

Solutions — Lesson 01

Worked answers for the homework tasks

Try the homework yourself before reading these. The reasoning matters more than the exact syntax.

Task 1 — Solution (iptables)

```
# Allow loopback (FIRST — locking out localhost breaks lots of services)
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A OUTPUT -o lo -j ACCEPT

# Allow ESTABLISHED,RELATED — replies to your outbound traffic come back
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

# Allow inbound SSH and HTTP
sudo iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW -j ACCEPT

# Default-deny anything else
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
```

Why this order matters

- **Loopback first** — many local services bind to `127.0.0.1`. If you set `INPUT` policy to DROP without an explicit accept rule on `lo`, you'll break DNS, package managers, and SSH itself.
- **ESTABLISHED before specific accepts** — every TCP connection's reply packets count as ESTABLISHED. Accepting them globally is faster (single rule) and simpler than thinking through every port.
- **Default-deny is set last** — if you set the default policy first, you'll lose your SSH session before adding the SSH rule.

Common mistake

Setting `iptables -P INPUT DROP` before adding the SSH accept rule. If you're SSH'd in remotely, your session dies. Always add accept rules *first*.

Task 2 — Solution (nftables)

```
# Create table and hooked chain
sudo nft add table inet filter
sudo nft 'add chain inet filter input { type filter hook input priority 0 ; po

# Allow loopback
sudo nft add rule inet filter input iif lo accept

# Allow established/related
sudo nft add rule inet filter input ct state established,related accept

# Allow new SSH and HTTP
sudo nft add rule inet filter input tcp dport 22 ct state new accept
sudo nft add rule inet filter input tcp dport 80 ct state new accept

# Save
sudo nft list ruleset > rules.nft
```

Reload pattern

```
sudo nft flush ruleset
sudo nft -f rules.nft
sudo nft list ruleset    # confirm
```

Format of `rules.nft`

```
table inet filter {
    chain input {
        type filter hook input priority filter; policy drop;
        iif "lo" accept
        ct state established,related accept
        tcp dport 22 ct state new accept
    }
}
```

```
    tcp dport 80 ct state new accept  
  }  
}
```

One bonus

nftables lets you set `policy drop` on the chain definition itself — no separate `-P` command needed. That's another concrete win over iptables.