Incident handler's journal

Date: 17-10-2024	**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 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. 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: 19-10-2024	**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	• NA
Additional notes	I was eager to start using Wireshark for the first time and analyze a packet capture file. However, the interface felt quite overwhelming at first. I now understand why it's such a powerful tool for analyzing network traffic.

Date: 21-10-2024	**Entry: #3**
Description	Capturing a packet.
Tool(s) used	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	• NA
Additional notes	As I'm still getting familiar with the command-line interface, capturing and filtering network traffic posed a challenge for me. I encountered a few hurdles due to using incorrect commands. However, after meticulously following the instructions and redoing some steps, I managed to successfully complete this activity and capture the network traffic.
