Incident handler's journal

By: cammi.sec

Date: July 7, 2025	**Entry: 001**
Description	A small U.S. health care clinic received a ransomware attack on Tuesday at approximately 9am, where they had all the company's files encrypted by an organized group of unethical hackers, asking for a large amount of money to provide the decryption key. Business operations shut down because employees were unable to access the files and software needed to do their job.
Tool(s) used	n/a
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An organized group of unethical hackers • **What** happened? Phishing emails were sent to several employees with a malicous attachment. After gaining access, the group encrypted all the company's files. • **When** did the incident occur? On Tuesday morning, around 9am. • **Where** did the incident happen? At a small health care clinic in the U.S. • **Why** did the incident happen? The cause of the security incident was a phishing email that contained a malicious attachment. It happened due to lack of employee experience in recognizing malicious and fake emails. Also, if an IDS was implemented, it could have been avoided.
Additional notes	To avoid future breaches, it's important to provide proper cybersecurity training for all employees, and implement tools to help identify and block suspicious emails.

Date: July 10, 2025	**Entry: 002**
Description	Analyzing a packet capture file.
Tool(s) used	Wireshark was used to analyze a packet capture file. Wireshark is a 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	Capture the 5 W's of an incident. • 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, the interface was very overwhelming with so many details and information. I can see why it's such a powerful tool for understanding network traffic, but it will take some practice to get comfortable with it.

Date: July 12, 2025	**Entry: 003**
Description	Capturing my first packet
Tool(s) used	For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the 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	Capture the 5 W's of an incident. • Who: N/A • What: N/A • Where: N/A • When: N/A • Why: N/A
Additional notes	I'm still learning to use the command-line interface, so using it to capture and filter network traffic was challenging. I got confused a couple of times because I used the wrong commands. But after carefully following the instructions and trying again, I was able to complete this activity and capture network traffic successfully.

Date: July 15, 2025	**Entry: 004**
Description	Investigate a suspicious file hash
Tool(s) used	or this activity, 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 a file or website has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash that was reported as malicious.
The 5 W's	Capture the 5 W's of an incident. • **Who:** An unknown malicious actor • **What:** An email sent to an employee contained a malicious file attachment with the SHA-256 file hash • **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:** An employee was able to download and execute a malicious file attachment through email.
Additional notes	This was interesting because it shows how important it is to have detection systems in place. How can this incident be prevented in the future? We should consider improving security awareness training so that employees are more careful with email attachments.

Reflections/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 commands for tcpdump was difficult for me. At first, I felt frustrated because I wasn't getting the right results. I had to redo some steps and figure out where I went wrong. What I learned from this was to read the instructions carefully 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 improved. At the beginning, I had some basic understanding of what detection and response meant, but I didn't fully understand how complex it actually is. As I progressed through the course, I learned about the incident lifecycle, the importance of proper documentation, and the different tools we use. Overall, I feel that my understanding has grown, and I have more knowledge about incident detection and response.

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

I really enjoyed learning about network traffic analysis and using the network protocol analyzer tools. It was my first time learning about network traffic analysis, so it was both challenging and exciting. I found it fascinating to be able to capture network traffic and analyze it. I am definitely interested in learning more about this topic, and I hope to become better at using these tools in the future.