TCPDump Basics - Cheat Sheet & Guide

TCPDump is a powerful command-line packet analyzer tool that allows you to capture or filter network traffic. It is commonly used by network administrators, security analysts, and penetration testers to inspect and troubleshoot network issues.

What is TCPDump?

TCPDump captures packets from a network interface and displays details such as source/destination IPs, ports, and protocol flags. Unlike Wireshark's GUI, TCPDump is lightweight and text-based, ideal for remote servers or quick captures.

Using TCPDump Without Root Access

By default, TCPDump requires root privileges to capture live traffic. Without root, you can still work with pre-captured `.pcap` files using the `-r` option. Example:

tcpdump -r traffic.pcap

Basic Syntax

tcpdump [options] [expression]

Examples:

- tcpdump -i eth0 → Capture packets on interface eth0
- tcpdump -c 10 → Capture only 10 packets
- tcpdump -n → Do not resolve hostnames (faster, clearer)
- tcpdump -nn → Do not resolve hostnames or ports
- tcpdump -v / -vv → Increase verbosity
- tcpdump -w file.pcap → Save captured packets to file for later analysis

Filters

Filters allow focusing on specific traffic of interest.

- tcpdump arp → Show ARP packets
- tcpdump icmp → Show ICMP packets (pings)
- tcpdump port 80 → Capture traffic on port 80 (HTTP)
- tcpdump src 192.168.1.1 → Show packets from source IP
- tcpdump dst 192.168.1.10 → Show packets to destination IP
- tcpdump host 192.168.1.5 → Show packets to/from a host
- tcpdump portrange 20-23 → Show traffic on port range 20–23
- tcpdump tcp[tcpflags] & tcp-rst != 0 → Show TCP packets with RST flag set
- tcpdump greater 1500 → Packets larger than 1500 bytes

Real-World Use Cases

- Detect DNS queries: tcpdump port 53
- Capture HTTP traffic: tcpdump port 80
- Decrypt HTTPS traffic with SSL keys: tcpdump -r file.pcap (then load ssl-key.log in Wireshark)
- Find suspicious connections: tcpdump dst port 22 and not src net 192.168.1.0/24
- Check ARP requests: tcpdump arp

Tips & Best Practices

- Always use filters to avoid overwhelming output.
- Combine tcpdump with Wireshark for deep analysis.
- Non-root users can analyze existing `.pcap` files.
- Use -w to save long captures for later review.
- Remember: tcpdump is powerful but raw, requires analyst interpretation.