S2E5 - analysing packets

Nicholas Morrison nick@nanocat.net

Connecting to the lab server

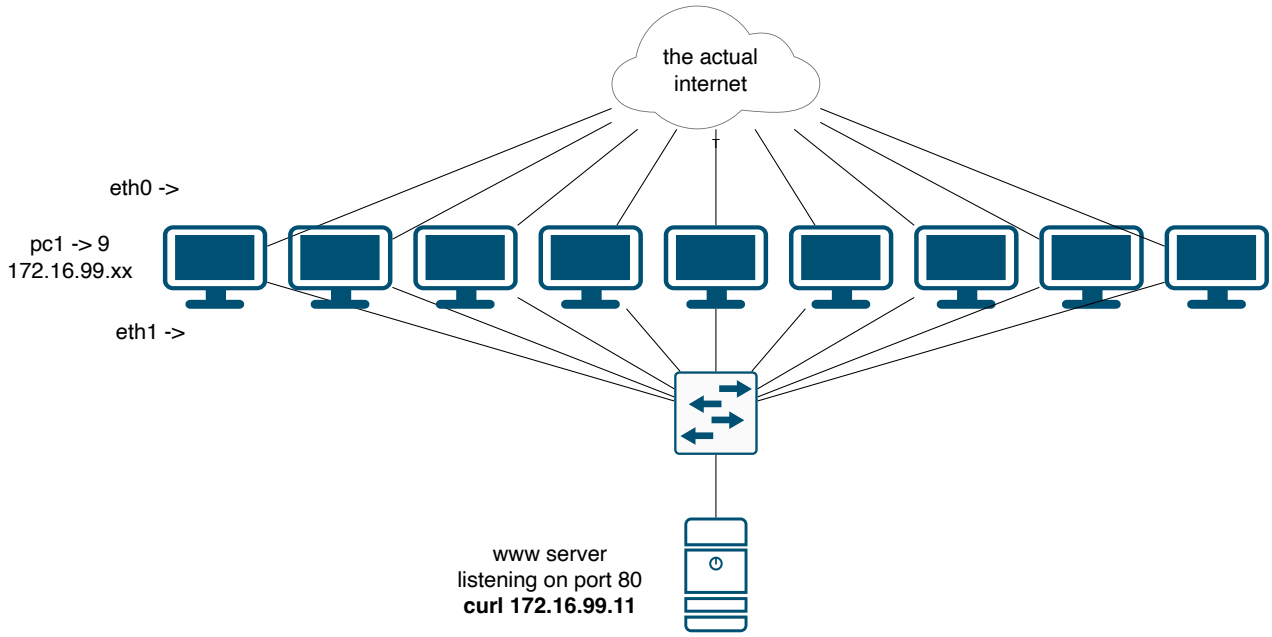
Connect to the lab server:

```
local$ ssh-keygen -R netlab.nanocat.net
local$ ssh lab@netlab.nanocat.net
Password: (see discord)
```

Connect to your router:

```
lab@netlab$ list-devices
lab@netlab$ connect DEVICE
```

Topology



Goals

- generate and capture some interesting traffic on the netlab server
- analyse the packet capture(s) locally using Wireshark

Preparing the packet capture

- decide which PC you are (pc1 -> pc9)
- find this PC's network namespace (`ip netns list` or `ip netns list | grep pcX`)
- run a tcpdump on your PC's `eth0` interface (because eth0 is connected to the Internet)
  - `ip netns exec NAMESPACE tcpdump -i eth0 -s 1500 -c 5000 -w YOUR_PERSONAL_FILENAME.pcap`

Generating some traffic

In another terminal, while the tcpdump is running, do each of the following:

- ping a site by name, that you have not pinged before
  - eg. `ping -c 10 www.idsoftware.com`
- traceroute to a site by name, with name lookups DISABLED
  - eg. `traceroute -w 1 -n nanocat.net`
- traceroute to a site by name, with name lookups ENABLED
  - eg. `traceroute -w 1 nanocat.net`
- fetch a file over http
  - `wget http://insecure.nanocat.net/files/snarf.txt`
- fetch a file over https
  - `wget https://nanocat.net/files/snarf.txt`
- fetch a file from an ftp server
  - eg. `wget ftp://ftp.uni-bayreuth.de/debian/README.CD-manufacture`

Transfer the packet capture

Back at your tcpdump terminal:

- `ctrl-c` the tcpdump, if it has not already exited (remember we set a limit of 5000 packets)
- make sure the .pcap file is there using `ls -l YOUR_PERSONAL_FILENAME.pcap` (or `ls -l *.pcap` if you can't remember)
- from your laptop, copy the file using SCP (secure copy protocol): `scp lab@netlab.nanocat.net:YOUR_PERSONAL_`
  .

Use Wireshark

- Things to try:
  - Use the filter bar to find your traffic:
    - filter by IP: `ip.host == 1.1.1.1` or `ip.dst == 1.1.1.1` or `ip.src == 1.1.1.1`
    - filter by TCP port: `tcp.port == 80` for http, `tcp.port == 443` for https, `tcp.port == 21 || tcp.port == 20` for FTP
  - "follow tcp stream" - right-click on an http packet, "Follow / TCP stream"
  - find a TCP three-way handshake (SYN / SYN-ACK / ACK)
    - the first three packets in your "follow tcp stream"
  - dig into a SYN packet
    - select a SYN packet, and "unfold" the packet details section