Nicolas Tiefnig

Netzwerkanalyse mit TCPDUMP

TCPDUMP

Homepage: www.tcpdump.org
Source Code: https://github.com/the-tcpdump-group/tcpdump
Handbuch: http://www.tcpdump.org/manpages/tcpdump.1.html

TCPDUMP - Einführung

Packet Sniffer für Linux/BSD

- TCP Packete
- UDP Packete
- ICMP Packete

Kommandozeile, sehr klein

TCPDUMP - Benutzung

tcpdump [interface] [flags] [filters]

- interface - Netzwerkschnittstelle
- flags - z.B ASCII ausgeben
- filters - z.B nur TCP anzeigen

TCPDUMP - TCP Kommunikation

sudo tcpdump -i lo -v -A proto TCP
interface = loopback
verbose output
ASCII output == Mithören
TCP Protokoll

TCPDUMP - ping

sudo tcpdump -i lo -v proto ICMP
interface = loopback
verbose output
TCP Protokoll

TCPDUMP - HTTP Kommunikation

sudo tcpdump -i wlo1 port 80 and src nt-com.org
interface = wlo1 (WLAN)
Port 80 als Zielport
alle ein/ausgehenden Packete die nt-com.org als Quelle haben