UNIVERSITÉ
DE REIMS
CHAMPAGNE-ARDENNE

IPTABLE

PRACTICAL WORK 5

TIZIANO NARDONE
UNIVERSITY OF REIMS | FRANCE

I. Services inventory

1. Service inventory on Debian

➔ sudo apt-get install iptables
➔ sudo apt-get install net-tools
➔ netstat -ntupal

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 10.0.2.15:53            0.0.0.0:*               LISTEN      -
tcp        0      0 10.22.141.16:53         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      -
tcp        0      0 10.22.141.16:22         10.22.141.14:52037      ESTABLISHED -
tcp        0      0 10.0.2.15:55761         199.7.83.42:53          TIME_WAIT   -
tcp        0      0 10.22.141.16:22         10.22.141.14:52036      ESTABLISHED -
tcp        0      0 10.0.2.15:41592         199.232.178.132:80      TIME_WAIT   -
tcp        0      0 10.0.2.15:41594         199.232.178.132:80      TIME_WAIT   -
tcp        0      0 10.0.2.15:41590         199.232.178.132:80      TIME_WAIT   -
tcp        0      0 10.0.2.15:40493         8.8.8.8:53              TIME_WAIT   -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 ::1:53                  :::*                    LISTEN      -
tcp6       0      0 fe80::a00:27ff:fe58::53 :::*                    LISTEN      -
tcp6       0      0 fe80::a00:27ff:fe47::53 :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:953                 :::*                    LISTEN      -
tcp6       0      0 ::1:6010                :::*                    LISTEN      -
udp        0      0 10.0.2.15:53            0.0.0.0:*                           -
udp        0      0 10.22.141.16:53         0.0.0.0:*                           -
udp        0      0 127.0.0.1:53            0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp6       0      0 ::1:53                  :::*                                -
udp6       0      0 fe80::a00:27ff:fe58::53 :::*                                -
udp6       0      0 fe80::a00:27ff:fe47::53 :::*                                -
```

2. Service inventory on Alpine

➔ sudo apk add net-tools
➔ sudo netstat -ntupal

```
alpine:~$ sudo netstat -ntupal
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2347/sshd: /usr/sbi
tcp        0      0 10.0.2.15:57340         151.101.122.133:80      TIME_WAIT   -
tcp        0      0 10.0.2.15:57342         151.101.122.133:80      TIME_WAIT   -
tcp        0      0 10.22.141.15:22         10.22.141.14:52042      ESTABLISHED 3059/sshd: talp [pr
tcp        0      0 10.22.141.15:22         10.22.141.14:52041      ESTABLISHED 3056/sshd: talp [pr
tcp6       0      0 :::22                   :::*                    LISTEN      2347/sshd: /usr/sbi
tcp6       0      0 :::443                  :::*                    LISTEN      3028/httpd
tcp6       0      0 :::80                   :::*                    LISTEN      3028/httpd
alpine:~$
```

3. Service inventory on Ubuntu

➔ sudo apt-get install net-tools
➔ sudo netstat -ntupal

```
tub@ubuntu:~$ sudo netstat -ntupal
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      614/named
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      592/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      670/sshd: /usr/sbin
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      614/named
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      2932/sshd: tub@pts/
tcp        0      0 10.22.141.17:22         10.22.141.14:52043      ESTABLISHED 2686/sshd: tub [pri
tcp        0      0 10.0.2.15:60082         51.158.154.169:80       TIME_WAIT   -
tcp        0      0 10.0.2.15:60084         51.158.154.169:80       TIME_WAIT   -
tcp        0      0 10.22.141.17:22         10.22.141.14:52044      ESTABLISHED 2692/sshd: tub [pri
tcp6       0      0 :::80                   :::*                    LISTEN      2475/apache2
tcp6       0      0 fe80::a00:27ff:fe92::53 :::*                    LISTEN      614/named
tcp6       0      0 fe80::a00:27ff:febb::53 :::*                    LISTEN      614/named
tcp6       0      0 ::1:53                  :::*                    LISTEN      614/named
tcp6       0      0 :::22                   :::*                    LISTEN      670/sshd: /usr/sbin
tcp6       0      0 ::1:953                 :::*                    LISTEN      614/named
tcp6       0      0 ::1:6010                :::*                    LISTEN      2932/sshd: tub@pts/
udp        0      0 127.0.0.1:53            0.0.0.0:*                           614/named
udp        0      0 127.0.0.53:53           0.0.0.0:*                           592/systemd-resolve
udp        0      0 10.0.2.15:68            0.0.0.0:*                           590/systemd-network
udp6       0      0 ::1:53                  :::*                                614/named
udp6       0      0 fe80::a00:27ff:febb::53 :::*                                614/named
udp6       0      0 fe80::a00:27ff:fe92::53 :::*                                614/named
tub@ubuntu:~$
```

II. Safe machine

4. Useful commands

➔ sudo iptables -L –line-numbers
➔ sudo iptables -D INPUT/OUTPUT/FORWARD numberOfTheLine

5. To clean tables

➔ sudo iptables -F //All chains are empty

6. Keep active connections

➔ sudo iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
➔ sudo iptables -A OUTPUT -m state --state ESTABLISHED -j ACCEPT

7. Policies

BECAREFUL with Policies

➔ sudo iptables -P INPUT DROP
➔ sudo iptables -P OUTPUT DROP
➔ sudo iptables -P FORWARD DROP

8. Rules

➔ sudo iptables -A OUTPUT -p icmp -j ACCEPT
➔ sudo iptables -A INPUT -p icmp -s 10.22.141.14/22 -j ACCEPT

➔ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
➔ sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT

➔ sudo iptables -A INPUT -p tcp --dport https -j ACCEPT
➔ sudo iptables -A OUTPUT -p tcp --dport https -j ACCEPT

- ➔ sudo iptables -A INPUT -i lo -j ACCEPT
- ➔ sudo iptables -A OUTPUT -o lo -j ACCEPT

- ➔ sudo iptables -A OUTPUT -p udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
- ➔ sudo iptables -A INPUT -p udp --sport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
- ➔ sudo iptables -A INPUT -p tcp --sport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
- ➔ sudo iptables -A INPUT -p tcp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT

9. Save configuration

- ➔ sudo apt-get install iptables-persistent
- ➔ sudo iptables-save > /etc/iptables/rules.v4

III. Port forwarding

10. Enable ip forwarding

- ➔ Edit /etc/sysctl.conf

```
# Uncomment the next line
net.ipv4.ip_forward=1
```

- ➔ sudo sysctl – p /etc/sysctl.conf
- ➔ iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 80 -j DNAT --to 172.18.10.26:80 # ip de la debian