IPv4 and ARP - Command Cheat Sheet

tcpdump

Command Options:

Flag	Description
-nn	No hostname or port resolution
-i	Specify interface for live capture
-w	Write output to file
-e	Print out MAC addresses
-c	Specify the number of packets to read
-v	Verbose output

Syntax:

- `tcpdump [OPTIONS] [BPF Filter]`

Capture traffic on an interface and write output to PCAP file:

- `sudo tcpdump -nn -i docker0 -w ~/analysis1.pcap`

Read a PCAP file and list packets with MAC address:

- `tcpdump -nn -r ~/combined-analysis.pcap -e | less -S`

Show all MAC addresses with their corresponding IP address:

- `tcpdump -nn -r ~/combined-analysis.pcap -e 'tcp port 8000' | cut -f 2,10 -d " " | cut -f 1-4 -d "." | sort | uniq -c | sort -n`

Print TTL values:

- `tcpdump -nn -r ~/mitm.pcap 'src host 119.85.45.179' -v | grep "ttl"`

mergecap

Combine two PCAP files:
`mergecap -w combined-analysis.pcap analysis1.pcap analysis2.pcap`

Linux Reference

Show interface information (including MAC address):

- `ip link show`

Manually turn interface on or off:

- `sudo ip link set dev docker0 [down/up]`

Manually change MAC address for an interface:

- `sudo ip link set dev docker0 address CA:FE:C0:FF:EE:00`

Send web request to locally hosted webpage:

- `curl http://localhost:8000`

`cut` command options:

Flag	Description
-f	Specifies the field (column)
-d	Specifies the delimiter

"Sort Sandwich":

- `sort | uniq -c | sort -n`