Netzwerk-Tools unter Unix/Linux und Windows

Unix: `traceroute`

Windows: `tracert`

Gibt den Weg aus, den Pakete vom aktuellen Rechner zum Zielrechner nehmen (mit allen Gateways).

`ping Rechnername`
(Unix und Windows) simple Messung der Antwortzeit zum Zielrechner

`mtr Ziel`
(Unix) Multi Traceroute, gibt die Antwortzeiten auch für alle Zwischenstationen aus.

`sudo netstat -tp`
Zeigt an, welche TCP-Verbindungen der eigene Rechner nach außen offen hat, und welches Programm sie geöffnet hat. (Unix)

`sudo netstat -tulpe (n)`
Zeigt an, welche Dienste auf dem eigenen Rechner laufen, und welches Programm dahinter steht. (Unix)

`ifconfig` ohne Parameter: (Unix) Listet ALLE IP-Adressen ALLER aktiven Karten (Windows: `ipconfig`)

`ifconfig -a` (ohne weitere Parameter): Listet auch die INAKTIVEN Netzwerkinterfaces.

Manuell ins Netz unter Linux:

1. `ifconfig eth0 192.168.0.1` (IP-Adresse für Netzwerkkkarte eth0 setzen)
2. `route add default gw 192.168.0.254` (Standard-Gateway setzen)
3. Nameserver eintragen als „`nameserver 192.168.0.254`“ in `/etc/resolv.conf`

„Verbotene“ Tools:

`nmap Zieladresse` oder `Zielnetzwerk`
Portscanner, listet die laufenden Dienste auf allen Rechnern des angegebenen Netzwerkes auf. Vorsicht: Nicht ohne Wissen des zuständigen Netzwerkadministrators starten, da Scanversuche oft als Angriffe protokolliert und zurückverfolgt werden!

`ettercap`
Aktiver Sniffer mit ARP-Poisoning, ***kein Spielzeug***, ohne Zustimmung der Beteiligten nach deutschem Recht verboten (→ Ausspähen von Daten)!!! (Unix und Windows)