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 to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: April 24, 2025	**Entry: #1**
Description	Documenting a cybersecurity incident.
Tool(s) used	None.
The 5 W's	● **Who** caused the incident? **An organized group of unethical hackers**. ● **What** happened? **A ransomware security incident.** ● **When** did the incident occur? **At a health care company.** ● **Where** did the incident happen? **Tuesday 9:00 a.m.** ● **Why** did the incident happen? ● **Unethical hackers accessed the company's systems through a phishing attack and deployed ransomware, encrypting critical files. Their motive was financial, as they demanded a large ransom for the decryption key.**
Additional notes	1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key? 3. What was the vulnerability found by the unethical hackers?

Date: May 12, 2025	**Entry: #2**
Description	Analyzing an Incident Final Report.
Tool(s) used	None.
The 5 W's	• **Who** caused the incident? **An unidentified attacker exploiting a vulnerability in the e-commerce web application.** • **What** happened? **The attacker gained unauthorized access to approximately 50,000 customer records containing PII and financial data.** • **When** did the incident occur? **The incident was identified on December 28, 2022, at 7:20 p.m. PT.** • **Where** did the incident happen? I**t occurred within the organization's e-commerce web application.** • **Why** did the incident happen? **Due to a web application vulnerability that allowed forced browsing by modifying order numbers in URLs.**
Additional notes	Delayed Reporting: The initial phishing email was ignored, delaying the response and potentially increasing the impact. It's essential to strengthen employee awareness and reporting protocols for suspicious communications. Lack of Input Validation: The forced browsing vulnerability suggests insufficient input validation and poor URL access control, highlighting the need for secure coding practices. Extent of Data Exposure: While 50,000 records were confirmed compromised, further analysis should determine if additional records were accessed but not

	exfiltrated. Incident Response Improvement: Establish a more robust incident response playbook to ensure faster identification, escalation, and containment of future threats. Legal and Regulatory Review: Ensure compliance with data breach notification laws and assess the legal implications of the incident.

Date: April 30, 2025	**Entry: #3**
Description	Analyzing a packet capture file
Tool(s) used	I used Wireshark, a network protocol analyzer with a graphical interface, to analyze a packet capture file. It helps cybersecurity analysts monitor network traffic to detect and investigate malicious activity.
The 5 W's	● **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 although the interface seemed overwhelming at first, I quickly saw its value as a powerful tool for analyzing

	network traffic.

Date: May 14, 2025	**Entry:** #4
Description	Capturing my first packet
Tool(s) used	I used tcpdump, a command-line network protocol analyzer, to capture and analyze traffic. Like Wireshark, it helps security analysts filter and examine network data for cybersecurity purposes.
The 5 W's	● **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	As a beginner with the command line, I found capturing and filtering network traffic challenging at first. I made some mistakes, but by following instructions and retrying steps, I successfully completed the activity.

Date: May 16, 2025	**Entry: #5**
Description	Investigate a suspicious file hash
Tool(s) used	For this activity, I used VirusTotal to analyze a suspicious file hash, which was flagged as malicious. Acting as a SOC analyst during the Detection and Analysis phase, I investigated the alert to determine if it indicated a real threat.
The 5 W's	● **Who** caused the incident? An unknown malicious actor ● **What** happened? An employee received an email with a malicious file attachment identified by the SHA-256 hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. ● **When** did the incident occur? At 1:20 p.m., the SOC received an alert from the intrusion detection system about the detected file. ● **Where** did the incident happen? An endpoint used by staff at a financial services provider ● **Why** did the incident happen? An employee downloaded and ran a malicious email attachment.
Additional notes	To prevent this in the future, it's important to enhance security awareness training so employees are more cautious with email attachments and links.

Reflections/Notes: Record additional notes.

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

Yes, I found the activity using tcpdump quite challenging. Because I'm new to using the

command line, and learning the syntax of a tool like tcpdump was a significant learning curve.

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

Yes, it changed. I learned about many things I hadn't even seen in college. I felt closer to being a real security analyst.

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

I really enjoyed exploring network traffic analysis and using protocol analyzer tools for the first time. It was both challenging and exciting to learn how to capture and examine live network data. This experience sparked my interest in the topic, and I'm motivated to deepen my skills and become more proficient with these tools in the future.