## Security & Firewall (Plus)

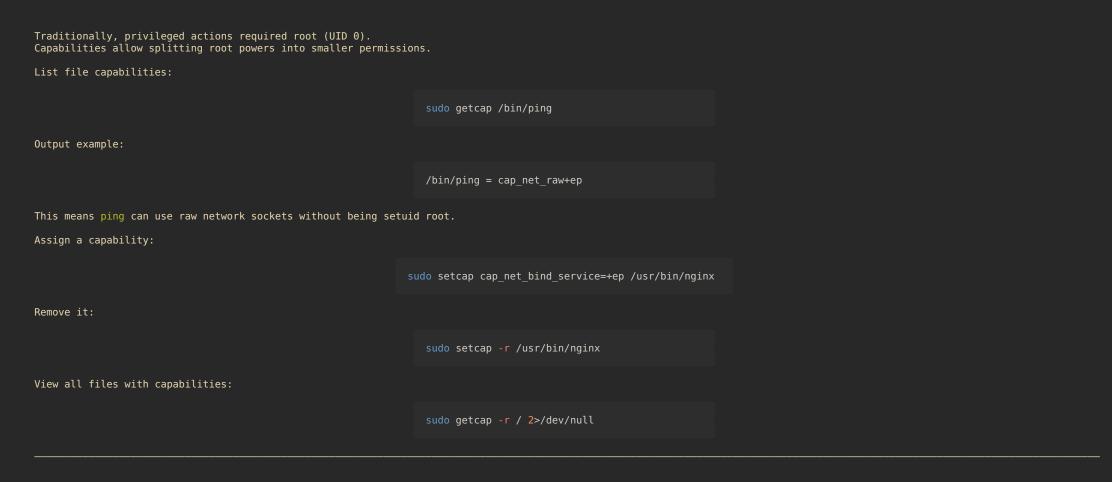
Linux Commands Course · Section 19

### **Linux Security Layers**

Linux security operates on multiple levels:

- Discretionary Access Control (DAC): standard file permissions and ownership.
   Capabilities: fine-grained privileges for executables.
   Mandatory Access Control (MAC): enforced security frameworks (SELinux, AppArmor).
   Network Firewall: traffic filtering with ufw, firewalld, or nftables.

### File Capabilities - getcap, setcap



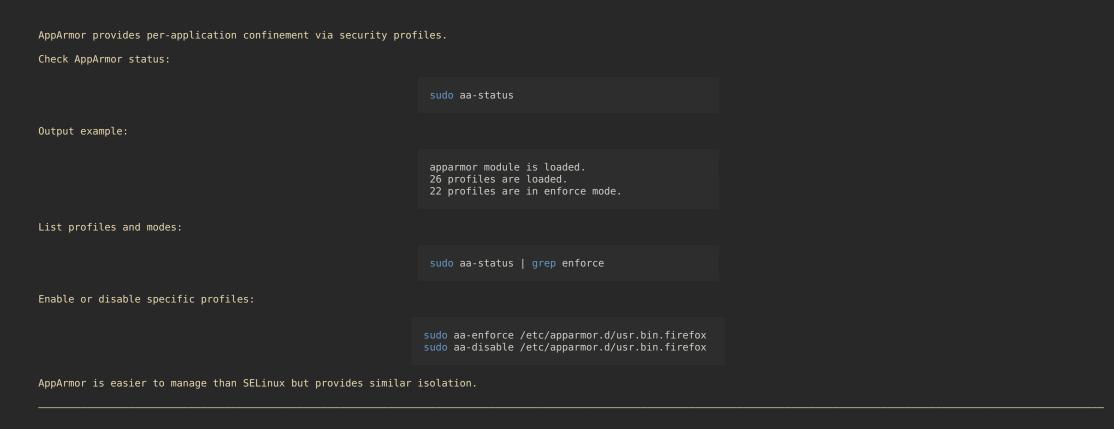
# Mandatory Access Control (MAC)

Beyond standard ownership and permissions, Linux can enforce additional security through **SELinux** or **AppArmor**.

## **SELinux (Security-Enhanced Linux)**

Developed by the NSA, SELinux enforces strict policy rules for processes and files. Check mode: Possible modes: • Enforcing — policy actively blocks violations • Permissive — logs violations but allows actions • Disabled — inactive Temporarily change mode (root only): sudo setenforce 0 # switch to Permissive sudo setenforce 1 # back to Enforcing View logs: sudo cat /var/log/audit/audit.log | grep denied Permanent configuration is in /etc/selinux/config.

