Incident handler's journal

Date: 22nd November 2024	**Entry:** #1
Description	A cybersecurity Incident
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who** : An organized group of unethical hackers. ● **What** : A ransomware incident. ● **When** : Tuesday morning at approximately 09:00 AM. ● **Where** : At a health care company. ● **Why** : Attackers sent the targeted phishing email to several employees of the company which contained the malicious attachment which installed the malware on the employee's computer once it was downloaded. Once the attackers gained access, they deployed their ransomware which encrypted 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: 22nd November 2024	**Entry:** #2
Description	For this activity, I used wireshark to analyze a packet capture file.i.e sample.pcap. Wireshark is a network protocol analyzer tool as well as network packet sniffer that allows security analysts to capture and analyze the network traffic. Applied filters to extract what's necessary for detecting and investigating malicious activity.
Tool(s) used	Wireshark
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 have used Wireshark before but i wasn't aware about all the filter and how better we can use it to find the information.

Date: 22nd November 2024	**Entry:** #3
Description	Capturing network packets.
Tool(s) used	tcpdump

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	Tcpdump, like Wireshark, is both a **network protocol analyzer** and a **network packet sniffer**. However, unlike Wireshark, it operates exclusively via the command-line interface, making it less intuitive for users unfamiliar with command-line syntax. While it is powerful and lightweight, its lack of a graphical user interface (GUI) can make it more challenging to use compared to Wireshark's visually intuitive layout.

Date: Record the date of the journal entry.	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	VirusTotal is a powerful tool used to analyze files and URLs for malicious content, including viruses, worms, trojans, and other threats. By leveraging contributions from security vendors and the wider cybersecurity community, it performs comprehensive checks for malicious activity. Additionally, VirusTotal employs sandboxing technology to detect hidden traces of malicious behavior in a controlled environment. This incident occurred during the **Detection and Analysis** phase. In this

	scenario, I stepped into the role of a **Security Analyst** at a SOC (Security Operations Center), tasked with investigating a suspicious file hash flagged by the security systems in place. After identifying the suspicious file, I conducted a detailed analysis and investigation to determine whether the alert indicated a genuine threat. The process involved correlating data, validating findings, and utilizing tools like VirusTotal to ensure accurate threat assessment.
The 5 W's	Capture the 5 W's of an incident. ● **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 ● **When** : At 01:20 PM an alert was sent to an organization's SOC after the intrusion detection system detected the file. ● **Where** : An employee's computer at a financial services company. ● **Why** : Employee downloaded and executed a malicious file attached to the phishing email sent by the hacker.
Additional notes	How can this incident be prevented in future? Doing more security awareness training so that employees can be more careful with what they click on.

Reflections/Notes: Record additional notes.