Cheatsheet on ports and iptables

Meedos

1. Standard ports

These are some of the most known standard ports :

Standard ports

Port	Service	Use
20	FTP Data	The opened port by the FTP Server to send data to the FTP Client
21	FTP	The default port that FTP servers bind to
22	SSH	Secure Shell for remote connection
23	Telnet	Remote connection using Telnet
25	SMTP	Simple Mail Transfer Protocol, used for email routing between mail servers
53	DNS	The Port the Domain Name Service listens to DNS requests
68	DHCP	The port used by the Dynamic Host Configuration Protocol server to give out IP addresses
79	Finger	Used to identify users on the system
80	HTTP	Hypertext Transfer Protocol
113	Auth	The port the indent server users to verify users are coming from the IP address they claim to be
389	LDAP	Lightweight Directory Access Protocol
5432	PostgreSQL	The port the postgreSQL database uses
6667	IRC	Internet Relay Chat server

2. Setup a firewall with iptables

There are different types of firewalls that don't work the same, some may also use up more CPU than others. Quick reminder on firewall types :

Packet-Filter :

Monitors the network traffic by filtering the incoming packets according to the information they carry. It checks for the destination and source port and IP address. It is implement by default on all modern Linux kernels

Connection tracking

Exemple of the stateful firewall : This firewall keeps track of the state of each connection in a table such as LISTEN, ESTABLISHED and CLOSING. This table keeps track of TCP and UDP transfer protocols

2.1. iptables

2.1.1. Tables

- table NAT (Network Address Translation) : used for port and IP translation
- table **table Filter**: it is the default table when none are specified. This table contains all the filtering rules. There are 3 channels : FOWARD for all packets traversing the firewall, INPUT for the entering packets and OUTPUT for the packets exiting.

- table MANGLE (Not very used apparently)

2.1.2. Main commands

-A --append
Exemple:

```
        iptables -A INPUT ...
```

-D --delete : Deletes a chain. Chains can be deleted either by specified by specifying the chain number or a rule to delete.
Exemple:

```
        iptables -D INPUT --dport 80 -j DROP
        iptables -D INPUT 1
```

-R --replace : replace a specified chain.
Exemple:

```
        iptables -R INPUT 1 -s 192.168.0.1 -j DROP
```

-I --insert : insert rules at a given position in the chain
Exemple:

```
        iptables -I
```

-L --list : lists rules
Exemple:

```
        iptables -L # prints all the rules of the FILTER CHAIN
        iptables -L INPUT  # prints all the INPUT rules of the FILTER CHAIN
```

Footnote: It is possible to make rules for every source IP "except" for a certain IP using the "!" character.

2.1.3. Matching commands