Incident handler's journal

Date: December 27th, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident This incident occurred in two phases: 1. **Detection and Analysis**: The scenario outlines how the organization first detected the ransomware incident. For the analysis step, the organization contacted several organizations for technical assistance. 2. **Containment, Eradication, and Recovery**: The scenario details some steps the organization took to contain the incident. For example, the company shut down its computer systems. However, since they could not work to eradicate and recover from the incident alone, they contacted several other organizations for assistance.
Tool(s) used	None
The 5 W's	• **Who**: An organized group of unethical hackers • **What**: A ransomware security incident • **Where**: At a healthcare 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	1. How could the healthcare company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key?

Date: December 28th, 2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark 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 detect and investigate 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.

Date: December 28th, 2024	**Entry:** #3
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	• **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 challenge. I got stuck a couple of times because I used the wrong commands. However after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic.

Date: December 29th, 2024	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	For 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 an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious. This incident occurred in the **Detection and Analysis** phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. 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.
The 5 W's	• **Who**: An unknown malicious actor • **What**: An email sent to an employee contained 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**: An employee was able to download and execute a malicious file attachment via e-mail.

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?

Reflections/Notes:

Were there any specific activities that were challenging for you? Why or why not?
I found working with **tcpdump** particularly challenging. Since I'm new to the command line, understanding the syntax for a tool like **tcpdump** was a steep learning curve. Initially, I felt frustrated because I wasn't getting the expected output. However, after retrying the activity and carefully reviewing my mistakes, I was able to figure out what went wrong. This experience taught me the importance of thoroughly reading instructions and approaching tasks methodically.

Has your understanding of incident detection and response changed after taking this course?
Yes, my understanding of **incident detection and response** has significantly deepened throughout this course. At the start, I had a basic idea of what detection and response involved, but I didn't fully grasp the complexity of the process. As I progressed, I gained insight into the **incident lifecycle**, the critical role of **plans, processes, and personnel**, and the tools used in incident response. Overall, I now have a much clearer and more comprehensive understanding of the field.

Was there a specific tool or concept that you enjoyed the most? Why?
I particularly enjoyed learning about **network traffic analysis** and using **network protocol analyzer tools**. Since this was my first exposure to analyzing network traffic, I found it both challenging and exciting. The ability to capture and examine network data in real-time was fascinating, and it sparked my interest in further exploring this area. I hope to continue developing my skills and become more proficient with these tools in the future.