IN4180 Workshop - Network monitoring

1. Bring up the docker environment and connect to the client with VNC. Instructions are in the README.

https://github.uio.no/moskjegs/in4180-docker-network

In the VNC desktop (http://localhost:8012, password "insecure")

2. Open a terminal and check that you can run `ping in4180-web-server`

3. Start Wireshark, double click `eth0` and begin a packet capture - ignore the two error messages (they are related to the docker environment)

Ping in4180-web-server again — can you see the traffic in Wireshark?

4. In a Terminal, download the web page with curl — (`curl http://in4180-web-server`)

Can you find the content of the web page in the TCP traffic captured by Wireshark?

4. Netcat can be used to open TCP connections, similar to telnet. Connect to the web server and pretend you are a client:

```
nc in4180-web-server 80
```

Then type the following HTTP request and press enter. Press CTRL-C or enter to exit. You should see the same output as you saw with curl.

```
GET /
```

6. The web server is compromised! Use available tools on the client to determine how.

Hint: use nmap to portscan the web server. Tools you need: nmap, netcat

When you access the compromised host, use the "`id`" command to verify if you have root access!

You should see:

```
uid=0(root) gid=0(root) groups=0(root)
```

7. Suricata, an IDS, is running on a SPAN port mirroring the traffic to/from the web server. Has it registered your activity?

From your computer terminal (not in VNC), use `docker exec -it in4180-span-server bash` to open a shell to it. The logs are in `/var/log/suricata`

8. Bonus task: How was the web server backdoored?
    a) Find the backdoor
    b) Remove it

To get shell access on the web server:

```
docker exec -it in4180-web-server bash
```

Some commands may require `sudo`