tcpdump

context

dit document geeft enkele voorbeelden van tcpdump

SSH/SNMP

```
tcpdump port 22 or port 161 and src <ipadres van bron server> -vvv
```

scan verbose op SSH en SNMP verkeer

ping

```
tcpdump -i <NIC> host <dest> and icmp
```

netwerk

```
tcpdump -i <NIC> net <CDR>
```

WinDump

- Windows equivalent, beschikbaar op WinDump website

meer info

- TCPdump primer
- tcpdump command line examples

Linux