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: April 15, 2025	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None
The 5 W's	• **Who:** An unethical group of hackers. • **What:** Employees opened a phishing email which had an attachment that allowed the encryption of company data. • **Where**: A health care clinic in the U.S • **When:** Tuesday 9:00 a.m. • **Why:** A phishing email that had a malicious attachment added to it was opened by employees which allowed the attacker to encrypt the organization's computer files. A note was left by the organized group of unethical hackers demanding money in return for the data decryption key.
Additional notes	1. How much of the company data was lost? 2. How many systems received the phishing email?

Date: April 17, 2025	**Entry:** #2
Description	Analyzing a packet capture file

Tool(s) used	In this activity I used the packet analyzer “Wireshark” to analyze a packet capture file. Wireshark allows for the capture of packets over a network using a graphical user interface or GUI, and allows the user to analyze network traffic. Wireshark is used for the detection of malicious activity over networks via packet capture file.
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 using wireshark so a lot of the exercises were new to me. At first glance there was a lot to take in on the graphical user interface but as I used it more I began to understand why it is used so much in cybersecurity.

Date: April 19, 2025	**Entry:** #3
Description	Capturing a packet
Tool(s) used	Tcpdump was used in this activity which allowed me to capture and analyze network traffic. Tcp dump uses a command-line interface rather than a GUI to capture 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	This was also one of my first times uses tcpdump and a command-line interface. Once you remember the commands it gets pretty simple to use. The issue for me was that there were a lot of commands to remember.steps, I was able to get through this activity and capture network traffic.

Date: April 21, 2025	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	In this activity I used a tool that analyzes files and URLs called “VirusTotal”. This tool will tell you if malicious content is detected and is a quick and efficient way to see if a website or file has been compromised. In this specific activity I analyzed a file hash which came back as malicious using VirusTotal.
The 5 W's	• **Who**: Unknown • **What**: An email was sent to an employee wich contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **Where**: a financial services company in the U.S • **When**: 1:20 p.m • **Why**: An email with a malicious attachment was sent to an employee who downloaded and executed the malicious file.
Additional notes	What security steps can be taken to prevent issues like this down the road?

Reflections/Notes:

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

The tcpdump activity was probably the most problematic for me just because it is a command line interface so having to remember all the commands takes time.

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

After completing this course I know I have learned so much more about incident detection and response. My ability to detect and respond to incidents now compared to what it was before I took this course is unrecognizable. I am much more confident and educated about malicious threats and how to handle them than before I took this course.

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

My favorite concept was learning about packet analysis tools and how to use them. There was an activity where a threat actor was flooding a network with SYN packets and I got to go in and see each individual packet with time stamps and IP addresses and figure out how to resolve this issue. I personally think dealing with threat actors and malicious activity feels similar to playing a game of chess, the threat actor makes his move and I have to respond so it makes it fun and challenging.
