# Netfilter / iptables

- Every packet is inspected by firewall rules. **Firewall rules determine what traffic your firewall allows and what is blocked.**
- The iptables firewall **uses tables** to organize its rules.
- Within each iptables table, rules are further organized within separate CHAINS. **Rules are placed within a specific chain of a specific table.**
- Within a chain, a packet starts at the top of the chain and is matched rule by rule.
- When a match is found **the target is executed.**
- **A target is the action that is triggered** when a packet meets the matching criteria of a rule. If the target is terminating no other rule will evaluate the packet.

Linux Security: The Complete Iptables Firewall Guide
By Andrei Dumitrescu

# NETFILTER CHAINS

1. INPUT - used for filtering **incoming packets**. Our host is the packet destination.

2. OUTPUT - used for filtering **outgoing packets**. Our host is the source of the packet.

3. FORWARD - used for filtering **routed packets.** Our host is router.

4. PREROUTING - used for DNAT / Port Forwarding

5. POSTROUTING - used for SNAT (MASQUERADE)