Debugging Networking

Why?

- We always need to debug
- Networking is hard. Non determinism, plus unreliable
- Bespoke tooling

Other Notes

- These are all linux tools. Several also exist on other OS’s but equivalents will be available
- I will be using Python for demonstrations
  - Because its quick for me to write
  - None of these tools/techniques are Python dependent
  - You’ll need some practice reading Python anyway

General Tips

- Isolate isolate isolate
- Use what you can control, if possible
- Stick to common design patterns
- Triple check your assumptions
- Keep tabs on what is worth testing
- Localhost is your friend, but also your enemy

What ports are in use currently?

lsof

- Lists open files
- Multitude of uses, but we want to list ports

sudo lsof -i -P -n

- sudo: run as supervisor
- -i: list internet files
- -P: Any ports are listed as numbers, not names
- -n: Any network numbers (e.g. IP) are given as numbers, not names

What ports are in use currently?

ss

- Socket statistics
- Replaces ‘netstat’ command

sudo ss -tulpn

- sudo: run as supervisor
- -t: Show TCP sockets
- -u: Show UDP sockets
- -l: Show listening sockets
- -p: Show process info of who has opened the socket
- -n: Any network numbers (e.g. IP) are given as numbers, not names

Can we filter these results down?

```
grep
```

- Global regular expression search and print

```
sudo lsof -i -P -n | grep LISTEN
```

- A|B : Pipe output of command A into B
- grep X: will apply regex X to all inputs, and only print if there is a match

Can we check one specific port?

grep

- We can filter for anything

sudo lsof -i -P -n | grep :<*port*>

- Grep is a powerful tool, with uses far beyond just networking

Is someone reachable?

```
ping
```

- Ping sends simple messages to an IP address and receives a response
- Uses ICMP protocol which doesn’t have attached port

```
ping <IP>
```

- <*IP*>: The IP address to try and ping

What ports are they listening on?

```
nmap
```

- Network mapper
- Can map arbitrary ports and IPs
- Used for auditors, designers, and hackers

```
nmap <IP>
```

- <*IP*>: The IP address to try and map

What about a specific port?

nmap

- Network mapper
- Can map arbitrary ports and IPs
- Used for auditors, designers, and hackers

nmap -p <*port*> <*IP*>

- -p <port>: The port specifically to inspect
- <*IP*>: The IP address to try and map

Can we test simple transactions?

telnet

- Telecommunication network
- Sends and receives ascii text, but that is often enough

telnet <*IP*> <*port*>

- <*IP*>: The IP address to connect to
- <*port*>:The port to connect to
- Once connected you need to manually type requests

Web browsers can navigate the net

- Your web browser can navigate to any IP/port address
- And they often have developer tools to inspect what has gone back and forth
- This isn’t always meaningful