

# Packet Filtering using iptables

---

Ahmed Mekkawy  
AKA linuxawy



# What is iptables/netfilter?



- The native firewall in GNU/Linux is iptables/netfilter.
- Netfilter is a kernel patch (now it's basic in all modern kernels, unless you compiled your own without it)
- Iptables is just a configuration tool for netfilter.
- You can uninstall iptables, but not netfilter.
- Netfilter cannot be stopped. Anyway you can remove all rules so it doesn't do anything.
- Iptables rules are volatile, you have to put them in a startup script to start with booting.



# What are the tables/ chains?



Tables => Chains => Rules

We have 3 tables:

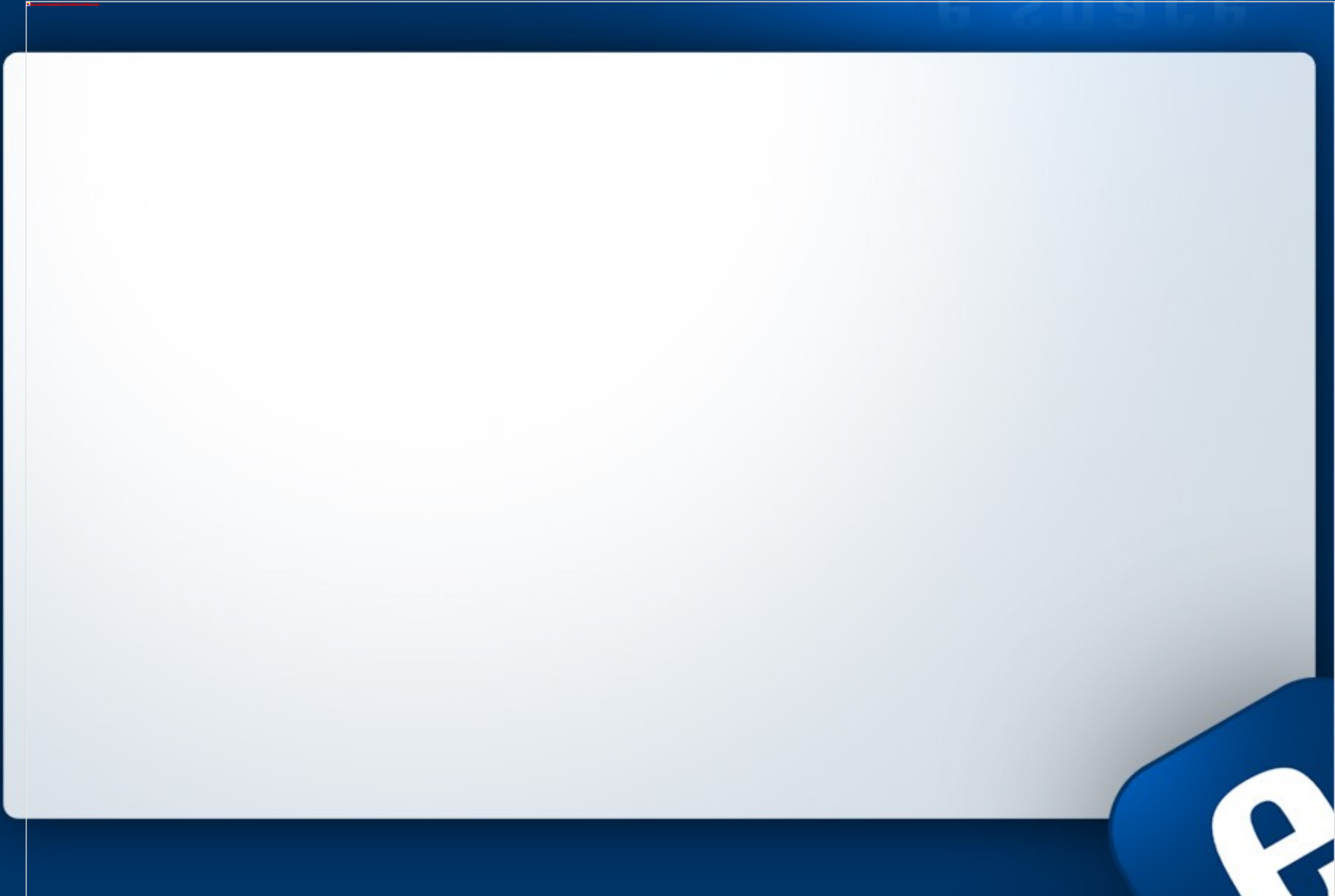
- Filter table
- Nat table
- Mangle table

