

netstat & ss

netstat und ss sind Netzwerk-Analyse-Tools, die offene Ports, laufende Netzwerkdienste und aktive Verbindungen anzeigen. Diese Informationen sind essentiell für Sicherheitsanalysen und die Fehlersuche bei Netzwerkproblemen.

Diese Dokumentation zeigt einen Sicherheitscheck. Die Tools netstat und ss werden dabei verglichen.

Voraussetzungen:

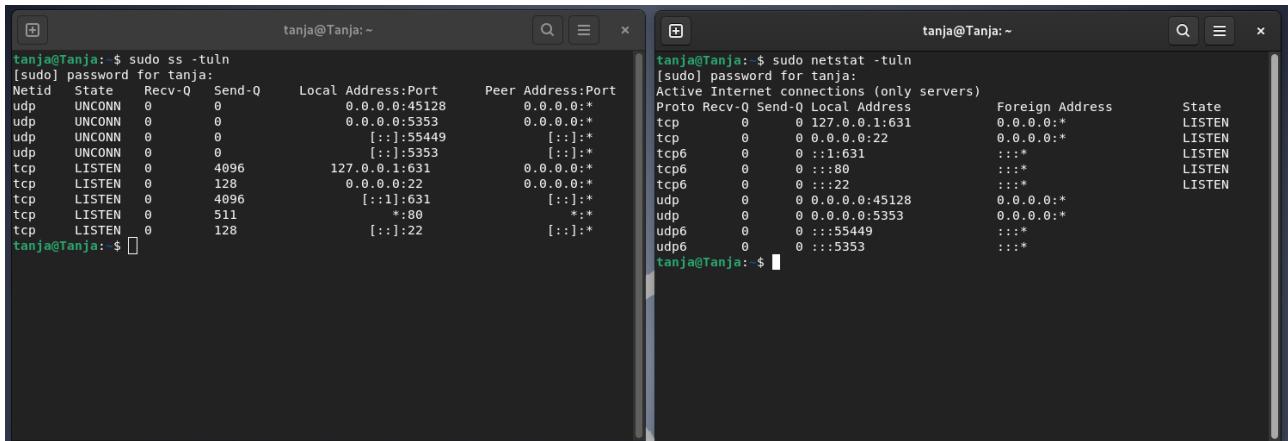
- Debian 13.2.0
- Root-Rechte
- netstat

Durchführung:

Schritt 1: Offene Ports identifizieren

[sudo ss -tuln](#)

[sudo netstat -tuln](#)



```
tanja@Tanja:~$ sudo ss -tuln
[sudo] password for tanja:
Netid State Recv-Q Send-Q Local Address:Port          Peer Address:Port
udp  UNCONN 0      0      0.0.0.0:45128            0.0.0.0:*
udp  UNCONN 0      0      0.0.0.0:5353             0.0.0.0:*
udp  UNCONN 0      0      [:]:55449                [:]:*
udp  UNCONN 0      0      [:]:5353                [:]:*
tcp  LISTEN 0     4096   127.0.0.1:631            0.0.0.0:*
tcp  LISTEN 0     128    0.0.0.0:22              0.0.0.0:*
tcp  LISTEN 0     4096   [:]:631                 [:]:*
tcp  LISTEN 0     511    *:80                   *:*
tcp  LISTEN 0     128    [:]:22                 [:]:*
```

```
tanja@Tanja:~$ sudo netstat -tuln
[sudo] password for tanja:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp     0      0 127.0.0.1:631            0.0.0.0:*
tcp     0      0 0.0.0.0:22              0.0.0.0:*
tcp6    0      0 ::1:631                ::*:*
tcp6    0      0 ::*:80                 ::*:*
tcp6    0      0 ::*:22                 ::*:*
udp     0      0 0.0.0.0:45128            0.0.0.0:*
udp     0      0 0.0.0.0:5353             0.0.0.0:*
udp6    0      0 ::*:55449               ::*:*
udp6    0      0 ::*:5353               :::*
```

Vergleich:

Beide Tools zeigen identische Informationen in leicht unterschiedlicher Darstellung. Im Gegensatz zu netstat ist ss das moderne Tool mit besserer Performance und wird aktiv weiterentwickelt. Es ist standardmäßig installiert und zeigt Informationen schneller an.

