TCPDump

Filter on port 80

```
tcpdump port 80
```

Filter on source port 80

```
tcpdump src port 80
```

Destination port 80

```
tcpdump dest port 80
```

All traffic for 192.168.1.1

```
tcpdump host 192.168.1.1
```

Save output

```
tcpdump tcp -w output.pcap
```

Resource: https://medium.com/swlh/introduction-to-tcpdump-635653f56177

Filter on service

In this case, we are filtering icmp traffic on the eth0 interface where the ICMP type field value is icmp-echo. We finish it with a full protocol decode (-vv) aka verbose output.

```
tcpdump -i eth0 icmp and icmp[icmptype]=icmp-echo -vv
```

Resources: http://alumni.cs.ucr.edu/~marios/ethereal-tcpdump.pdf

http://www.networksorcery.com/enp/protocol/icmp/msg8.htm

Listen for traffic over port 389

```
tcpdump -i eth0 -nn port 389
```

Resource: https://hackertarget.com/tcpdump-examples/

Revision #1
Created 2023-11-10 06:25:14 UTC by Ryan
Updated 2025-02-12 01:11:15 UTC by Ryan