

Homework — Lesson 01

~15 min · Two tasks · Bash only

Task 1 — Allow only SSH and HTTP, drop everything else

Using **iptables**, write rules that:

1. Allow inbound SSH (TCP/22) from anywhere.
2. Allow inbound HTTP (TCP/80) from anywhere.
3. Allow established/related return traffic.
4. Drop everything else inbound.
5. Allow all loopback traffic.

Self-check:

- `sudo iptables -L -v -n` shows your rules.
- From another host, `nmap -p 22,80,443 <your-ip>` shows 22 and 80 open, 443 filtered.
- Ping (ICMP) is blocked from outside.

Task 2 — Translate to nftables and persist

Recreate the same firewall using **nftables**:

1. Create a table and an input chain hooked at filter priority 0.
2. Add the four rules from Task 1.
3. Save the ruleset: `sudo nft list ruleset > rules.nft`.

4. Flush, then reload from file: `sudo nft flush ruleset && sudo nft -f rules.nft`.

Self-check:

- `sudo nft list ruleset` shows the same effective rules as Task 1.
- The `rules.nft` file is human-readable and can be edited.

[View solutions →](#)