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.

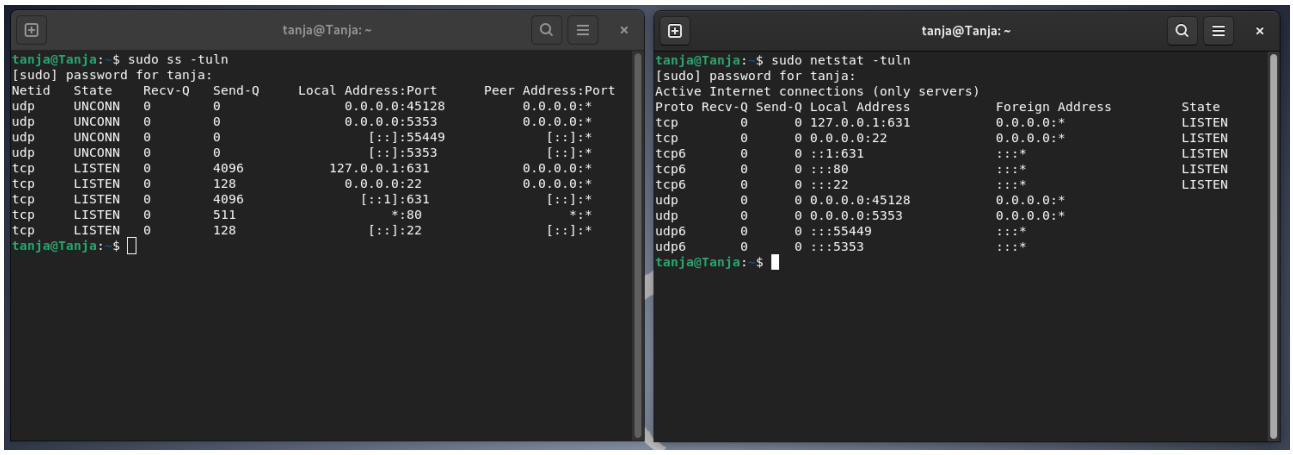
Voraussetzungen:

- Debian 13.2.0
- Root-Rechte
- netstat

Durchführung:

Schritt 1: Offene Ports identifizieren

sudo ss -tuln
sudo netstat -tuln



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.

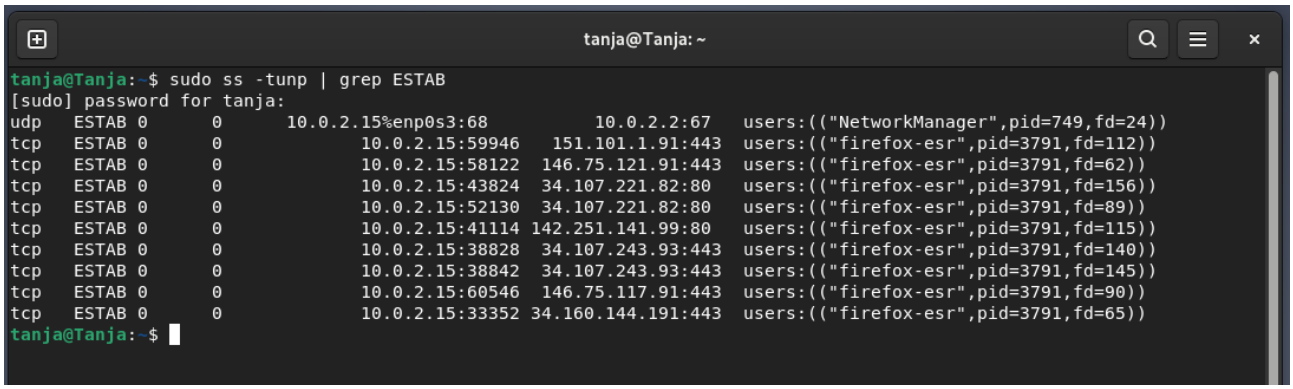
Ergebnis:

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



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.