Date: **2/09/2025**	**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.
Tools Used	Google Chrome Linux-Linux is a free, open-source operating system (OS) used for computers, servers, and other devices. It's a key part of modern computing, powering many industries.
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. A network analyst uses tcpdump on a Linux VM to capture and analyze live network traffic, saving packet data for further inspection and interpretation
Additional Notes	The task of capturing and analyzing network traffic using tcpdump falls under the Detection & Analysis phase of the NIST Incident Response Lifecycle. This phase involves identifying, analyzing, and understanding potential security incidents. By capturing and inspecting network traffic, you can detect anomalies or malicious activity, which helps in understanding the nature and scope of the threat