Netfilter Tables

1. filter
- filter is the default table for iptables.
- iptables filter table has the following built-in chains: INPUT, OUTPUT and FORWARD
2. nat
- nat table is specialized for SNAT and DNAT (Port Forwarding)
- iptables NAT table has the following built-in chains: PREROUTING, POSTROUTING and OUTPUT (for locally generated packets)
3. mangle
- iptables mangle table is specialized for packet alteration
- mangle table has the following built-in chains: PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING
4. raw
- The raw table is only used to set a mark on packets that should not be handled by the connection tracking system. This is done by using the NOTRACK target on the packet.
- raw table has the following built-in chains: PREROUTING and OUTPUT

In a nutshell

- **Incoming traffic** is filtered on the **INPUT CHAIN** of the filter table
- **Outgoing traffic** is filtered on the **OUTPUT CHAIN** of the filter table
- **Routed traffic** is filtered on the **FORWARD CHAIN** of the filter table
- **SNAT/MASQUERADE** is done on the **POSTROUTING CHAIN** of the nat table
- **DNAT/PortForwarding** is done on the **PREROUTING CHAIN** of the nat table
- To modify values from the packet headers we add rules to the **mangle table**
- To skip connection tracking we add rules with **NOTRACK target** to the **raw table**