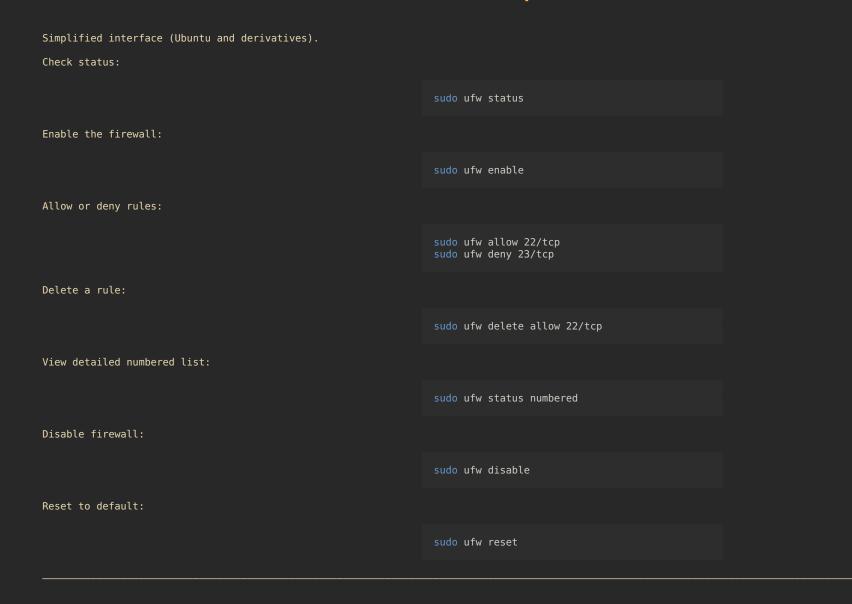
### AppArmor (Ubuntu and Debian)



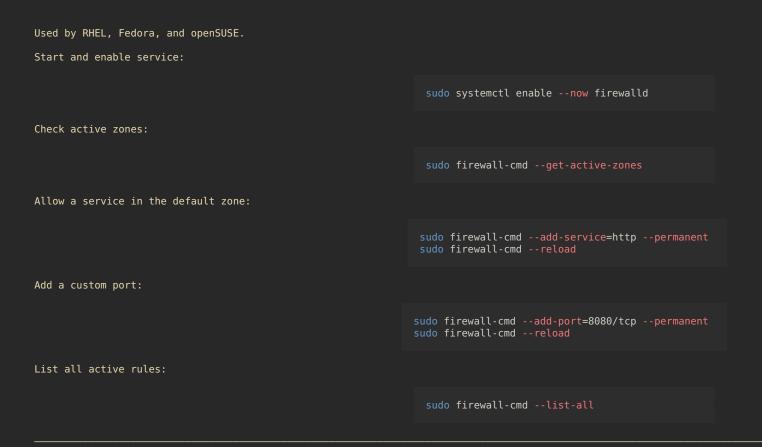
#### **Host Firewalls — Overview**

Linux firewalls filter traffic using the **netfilter** framework. There are several user-friendly frontends built on top of it.

## UFW (Uncomplicated Firewall)



#### firewalld and firewall-cmd



### nftables and iptables (Conceptual Overview)

```
nftables is the modern packet filter replacing iptables.
  • iptables — legacy interface (still widely used)

    nftables – unified replacement for IPv4/IPv6

Check active rules:
                                                                sudo nft list ruleset
Example nftables rule snippet:
                                                                table inet filter {
                                                                  chain input {
                                                                    type filter hook input priority 0;
                                                                    policy drop;
                                                                    iif "lo" accept
                                                                    ct state established, related accept
                                                                    tcp dport {22,80,443} accept
iptables equivalent (legacy):
                                                                sudo iptables -L -n -v
```

# When to Use Which

Tool	Recommended for	Notes
ufw	Simple desktop/server setups	Easy syntax
firewalld	Enterprise systems (RHEL/Fedora)	Zone-based rules
nftables	Advanced configurations	Modern standard
iptables	Legacy compatibility	Being replaced

#### Recap

- File capabilities: getcap, setcap (fine-grained privileges)
   MAC systems: SELinux (getenforce, setenforce), AppArmor (aa-status)
   Firewalls: ufw, firewall-cmd, nftables, iptables
   Defense layers work together never rely on just one.