future? Recommendation: Implement more potent phishing detection tools, regular

	cybersecurity training, and backup recovery strategies.

Date: March 11, 2025	**Entry:** #2
Description	Analyze a network packet capture file
Tool(s) used	For this activity, I used Wireshark to analyze a network packet capture file and gain insights into how network traffic is structured. The goal was to apply filters, inspect packets, and understand key protocols like TCP, UDP, and ICMP.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? N/A ● **What** happened?N/A ● **When** did the incident occur?N/A ● **Where** did the incident happen?N/A ● **Why** did the incident happen?N/A
Additional notes	This was my first time using Wireshark, and I was both excited and a little overwhelmed by the interface. However, after exploring the different panes and packet details, I quickly saw how powerful this tool is for understanding network traffic.

Date: March 11, 2025	**Entry:** #3

Description	Capturing my first packet
Tool(s) used	In this lab, I acted as a network analyst to capture and analyze live network traffic using tcpdump on a Linux virtual machine. The focus was identifying active network interfaces, filtering live traffic, saving it to a .pcap file, and analyzing it using different command-line flags.
The 5 W's	**Capture the 5 W's of an incident.** ● **Who** caused the incident? N/A ● **What** happened? N/A ● **When** did the incident occur? N/A ● **Where** did the incident happen? N/A ● **Why** did the incident happen? N/A
Additional notes	This was my first time using tcpdump, and it gave me a solid understanding of how traffic flows and how to extract meaningful insights from packet captures. The ability to view packets in real-time, apply filters, and interpret packet flags and contents is essential for future incident response and network forensics.

Date: March 13, 2025	**Entry:** #4
Description	An investigation was conducted regarding a phishing alert involving a suspicious file.
Tool(s) used	For this activity, I used VirusTotal to analyze a file hash that was reported as malicious. VirusTotal is an investigative tool that analyzes files and URLs for malicious content, such as viruses, worms, trojans, etc. It's very helpful if you want to quickly check if others in the cybersecurity community have reported an indicator of compromise, like a website or file, as malicious.

The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? A threat actor behind the phishing campaign is possibly part of a known cybercriminal group. ● **What** happened? An employee received a phishing email with a malicious attachment: a SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. The employee downloaded and opened the file and created multiple unauthorized executable files on the system. An intrusion detection system detected these executables, triggering an alert to the SOC. ● **When** did the incident occur? At 1:20 p.m., IDS detected malware execution and alerted the SOC. ● **Where** did the incident happen? The incident occurred on an employee's workstation within the organization's internal network. ● **Why** did the incident happen? The phishing email bypassed security filters, and the employee unknowingly executed a malicious file. The attack was likely intended to compromise the system, install malware, or exfiltrate sensitive data.
Additional notes	How can email security be strengthened to detect similar threats? Should company policies restrict employees from opening password-protected attachments from unknown sources?

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes:

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

I found using VirusTotal challenging because analyzing hash values and interpreting results required a deeper understanding of threat intelligence. Understanding how to differentiate between false positives and confirmed threats took time, but I improved with practice.

Has your understanding of incident detection and response changed since taking this course?

Yes, my understanding has improved significantly. I now recognize the importance of layered security, the role of different tools in detecting threats, and how incident response follows a structured approach like the NIST framework. I also better understand how SOC teams investigate and escalate alerts.

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

I enjoyed working with Wireshark because it was intuitive and easy to navigate. Analyzing network traffic in real time helped me understand how packets move through a network and how to identify suspicious activity, such as malicious connections or abnormal data transfers. It provided valuable insights into network security.