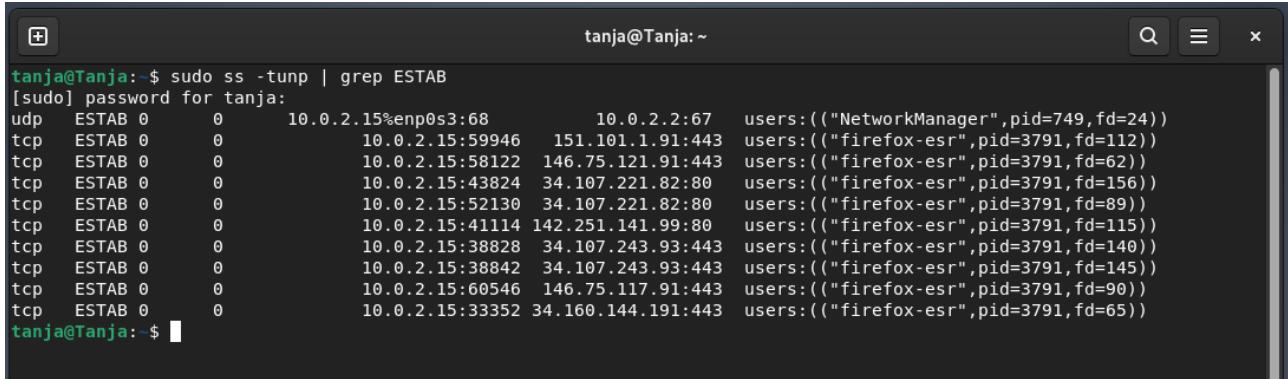
Ergebnis:

Webserver (Port 80): Läuft nur auf IPv6, nicht auf IPv4. HTTP ist unverschlüsselt – Daten können im Netzwerk mitgelesen werden. Für den lokalen Testbetrieb unkritisch, für Produktivsysteme sollte HTTPS (Port 443) verwendet werden.

SSH (Port 22) ist auf allen Netzwerk-Interfaces aktiv und ermöglicht Fernzugriff. Für einen lokalen Testservers im privaten Netzwerk ist dies unkritisch. Für Produktivsysteme empfiehlt sich jedoch die Beschränkung auf bestimmte IP-Adressen sowie key-basierte Authentifizierung anstelle von Passwort-Login.

Schritt 2: Aktive Verbindungen prüfen

[sudo ss -tunp | grep ESTAB](#)



```
tanja@Tanja:~$ sudo ss -tunp | grep ESTAB
[sudo] password for tanja:
tcp  ESTAB  0      10.0.2.15%enp0s3:68          10.0.2.2:67      users:(("NetworkManager",pid=749,fd=24))
tcp  ESTAB  0      10.0.2.15:59946       151.101.1.91:443   users:(("firefox-esr",pid=3791,fd=112))
tcp  ESTAB  0      10.0.2.15:58122       146.75.121.91:443  users:(("firefox-esr",pid=3791,fd=62))
tcp  ESTAB  0      10.0.2.15:43824       34.107.221.82:80    users:(("firefox-esr",pid=3791,fd=156))
tcp  ESTAB  0      10.0.2.15:52130       34.107.221.82:80    users:(("firefox-esr",pid=3791,fd=89))
tcp  ESTAB  0      10.0.2.15:41114       142.251.141.99:80   users:(("firefox-esr",pid=3791,fd=115))
tcp  ESTAB  0      10.0.2.15:38828       34.107.243.93:443  users:(("firefox-esr",pid=3791,fd=140))
tcp  ESTAB  0      10.0.2.15:38842       34.107.243.93:443  users:(("firefox-esr",pid=3791,fd=145))
tcp  ESTAB  0      10.0.2.15:60546       146.75.117.91:443   users:(("firefox-esr",pid=3791,fd=90))
tcp  ESTAB  0      10.0.2.15:33352       34.160.144.191:443  users:(("firefox-esr",pid=3791,fd=65))
tanja@Tanja:~$
```

Ergebnis:

1 UDP-Verbindung: NetworkManager (DHCP/Automatische Netzwerkkonfiguration)

9 TCP-Verbindungen: firefox-ESR

- 6x HTTPS (Port 443)
- 3x HTTP (Port 80)

Firefox unterhält 9 aktive Verbindungen: 6 davon nutzen verschlüsseltes HTTPS, 3 verwenden unverschlüsseltes HTTP (Port 80). Bei letzteren handelt es sich um Zugriffe auf den lokalen Testwebserver, was für diese Umgebung unkritisch ist.

Fazit:

Die Sicherheitsanalyse zeigt keine kritischen Befunde für diese Testumgebung. Für Produktivsysteme sind jedoch zusätzliche Sicherheitsmaßnahmen erforderlich: HTTPS statt HTTP und SSH-Absicherung durch IP-Beschränkung und Key-Authentifizierung. ss ist als modernes Tool zu bevorzugen, netstat bleibt für Kompatibilität relevant.