Network Tools

- A reminder about ethics
- Up till now:
  - ping
  - tcpdump
- Today:
  - nmap
  - nc
- Later:
  - Scapy

Ethics/Laws (from a non-lawyer)

- Do you have premission to run these commands?
- Will they bother anyone else?
- How is the system likely to react?

`ping`

- `ping` crafts a packet (ICMP, which is not TCP or UDP. . .) which requires a respnose
  - `ping` continues to listen for a response and provides metrics

tcpdump

Very useful command for inspecting traffic on a network.

- has many *filter* options to only capture desired traffic (or `!` ignore unwanted traffic)
- typically installed everywhere
- underpinning of graphical program Wireshark (uses same filters!)

Scapy (later)

- `scapy` captures, crafts, manipulates, sends, and recieves packets via python
  - very advanced, but you need to understand what a packet "looks" like

nmap

Network exploration and security / port scanner (according to the `man` page).

Here be dragons!

`nmap` can generate a LOT of traffic in a short amount of time, and almost always appears malicious. Run it only on systems you have permission to (both incoming and outgoing)!
This tool can also be quite stealthy, generating a lot of useful information by simply listening.

> *The quieter you become the more you are able to hear.*
> *-Rumi (& the Kali linux motto)*

`netcat` or `nc`

Tool to inspect create sockets (application connections to an IP port). Allows you to simply connect to another host IP and port, or to bind to a port locally and listen.

Think the `cat` command for network sockets.