Werkzeuge zur Netzwerkdiagnose

Markus Dahms

BraLUG e.V.

16. Januar 2008

Überblick

Rechtliches

- Benutzung der Werkzeuge im Zusammenhang mit Netzwerken und Rechnern nur im Wissen und mit der Erlaubnis des Eigentümers zulässig (§202a StGB: „Ausspähen von Daten“, §202b StGB: „Abfangen von Daten“
- Besonders kritisch ist der am 11. August 2007 in Kraft getretene §202c StGB: „Vorbereiten des Ausspähens und Abfangens von Daten“. Beschaffung, Herstellung und Verbreitung von Programmen, deren Zweck die Begehung einer Straftat nach §202a oder §202b StGB ist, ist strafbar.
- *ich bin kein Anwalt*

TCP/IP-Referenzmodell

TCP/IP-Schicht	**≈ OSI-Schicht**	**Beispiel**
Anwendungsschicht	5 - 7	HTTP, FTP
Transportschicht	4	TCP, UDP, SCTP
Vermittlungsschicht	3	IPv4, IPv6
Netzzugangsschicht	1 - 2	Ethernet, IEEE 802.11

Außerdem wichtig

- *Domain Name System* – Namensauflösung
- Routing
- eventuelle Paketfilter
- Proxy-Server

Ethernet-Diagnose

- Linux-Kernel bezeichnet Ethernet-Schnittstellen mit `eth*`
- `ifconfig -a` zeigt alle erkannten Netzwerkgeräte an (nicht nur Ethernet), alternativ auch `netstat -i` oder `ip link show`
- `ethtool` bzw. `mii-tool` überprüft Link-Status

IP-Konfiguration & -Tests

- Kontrolle der Konfiguration: `ifconfig`
  - stimmt die IP-Adresse?
  - ist das Gerät aktiv?
  - werden Fehler angezeigt?
  - empfangene *und* gesendete Pakete?
- Netzwerktest mit ICMP-Paketen: `ping`
  - Antwortzeiten, verlorene oder doppelte Pakete?
  - Achtung: ICMP Echo/Reply kann deaktiviert werden
- Adressauflösung im Ethernet: `arp`

dynamische Konfiguration – DHCP

- `dhclient` (alternativ `dhcpcd` oder `pump`) „zu Fuß“ starten
- korrekte IP-Adresse?
- Routen, Broadcast-Adressen, DNS-Server und Such-Domain richtig?

Routing

- wichtig, um aus einem Subnetz in ein anderes zu gelangen
- meist über ein Standard-Gateway realisiert
- `route` oder `netstat -r` zeigen Routing-Informationen an
- Gateway (Router) muss im gleichen Subnetz liegen
- `traceroute` zeigt die verschiedenen Stationen auf dem Weg eines IP-Pakets

Namensauflösung testen

- Konfiguration in `/etc/resolv.conf`, `/etc/host.conf` und `/etc/nsswitch.conf`
- Test mit `nslookup`, `host` oder `dig`
- bei Fehlfunktion der lokalen DNS-Server öffentlichen Server testen, z.B. `141.1.1.1`

Paketfilter: iptables

- `iptables -L` zeigt Konfiguration an
- Policies müssen auf `ACCEPT` stehen oder Pakete müssen explizit erlaubt werden
- Paketfilter im Zweifel ausschalten
- *Aber*: NAT wird unter Umständen zum Routing benötigt

Offene Ports

- lokal: `netstat`
  - `-a` – alle Ports, auch Server
  - `-t` – TCP-Ports
  - `-u` – UDP-Ports
  - `-n` – keine Auflösung von Host- und Service-Namen
  - `-p` – Programm, dass den Port geöffnet hat, anzeigen (nur `root`)
- entfernt: `nmap`
  - Brute-Force-Portscanner
  - siehe *Rechtliches*

TCP-Strecken testen

- Verbindungstest auf entfernten Server z.B. mit `telnet`
- Aufbau eigener Minimal-Server und -Clients mit `netcat`

Linux-Mechanismen zu weiteren Einstellungen

- `sysctl` oder `/proc/sys/*` bieten viele Möglichkeiten zum Feintuning
  - `net.ipv4.conf.all.rp_filter` – Spoof protection
  - `net.ipv4.tcp_syncookies` – TCP SYN cookies
  - `net.ipv4.ip_local_port_range` – Bereich der automatisch vergebenen Ports
  - `net.ipv4.conf.default.forwarding` – Schalter für IP-Forwarding (benötigt für Router)
  - `net.ipv4.icmp_echo_ignore_broadcasts` – keine ICMP-Echo-Antworten bei Broadcast-Anfragen

HTTP? Proxy?

- häufige Fehlerursache bei `HTTP` ist ein nicht funktionierender Proxy-Server
  - falscher Proxy-Server eingestellt
  - Proxy-Server down
  - kein Proxy vorhanden, weil keiner benötigt wird

Paketanalyse mit `tcpdump`

- horcht *alle* IP-Pakete ab, die auf einem Netzwerkgerät ankommen oder gesendet werden
- unterstützt nicht nur `TCP`, sondern auch `UDP`, `ICMP`, `ARP` u.v.m.
- relativ einfach zu bedienendes Filtersystem mit logischen Verknüpfungsmöglichkeiten

- grafisches Programm (GTK+)
- kann `tcpdump`-Paketmitschnitte lesen
- Filter möglich
- bequeme Protokollanalyse

WLAN-Konfiguration

- WLAN-spezifische Einstellungen mit `iwconfig`
- generelle Netzwerkeinstellungen mit `ifconfig`
- kartenspezifische Einstellungen mit `iwpriv` oder speziellen Programmen wie `wlanconfig` (MadWifi)

WLAN-Netze anzeigen

- `iwlist $IF scan`

Häufige Fehlerursachen

- falsch/für das falsche Netz konfiguriert
- schon benutzte MAC, IP oder Port belegt
- Firewall blockiert zuviel
- fehlender Gateway oder Proxy
- Netzwerkgeräte in der falschen Reihenfolge eingebunden
- Hardware-Defekt (Kabelbruch, defekte NIC, etc.) oder schlechte Verbindung (WLAN)