Incident handler's journal

Date: September 19 ,2023	**Entry: #1**
Description	Documenting a cybersecurity incident This incident occurred in the 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 that the organization took to contain the incident. For example, the company shut down their 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 ● **When:** Tuesday 9:00 a.m. ● **Where:** At a health care company ● **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 health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key?

Date: September 20 ,2023	**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 in detecting and investigating malicious activity.
The 5 W's	● **Who:** N/A ● **What:** N/A ● **When**: N/A ● **Where**: 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: September 22 ,2023	**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 ● **When**: N/A ● **Where**: 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. But after carefully following the instructions and redoing some steps, I was able to get through this activity and capture network traffic.

Date: September 24 ,2023	**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 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93b527f6b ● **When:** At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file ● **Where:** An employee's computer at a financial services company ● **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:

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. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response.