Incident handler's journal

Date: July 23, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident The incident occurred in two separate stages: ● **Detection and Analysis**: The organization initially identified the ransomware incident and requested technical assistance from various external organizations for analysis. ● **Containment, Eradication, and Recovery**: The organization took immediate action to contain the incident, including deactivating their computer systems. Recognizing the need for external expertise, they collaborated with multiple organizations to eliminate the ransomware and restore their systems.
Tool(s) used	None
The 5 W's	● **Who**: An organized group of unethical hackers ● **What**: A ransomware security incident ● **Where**: At a health care 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. What preventative measures can the healthcare company implement to mitigate the risk of similar incidents occurring in the future? 2. Should the company remit payment of the ransom in order to obtain the decryption key?

Date: July 25 2024	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	In this exercise, I employed Wireshark, a network protocol analyzer equipped with a graphical user interface, to examine a packet capture file. Wireshark is an invaluable tool in cybersecurity because it allows security analysts to capture and analyze network traffic, which can assist in the detection and investigation of malicious activity.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I was keen to commence this exercise and examine a packet capture file, as I had no prior experience utilizing Wireshark. The interface was initially daunting; however, I now comprehend why it is considered such a potent tool for network traffic analysis.

Date: July 25 2024	**Entry:** #3
Description	Capturing my first packet
Tool(s) used	In this exercise, I utilized the command-line network protocol analyzer tcpdump to capture and analyze network traffic. Tcpdump, which has similar capabilities to Wireshark, is a valuable tool for cybersecurity professionals because it allows them 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	Capturing and filtering network traffic using the command-line interface presented challenges due to my limited experience. Incorrect commands resulted in minor setbacks; however, by carefully adhering to the instructions and revisiting certain steps, I successfully completed the activity and captured the network traffic.

Date: July 27 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:

The unfamiliarity with the command line presented a significant challenge during the tcpdump activity. Learning the syntax for tcpdump presented a steep learning curve, and the initial frustration with incorrect outputs necessitated repeating the activity. This experience highlighted the importance of carefully reading and methodically working through instructions.

My knowledge of incident detection and response has grown substantially as a result of this course. While I possessed a foundational understanding of the subject at the outset, I lacked a comprehensive appreciation of its intricacies. Throughout the course, I acquired valuable insights into the incident lifecycle, the critical role of plans, processes, and personnel, and the tools utilized in incident response. Overall, I believe that my knowledge and comprehension of incident detection and response have increased significantly, and I am now better prepared to manage such incidents.

Learning about network traffic analysis and using network protocol analyzer tools was challenging, yet exciting. The ability to capture and analyze network traffic in real time was fascinating and sparked my interest in further exploration of this area. I aim to enhance my proficiency in using these tools in the future.
