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: Jan 11, 2025	**Entry:** #1
Description	Logging a cybersecurity incident This event unfolded in two primary phases: 1. **Detection and Assessment:** The case study describes how the organization initially identified the ransomware attack. During the analysis phase, the company reached out to multiple external entities for technical support. 2. **Containment, Elimination, and Recovery:** The scenario outlines several measures taken to control the situation. One such action included shutting down the organization's computer systems. However, due to the complexity of the incident, the company sought external assistance for eradication and recovery efforts.
Tool(s) used	None
The 5 W's	• **Who:** A coordinated group of malicious hackers • **What:** A ransomware security breach • **Where:** A healthcare organization • **When:** Tuesday at 9:00 a.m. • **Why:** The breach was made possible by cybercriminals who executed a phishing attack, gaining unauthorized access to the company's network. Once inside, they deployed ransomware that encrypted critical files. Their primary motivation appeared to be financial, as they left a ransom note demanding a significant payment in exchange for the decryption key.

Additional notes	1. What preventative measures could the healthcare company implement to reduce the likelihood of a similar incident?

Date: Jan 17 2025	**Entry:** #2
Description	Examining a packet capture file
Tool(s) used	Wireshark
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I was eager to dive into the task. Initially, the interface seemed overwhelming. However, I quickly understood why it is such a valuable tool for monitoring and analyzing network traffic.

Date: Jan 24 2025	**Entry:**#3
Description	Capturing my first network packet
Tool(s) used	tcpdump
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A

	• **When**: N/A • **Why**: N/A
Additional notes	Capturing and filtering network traffic with `tcpdump` was challenging. I encountered some errors due to incorrect commands. However, after reviewing the instructions carefully and repeating some steps, I successfully completed the activity and captured network traffic.

Date: Feb 5 2025	**Entry:** #4
Description	Investigating a suspicious file hash
Tool(s) used	In this task, I used VirusTotal, an analytical tool that scans files and URLs for potential threats like viruses, worms, and trojans. This tool is particularly useful for verifying whether a given indicator of compromise such as a website or file has been flagged as malicious by the cybersecurity community. This scenario placed me in the role of a Security Operations Center (SOC) analyst investigating a suspicious file hash during the **Detection and Analysis** phase. After the organization's security tools detected a potentially harmful file, I conducted an in-depth examination to confirm whether it represented a legitimate threat.
The 5 W's	• **Who:** An unidentified cybercriminal • **What:** An email containing a harmful file attachment with the SHA-256 hash:`54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b` • **Where:** The affected computer belonged to an employee at a financial services firm • **When:** At 1:20 p.m., an alert was sent to the SOC after the intrusion detection system identified the file

	• **Why:** The employee unknowingly downloaded and executed a malicious email attachment
Additional notes	How can we prevent this type of attack in the future? Should we strengthen employee security awareness training to ensure they exercise caution when handling email attachments?

Reflections/Notes:

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

The activity involving `tcpdump` was especially challenging for me. Since I am relatively new to using command-line tools, understanding the correct syntax requires a steep learning curve. Initially, I was frustrated due to incorrect outputs. However, by carefully reviewing the instructions and proceeding methodically, I was able to resolve my mistakes and complete the task successfully.

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

Absolutely. Before starting this course, I had a basic grasp of incident detection and response. However, I did not fully appreciate the intricacies involved. As I progressed, I gained a deeper understanding of incident management workflows, the importance of structured response plans, and the tools that facilitate detection and mitigation. I now feel significantly more confident in my knowledge of incident detection and response strategies.

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

I really enjoyed exploring network traffic analysis and applying this knowledge using network protocol analyzers. I experienced these tools before but this course allowed me to go more deeper in my understanding of these tools. It was fascinating to see how these tools provide real-time insights into network activity. I am eager to continue learning and hope to become more proficient in using these tools.

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.