We will focus on the filter table today, in filter table we have 3 main chains, which are:

- INPUT chain
- FORWARD chain
- OUTPUT chain



# Packets path



# Iptables syntax



How to add a rule:

- iptables -t table -A/I chain condition -j target
- iptables -A INPUT -p tcp --dport 80 -j ACCEPT

How to list rules:

- iptables -t (table) -L (-n) (--line-number)

How to delete a rule:

- iptables -t (table) -D (chain) (condition) (action)
- iptables -t (table) -D (chain) (rule number)



# conditions



- -p tcp,udp,icmp,all
- -s source\_ip
- -d destination\_ip
- --sport source\_port
- --dport destination\_port
- -i input\_interface
- -o output\_interface
- -m state --state NEW,ESTABLISHED,RELATED
- ... etc

-p tcp -s IP --sport 80 --d IP -m state --state NEW



# Targets

- ACCEPT: let it pass
- DROP: ignore it, and don't send any response.
- REJECT: drop the packet, and reply with error message (e.g port not used, host unreachable, .. etc) - to be used if you want the attacker not to know that you are using a firewall.
- COSTOM\_CHAIN: to direct the packet to a custom chain.
- SNAT, DNAT, .... : not used in filter table, to be used in the nat and mangle table, explained in other sessions isA.



# 3-way connection



The 3-way connection is the most commonly used connection. That happens in 3 steps:

- Step 1: client initiates the connection to the server. The connection type is now NEW.
- Step 2: server replies with acknowledgment, the connection is now in the ESTABLISHED state.
- Step 3: the client acknowledges the server, and starts to send its data in an ESTABLISHED connection.

After that, the connection continues in both ways normally.



# iptables initialization



- First, we flush all chains, delete custom chains, zero all counters:

```
iptables -F
```

```
iptables -X
```

```
iptables -Z
```

- Turn off IP forwarding:

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

- Enable dynamic IP support. 1: enable, 2: verbose, 0: disable

```
echo "1" > /proc/sys/net/ipv4/ip_dynaddr
```

- To use RELATED in ftp rules, add ip\_conntrack\_ftp:

```
modprobe ip_conntrack_ftp
```



# Set policies, enable loopback



- Set default policy to DROP:

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

```
iptables -P FORWARD DROP
```

- Enable all connections on the loopback interface:

```
iptables -A INPUT -i lo -j ACCEPT
```

```
iptables -A OUTPUT -i lo -j ACCEPT
```



# Enable pings



- Enable incoming/outgoing pings:

- Incoming:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

```
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

- Outgoing:

```
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
```

```
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```



# Add your rules

## Example: web server



```
iptables (-t filter) -A INPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables (-t filter) -A OUTPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```



# Special connections: ftp



- You must enable kernel module `ip_conntrack_ftp`
- FTP has 3 types of connections:
  - Control Port: Port 21, normal 3 way connection initiated by client.
  - Active connection: Port 20, normal 3 way connection RELATED to the previous connection, initiated by client
    - Passive connection: 3 way connection RELATED to the control connection, initiated by the server from a random port on the server to a random port at the client



# ftp - continued

- # Control Port:

- iptables -A OUTPUT -p tcp --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT

- iptables -A INPUT -p tcp --sport 21 -m state --state ESTABLISHED -j ACCEPT

- # Active mode:

- iptables -A OUTPUT -p tcp --dport 20 --sport 1024: -m state --state RELATED,ESTABLISHED -j ACCEPT

- iptables -A INPUT -p tcp --sport 20 --dport 1024: -m state --state ESTABLISHED -j ACCEPT

- # Passive mode:

- iptables -A OUTPUT -p tcp --dport 1024: --sport 1024: -m state --state ESTABLISHED -j ACCEPT

- iptables -A INPUT -p tcp --sport 1024: --dport 1024: -m state --state RELATED,ESTABLISHED -j ACCEPT



Thank you

Questions??

[ahmed.mekkawy@espace.com.eg](mailto:ahmed.mekkawy@espace.com.eg)

