Tcpdump Network Traffic Analysis Lab – Portfolio Overview

Objective

The objective of this lab was to gain hands-on experience using tcpdump to identify network interfaces, capture live packet data, and analyze network traffic. The exercise demonstrates core network analysis and forensic skills used by cybersecurity professionals to inspect and filter packets at the command-line level.

Tools & Environment

• Tool Used: tcpdump
• Operating System: Linux
• Key Commands: ifconfig, tcpdump, curl
• File Type: .pcap (packet capture file)
• Protocols Observed: TCP, IP, Ethernet

Key Learning Outcomes

1. Identified available network interfaces using ifconfig and tcpdump -D.
2. Captured live network traffic from the eth0 interface with tcpdump using flags such as -v (verbose) and -c (capture count).
3. Analyzed captured traffic to interpret IP, TCP, and Ethernet properties including TOS, TTL, flags, and checksums.
4. Captured HTTP (TCP port 80) traffic into a pcap file for inspection and analysis.
5. Applied tcpdump filters (-r, -nn, -X) to examine packet header data and raw hexadecimal payloads.

Technical Highlights

• Used **sudo ifconfig** and **sudo tcpdump -D** to identify available network interfaces.
• Captured five packets of live data using **sudo tcpdump -i eth0 -v -c5**.
• Generated web traffic with **curl opensource.google.com** to capture HTTP packets.
• Saved packet captures using **sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap**.
• Filtered and viewed saved data using **sudo tcpdump -nn -r capture.pcap -v** and **-X** for hexadecimal/ASCII output.

Cybersecurity Relevance

This lab reinforced practical network forensics and packet inspection skills crucial for incident response and threat analysis. tcpdump is a powerful command-line tool for capturing and inspecting live network data. Understanding how to collect, filter, and interpret this information helps analysts detect suspicious activity, verify configurations, and perform root cause

analysis.

Key Takeaway

By completing this lab, I strengthened my foundational skills in network traffic analysis, interface identification, and command-line packet capture using tcpdump. These skills are essential for security analysts, penetration testers, and network defenders responsible for monitoring and investigating network activity.

Commands Used in This Lab

```
sudo ifconfig
    → Displays all available network interfaces on the system.

sudo tcpdump -D
    → Lists all network interfaces available for packet capture.

sudo tcpdump -i eth0 -v -c5
    → Captures 5 packets from the eth0 interface with verbose output.

sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &
    → Captures 9 HTTP (port 80) packets from eth0 and saves them to a capture file in

curl opensource.google.com
    → Generates HTTP traffic for packet capture.

ls -l capture.pcap
    → Verifies the presence and details of the captured file.

sudo tcpdump -nn -r capture.pcap -v
    → Reads and displays packet header data from a saved capture file with verbose de

sudo tcpdump -nn -r capture.pcap -X
    → Displays packet data in both hexadecimal and ASCII formats for deeper forensic
```