Incident handler's journal

Date: Dec 21, 2024	**Entry: #1**
Description	Documenting a cybersecurity incident involving ransomware at a healthcare company, which led to encrypted files and a ransom demand.
Tool(s) used	None.
The 5 W's	• **Who**: An organized group of unethical hackers • **What**: A ransomware security incident • **When**: Tuesday at approximately 9:00 a.m. • **Where**: At a healthcare company • **Why**: The incident occurred due to a successful phishing attack that led to ransomware deployment.
Additional notes	• Train employees in phishing awareness • Implement advanced email and traffic filtering • Enforce data access restrictions • Regularly update and patch systems • Maintain offsite backups • Develop a quick-response incident plan • Deploy antivirus and anti-malware with Ransome detection • Consult for non-payment recovery options

Date: Dec 25, 2024	**Entry: #2**
Description	Analyzing a packet capture file
Tool(s) used	In this exercise, I used Wireshark, which is renowned for its ability to dissect and analyze network traffic through a graphical interface. Its role in cybersecurity is pivotal, offering insights into network communication that are crucial for identifying suspicious activities.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: N/A ● **What**: N/A ● **When**: N/A ● **Where**: N/A ● **Why**: N/A
Additional notes	As someone who has previously engaged with Wireshark, This exercise was an opportunity to further improve my skills in network analysis.

Date: Dec 27, 2024	**Entry: #3**
Description	Capturing a Packet
Tool(s) used	This time, I used something called tcpdump to catch and look at what's happening in network traffic. Tcpdump is a tool that you use through typing commands instead of clicking around. It's a bit like Wireshark because it helps people who work with computer security to grab, sort, and check out network traffic.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: N/A ● **What**: N/A ● **When**: N/A ● **Where**: N/A ● **Why**: N/A
Additional notes	I'm not totally new to using command lines, thanks to some experience with Linux, so that background helped me get started with tcpdump. Even so, figuring out the right commands to capture and sort the network traffic was a bit tricky at first. It felt good to use what I knew about Linux commands here, and it definitely made the learning curve a little easier to climb.

Date: Dec 29, 2024	**Entry: #4**
Description	Analyzing a Malicious File Hash
Tool(s) used	For this task, I used VirusTotal, a comprehensive tool for analyzing files and URLs to identify malicious content such as viruses, worms, trojans, and more. It serves as an efficient resource for confirming whether a specific indicator of compromise, such as a file or website, has been recognized as malicious within the cybersecurity community. My usage involved analyzing a file hash reported as malicious. This inquiry took place during the Detection and Analysis phase, positioning me as a security analyst within a SOC tasked with investigating a suspicious file hash. Following the detection of the file by our security systems, a deeper investigation was required to ascertain the legitimacy of the threat.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: An unidentified malicious entity ● **What**: A malicious file attachment in an email, identified by its SHA-256 hash ● **When**: Alert dispatched to the organization's SOC at 1:20 p.m. following detection by the intrusion detection system. ● **Where**: On an employee's workstation within a financial services corporation ● **Why**: Execution of a malicious file attachment from an email by an employee.
Additional notes	This incident highlighted the sophistication of phishing attacks and the importance of vigilance at every level of an organization. For avoiding this kind of trouble in the future, maybe we should boost our security training? Making sure everyone knows to be careful about what they click could help a lot.