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: June 1, 2025	**Entry:** #1
Description	A ransomware attack that was executed through phishing.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who?** An organized group of unethical hackers • **What?** A ransomware attack • **When?** Tuesday at 9:00 a.m. • **Where?** A small US healthcare company. • **Why?** The employees of the company accidentally clicked on the phishing email's link which downloaded a malicious attachment into the computer. The download encrypted all the files within the computer systems of the company. There are several reasons for why this incident occurred. The motive for the hackers seems to be financial because they demand money in exchange for data. So, to answer the why question, it would be money.
Additional notes	After recovering data, training employees on how to identify phishing emails and other social engineering tactics should become the company's main focus.

	This incident might have been avoided if phishing exercises or social engineering training modules had been implemented.

Date: June 02, 2025	**Entry:** #2
Description	An employee clicked on a malicious file sent via email. The downloaded file created multiple unauthorized files on the computer containing malicious content.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who?** Malicious actor • **What?** An employee received an email containing an attachment. Once the file was downloaded, it led to multiple malicious files being downloaded. • **When?** Employee receives email at 1:11 p.m. and IDS detects the executable file at 1:20 p.m. • **Where?** Financial services company • **Why?** There might be various reasons for this attack. The attackers might want to steal the company's data, such as customers card information or PII, and sell it on the dark web. They may encrypt the data and ask for a ransom, or their motive could have been to hinder operations at the company.

Additional notes	I believe that teaching employees about phishing and social engineering tactics can help prevent these attacks from being successful.

Date: June 02, 2025	**Entry: #3**
Description	A ransomware attack occurred due to a vulnerability in the web application. This vulnerability was exploited to gain access to sensitive customer data.
Tool(s) used	Pen testing
The 5 W's	Capture the 5 W's of an incident. • **Who?** A malicious threat actor • **What?** An employee received a ransom email demanding an amount of $ 25,000 for stolen customer data, which was initially ignored. A follow up email with a data sample and higher demand escalated the situation into investigation. This breach led to 50,000 exposed customer records. • **When?** December 28 , 2022 at 7:20 P.T. • **Where?** An e-commerce company • **Why?** There was a vulnerability in the e-commerce web application which made it easier for the attacker to compromise the data. The motive seems to be financial because the attacker wants money in exchange for data confidentiality.
Additional notes	Conducting vulnerability assessments regularly and performing penetration testing would help improve the company's security posture and reduce

	vulnerabilities that could be exploited. Employees should also undergo training to identify threats and phishing emails, so alerts regarding ransomware aren't ignored.

Date: June 02, 2025	**Entry: #4**
Description	Capturing my first packet
Tool(s) used	I used tcpdump to capture my first data packet. Tcpdump is a network protocol analyzer that uses a command line to interact with users. I analyzed network traffic and learned about the basics of data packets. Tcpdump is similar to Wireshark, as both of them are network analyzer tools, but Wireshark uses a graphical user interface to interact with the user.
The 5 W's	Capture the 5 W's of an incident. • **Who?** N/A • **What?** N/A • **Where?** N/A • **Why?** N/A
Additional notes	Although I have previously worked with Bash commands, capturing and analyzing a data packet using tcpdump was a challenge. This is because there were a couple of new commands to capture the data packet. I struggled to understand the commands and the filters, as they were new to me, but eventually, I learned how to work with tcpdump.

Date: June 02, 2025	**Entry: #5**
Description	Analyzing a packet capture file using Wireshark.
Tool(s) used	I used Wireshark to analyze a packet capture file. Wireshark is a popular network-analyzing tool for capturing data packets. It uses a graphical user interface. Wireshark is a very useful tool for security analysts, as it helps detect and investigate malicious network packets.
The 5 W's	Capture the 5 W's of an incident. • **Who?** N/A • **What?** N/A • **Where?** N/A • **Why?** N/A
Additional notes	Although Wireshark uses a graphical user interface, I found it a bit overwhelming to work with. There were so many components to Wireshark, and it confused me. I felt like tcpdump gave more specific and relevant information about the packets than Wireshark.

Reflection/notes

All of the activities taught me new things about networks, incident detection, recovery strategies, documentation, and logging tools. One of my favorite activities was querying using Splunk. It taught me how to apply filters and use the Splunk query language to retrieve data. Other activities, such as capturing data packets, were new and interesting.