Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 02/09//2025	**Entry:** Capture your first packet
Description	Performing tasks associated with using tcpdump to capture network traffic. Capture the data in a packet capture (p-cap) file and then examine the contents of the captured packet data to focus on specific types of traffic.
Tool(s) used	Google Chrome Linux
The 5 W's	- **Who**: network analyst - myself - **What**: needs to use tcpdump to capture and analyze live network traffic from a Linux virtual machine. - **Where**:Linux - **When:** Timestamp of tcp outputs - **Why:** identify network interfaces, use the tcpdump command to capture network data for inspection, interpret the information that tcpdump outputs regarding a packet, and save and load packet data for later analysis.

Additional notes	