

Netzwerksicherheit

Test: Was läuft auf meinem Rechner?

```
sudo netstat -tulpen
```

Test: Was läuft auf einem Rechner im Netzwerk?

(Hier: Nur TCP-Dienste, der Rechner wird NICHT vorher angepingt, Betriebssystem erraten)
(Warnung: Scan-Versuch vorher mit Betreiber abklären, einige Gateways sperren Scanner vom Netz aus!)

```
sudo nmap -P0 -sT -O ip-adresse
```

Ganze Netze scannen:

```
sudo nmap -P0 -sT -O ip-netzadresse/netzmaske
```

Schaut nach, auf welchem Rechner im 10-er Netz ein SSH-Server (TCP Port 22) läuft

```
sudo nmap -P0 -sT -O --open -p 22 10.0.0.\*
```

Sicherheits-Tools zum aktiven und passiven **Finden von Sicherheitsproblemen:**

OpenVAS (ehemals nessus)

Hacker-Tools zum Übernehmen von Verbindungen oder Mitloggen von Passwörtern:

ettercap

Netzwerk-Analyse:

wireshark

Firewall selber bauen: iptables unter Linux (sehr umfangreich)