

## ▢ Øvelse 19 – Installation af iptables

### ▢ Information

Formålet med denne øvelse er at introducere Netfilter-administrationsværktøjet *iptables* og give dig mulighed for at konfigurere det.

I Linux håndteres netværksfiltrering (firewall) af kerne-modulet *Netfilter*. Direkte interaktion med *Netfilter*-modulet er komplekst og ineffektivt, så der bruges typisk et interface. Et eksempel på et sådant interface er *iptables*, som vi anvender i undervisningen til at implementere firewall-regler.

Du kan læse mere om *iptables* i *Mastering Linux Security & Hardening*, kapitel 5, som var en del af forberedelsen til i dag.

I de følgende øvelser skal *iptables* installeres på din Ubuntu-serverinstans.

---

### ▢ Instruktioner

#### 1▢ Installation og grundlæggende kontrol

1. Installer *iptables* med kommandoen: `sudo apt install iptables`
  2. Udskriv versionsnummeret med kommandoen: `sudo iptables -V`
  3. Installer *iptables*-persistent med kommandoen: `sudo apt install iptables-persistent`
- 

#### 2▢ Gennemgang af firewall-regler

1. Udskriv alle firewall-regler (regelkæden) med kommandoen: `sudo iptables -L`
    - Hvad betyder *INPUT*, *FORWARD* & *OUTPUT*?
    - Hvilken en regel bør blokeret alt ved en host baseret firewall?
  2. Reflekter over, hvad der menes med firewall-regler, samt hvad der menes med "regelkæden".
-

## □ Vigtigt – Persistens af regler

### **OBS Vigtig!**

**Når man har ændret en iptables firewall-regel, skal man manuelt gemme den nuværende regelopsætning med kommandoen:** `sudo netfilter-persistent save`

Ellers er regellisten tom efter genstart.

Med den grundlæggende opsætning på plads, er du nu klar til at lave nogle regler i firewallen.

---

## □ Links

- [iptables manual page](#)
- 

Last update: 2026-03-20 13:58:28