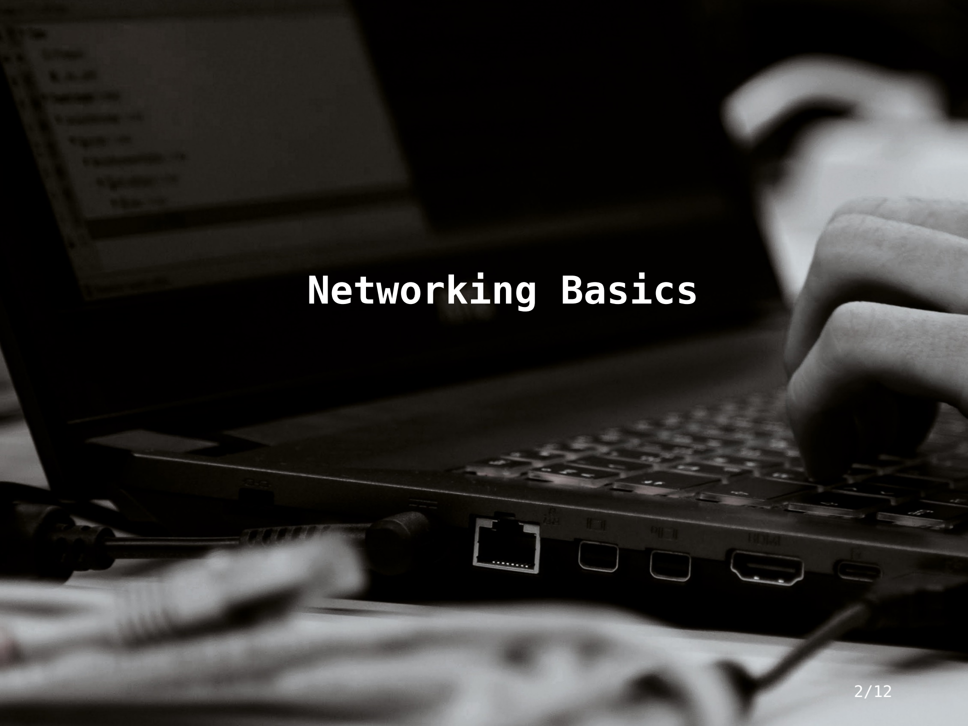
Network

Michael Preisach

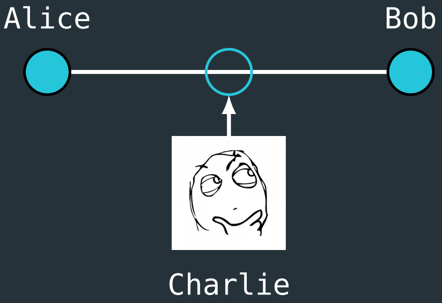
May 17 2019



Networking Basics

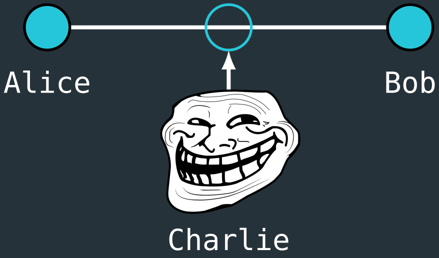
Networking Basics

- How do you get the traffic between Alice and Bob?



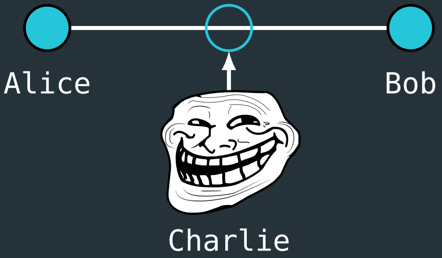
Networking Basics

- Alice and Bob are connected directly:
  - Use two bridged interfaces on your computer and connect them to Alice and Bob
- Alice and Bob are connected via a hub
  - Just plug in to one port of the hub



Networking Basics

- Alice and Bob are connected via a switch:
  - Managed switch: Mirror the port of either Alice or Bob to Charlie
  - Unmanaged switch: use a managed switch



Networking Basics

- How do you capture the traffic?
    - tcpdump (CLI)
    - Wireshark (GUI)

Example: Capturing traffic from eth0

```
sudo tcpdump -i eth0 -w capture.dump
```

Wireshark

Wireshark

- Open a `.dump` file OR capture from NIC
- Filter traffic
  - Big variety of supported protocols
  - Filter rules down to single bits of a protocol possible
  - Where should I start?

Wireshark

- Find the interesting parts in a dump: Filter packets
  - by IP address,
  - port number,
  - protocol flag,
  - ...
- `Menu->Analyze->Follow->* Stream`
  - Displays the payload of one connection (SYN to FIN)

Example: Filtering packets in Wireshark

```
ip.dst==192.168.1.1 and tcp.dstport==1337
ip.addr==192.168.1.1 and tcp.port==1337
tcp.flags.reset==1
```

Conclusion

Conclusion

- TCPdump can also handle filter rules (same syntax)

Example: TCPdump with filter rule

```
sudo tcpdump -i eth0 -w capture.dump "ip == 192.168.1.1 and
    tcp.port == 1337"
```

- TCPdump man page: www.tcpdump.org/manpages/tcpdump.1.html
- Wireshark User’s Guide: www.wireshark.org/docs/wsug_html_chunked

Happy Dumpster Diving!