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: 18 June, 2025	**Entry: #1**
Description	Documenting a cybersecurity incident.
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 happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	The health care company can prevent an incident like this from occurring again by training their employees, conducting phishing tasks to educate them about these kind of attack and what to do in future if this kind of situation happens again. The company should also have backup of critical and important information and data of patient’s and financial in this kind of situation when a ransomware or any other attacks occur to safeguard critical operations of the company.

Date: 20 June, 2025	**Entry: #2**
Description	Analyzing a packet capture file
Tool(s) used	I used Wireshark to analyze a packet capture file. Wireshark is an open-source network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help 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	I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic. It is design to help find patterns and filter the data in order to focus on the network traffic that is most relevant to security investigations.

Date: 23 June, 2025	**Entry: #3**
Description	Investigate a suspicious file hash
Tool(s) used	I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the

	cybersecurity community. To investigate the suspicious files hash I used VirusTotal to analyze it, and which was reported as malicious.
The 5 W's	• **Who**: An unknown malicious actor • **What**: An email was sent to an employee containing a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **Where**: An employee's computer at a financial services company • **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file • **Why**: The employee downloaded the attachment file via Email out of curiosity and opened the file and it executed a malicious payload on the computer.
Additional notes	How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on? 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 or false alert.

Date: 25 June, 2025	**Entry: #4**
Description	Capturing my first packet
Tool(s) used	I used tcpdump to capture and analyze network traffic. Tcpdump is a Open-Source network protocol analyzer that's accessed using the Linux based command-line interface. Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows 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 new to using the command-line interface, so using it to capture and filter network traffic was a big challenge and understanding what is happening during the network traffic was overwhelming. But after carefully following the instructions and redoing some steps, I was able to understand this activity and captured network traffic.

Reflections/Notes: Record additional notes.

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

I really found the activity using tcpdump challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated because I wasn't getting the right output. I redid the activity and figured out where I went wrong. What I learned from this was to carefully read the instructions and work through the process slowly.

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

After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used.