TCPDUMP usage

tcpdump -i any “net 192.168.0.0/16 or net 172.16.0.0/16” -w ~/file.pcap

tcpdump -i eth0

- **-i any** (listen on any interface)

Type: **host**, net (ip/sm), **port**

- tcpdump host 1.1.1.1

Direction: **src** , **dst** (traffic in one direction)

- tcpdump src port 1025
- tcpdump **portrange** 21-23

Protocols: **tcp**, udp, icmp, ...

- tcpdump icmp

tcpdump -nnSX port 443

- -X hex output for packet content
- -S get entire packet
- **-cn** .... capture n number of packets
- **-nn** ... don't resolve hostnames or ports

tcpdump -i any -w capfile.pcap

- **-w** write to file "capture_file"
- **-r** file to read input from

tcpdump -i any -qs 500

- q quite, s size in bytes

A tcpdump Tutorial with Examples - 50 Ways to Isolate Traffic | Dan
is without question the premier network analysis tool because it provides bo
simplicity in one interface. My other tutorials This tutorial will show you how
traffic in various ways-from IP, to port, to protocol, to application-layer traffic
https://danielmiessler.com/study/tcpdump/

Combinations

- and , &&
- or , ||
- Except: not , !

tcpdump src host 192.168.51.4 and dst port 22

- host can be omitted

tcpdump 'src net 192.168.0.0/16 **and (**dst net 10.0.0.0/8 **or** 172.16.0.0/16)'

- traffic from one net to 2 net

tcpdump dst 172.16.51.4 and **not** dst port 22

tcpdump -vv port ftp **or** ftp-data

- verbose, will catch the passwd.

tcpdump -vv | grep GET

```
[root@az-fer5 ~]# jobs
[1]+  Running                 tcpdump -i any host 192.168.5.4 -w /home/vchung14/thurs2.pcap &
[root@az-fer5 ~]# fg 1
tcpdump -i any host 192.168.5.4 -w /home/vchung14/thurs2.pcap
^C347 packets captured
349 packets received by filter
0 packets dropped by kernel
[root@az-fer5 ~]#
```