



# Cybersecurity Lab Journal – Entry #2

## Lab Description:

In this lab, I used tcpdump in Linux to capture and look at network traffic. I learned how to find the right network interface, capture packets, and filter them to focus on certain types of traffic. I also practiced saving the capture and checking packet details.

<b>Date:</b> Record the date of the journal entry.	<b>Entry:</b> #2 <b>Date:</b> October 6, 2025
Description	I used tcpdump commands to capture and inspect packets in real time. I filtered for port 80 traffic and saved it to a .pcap file for later review.
Tool(s) used	tcpdump
Key Findings / Skills Practiced:	<b>Key Findings / Skills Practiced:</b> <ul style="list-style-type: none"><li>• Used ifconfig and tcpdump -D to find network interfaces.</li><li>• Captured packets from eth0 with sudo tcpdump -i eth0 -v -c5.</li><li>• Filtered HTTP packets using port 80.</li><li>• Saved captured data to a file and reviewed it using <code>-nn</code> and <code>-X</code> flags.</li></ul>
Additional notes	The lab was straightforward. It helped me get used to capturing and reading network traffic directly from the terminal

