Incident Handler's Journal

Date: Dec 07, 2023	**Entry:** #1
Description	Documenting a cybersecurity incident
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. Subsequently, they initiated ransomware on the systems, encrypting vital files. The attackers seem driven by financial motives, evident in the ransom note they issued, demanding a substantial amount in exchange for the decryption key.
Additional notes	Implement robust cybersecurity measures such as encryption, multi-factor authentication, regular system updates, and intrusion detection systems to safeguard sensitive patient data. Legal implications and ethical concerns associated with paying a ransom should be considered. Some jurisdictions prohibit ransom payments to cyber criminals. Consult with law enforcement and cybersecurity professionals to explore options and understand potential risks before making a decision.

Date: Dec 07, 2023	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	In this activity, I employed Wireshark to analyze a packet capture file. Wireshark, a network protocol analyzer featuring a graphical user interface, holds significant value in cybersecurity. It empowers security analysts to capture and scrutinize network traffic, aiding in the detection and investigation of malicious activities.

Incident Handler's Journal

The 5 W's	● **Who**: N/A ● **What**: N/A ● **Where**: N/A ● **When**: N/A ● **Why**: N/A
Additional notes	Having never utilized Wireshark previously, I was enthusiastic to embark on this exercise and delve into the analysis of a packet capture file. Initially, the interface appeared quite overwhelming. However, I quickly recognized its power as a tool for comprehending network traffic, which explains its reputation as a powerful asset.

Date: Dec 07, 2023	**Entry:** #3
Description	Capturing my first packet
Tool(s) used	In this activity, I utilized tcpdump to capture and analyze network traffic. Tcpdump operates as a network protocol analyzer accessible via the command-line interface. Much like Wireshark, tcpdump holds significance in cybersecurity by enabling security analysts to capture, filter, and meticulously analyze network traffic.
The 5 W's	● **Who: N/A** ● **What: N/A** ● **Where: N/A** ● **When: N/A** ● **Why: N/A**
Additional notes	Utilizing the command-line interface for capturing and filtering network traffic can present a challenge. Nevertheless, by dedicating more practice time, meticulously following the instructions, and revisiting certain steps, I successfully navigated through this activity and managed to capture the network traffic.

Date: Dec 07, 2023	**Entry:** #4
Description	Investigate a suspicious file hash

Incident Handler's Journal

Tool(s) used	In this activity, I employed VirusTotal, an investigative tool designed to scrutinize files and URLs for various forms of malicious content, including viruses, worms, trojans, and other threats. It proves highly beneficial when one needs to swiftly verify whether an indicator of compromise, such as a website or file, has been flagged as malicious by the wider cybersecurity community. In this instance, I utilized VirusTotal to analyze a file hash, which was flagged as malicious. This incident took place during the Detection and Analysis phase. The situation positioned me in the role of a security analyst at a Security Operations Center (SOC) tasked with investigating a suspicious file hash. Following the detection of the suspicious file by the existing security systems, I was required to conduct a comprehensive analysis and investigation to ascertain whether the alert indicated an actual 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	Implement robust endpoint security solutions that can detect and mitigate suspicious file hashes or any potentially harmful activities on the network. Establish clear incident response protocols and encourage employees to promptly report any suspicious activity or files to the security team. This fosters a proactive approach to incident handling and helps in mitigating potential threats swiftly.

Reflections/Notes:

Upon completing this course, my comprehension of incident detection and response has significantly advanced. Initially, I possessed a rudimentary understanding of what these concepts encompassed, yet I was unaware of their intricate complexities. As the course unfolded, I delved into the comprehensive lifecycle of an incident, grasped the pivotal significance of well-defined plans, processes, and human involvement, and familiarized myself with the array of tools employed in this domain. Overall, I am pleased to acknowledge that my perspective has undergone a substantial transformation, leaving me better equipped with profound knowledge and insight into incident detection and response.

Incident Handler's Journal

I thoroughly enjoyed delving into network traffic analysis and putting my knowledge into practice using network protocol analyzer tools. This was my initial exposure to network traffic analysis, presenting both challenges and thrills. The process of capturing and analyzing network traffic in real-time using specialized tools fascinated me. I am keenly interested in further exploring this subject and aspire to enhance my proficiency in utilizing network protocol analyzer tools in the future.