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: July 23, 2024	**Entry:** #1 Cybersecurity Incident Documentation
Description	Documenting a cybersecurity incident This incident occurred in the two phases: 1. **Detection & Analysis:** The organization identified the breach and reached out to external cybersecurity teams for support in assessing the scope and origin of the ransomware attack. 2. **Containment, Eradication & Recovery:** The company took swift action by shutting down systems to contain the threat. Due to limited internal capabilities, they relied on external partners for the full remediation and recovery process.
Tool(s) used	None
The 5 W's	● **Who**: A coordinated group of malicious threat actors ● **What**: A ransomware attack compromising critical systems ● **Where**: A healthcare organization ● **When**: Tuesday at 9:00 AM ● **Why**: A phishing email was used to infiltrate the network. Once inside, attackers deployed ransomware to encrypt sensitive files. The motive appeared financial, as the attackers demanded a ransom in exchange

	for a decryption key.
Additional notes	1. What proactive security practices could prevent this in the future? 2. Should the organization ever consider paying the ransom?

Date: July 25 2024	**Entry:** #2 Packer Capture File Analysis
Description	I analyzed a packet capture (PCAP) file using Wireshark.
Tool(s) used	I used Wireshark, a GUI based network traffic analysis tool.
The 5 W's	● **Who**: N/A ● **What**: N/A ● **Where**: N/A ● **When**: N/A ● **Why**: N/A
Additional notes	This was my first time working with Wireshark. Although the interface felt overwhelming initially, I quickly began to appreciate how much insight it provides into real time network behavior.

Date: July 25 2024	**Entry:** #3 Capturing Network Traffic
Description	I captured live network traffic using tcpdump.
Tool(s) used	For this activity, I used tcpdump, a CLI based network protocol analyzer.

The 5 W's	● **Who**: N/A ● **What**: N/A ● **Where**: N/A ● **When**: N/A ● **Why**: N/A
Additional notes	As someone coming from Python and still learning command lines, this exercise challenged me. I had to redo several steps due to syntax mistakes but eventually succeeded by following directions closely. It was a great lesson in persistence and attention to detail.

Date: July 27 2024	**Entry:** #4 Investigating a Suspicious File Hash
Description	I investigated a file hash to determine whether it was associated with malicious activity. This simulation placed me in the role of a Security Operations Center analyst responding to an alert during the detection and analysis phase of an incident.
Tool(s) used	For this activity, I used VirusTotal. This is a threat intelligence platform for investigating files, URLs, and hashes This incident occurred in the Detection and Analysis phase. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat.
The 5 W's	● **Who:** Unknown threat actor ● **What:** Malicious email attachment identified by its SHA-256 hash ● **Where:** Financial services company (victim's endpoint) ● **When:** 1:20 PM – detection triggered in SOC ● **Why:** The employee opened an email and downloaded the attached file, unknowingly executing malware.

Additional notes	This underscores the importance of user training and phishing awareness. Should this company invest in enhanced cybersecurity awareness programs?

Reflections/Notes:

Using tcpdump was the hardest part. But after reattempting the exercise, I gained confidence and developed better troubleshooting skills.

I now understand that incident response is much more than identifying alerts. It's about preparation, structured response plans, using the right tools, and rapid communication. Each step from detection to recovery plays a vital role.

Network traffic analysis stood out. Using tools like Wireshark and tcpdump to inspect packets felt like uncovering invisible clues. I enjoyed the hands-on nature of these tools and want to dive deeper into network forensics.

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.