
FIREWALL

Scansione delle porte

- Come vedere i servizi attivi nella nostra vm? Con `netstat`! (`man netstat`)

```
# sudo netstat --inet -anp
```

```
root@las:~#
root@las:~# netstat  --inet -anp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:13              0.0.0.0:*               LISTEN      1114/inetd
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN      1345/dovecot
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN      1345/dovecot
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1250/nginx: master
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      1114/inetd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      874/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1149/sshd
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      1516/master
tcp        0      0 0.0.0.0:8000            0.0.0.0:*               LISTEN      1850/docker-proxy
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN      1345/dovecot
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN      1345/dovecot
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      1258/slapd
tcp        0      0 0.0.0.0:37              0.0.0.0:*               LISTEN      1114/inetd
tcp        0      0 0.0.0.0:7               0.0.0.0:*               LISTEN      1114/inetd
tcp        0      0 0.0.0.0:9               0.0.0.0:*               LISTEN      1114/inetd
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      1580/mysqld
tcp        0      0 127.0.0.1:59888         127.0.0.1:389           ESTABLISHED 1147/nscd
tcp        0      0 127.0.0.1:389           127.0.0.1:59888         ESTABLISHED 1258/slapd
tcp        0    176 192.168.64.128:22       192.168.64.1:56258      ESTABLISHED 6754/sshd: faromano
udp        0      0 0.0.0.0:9               0.0.0.0:*                           1114/inetd
udp        0      0 127.0.0.53:53           0.0.0.0:*                           874/systemd-resolve
udp        0      0 192.168.64.128:68       0.0.0.0:*                           863/systemd-network
root@las:~#
```

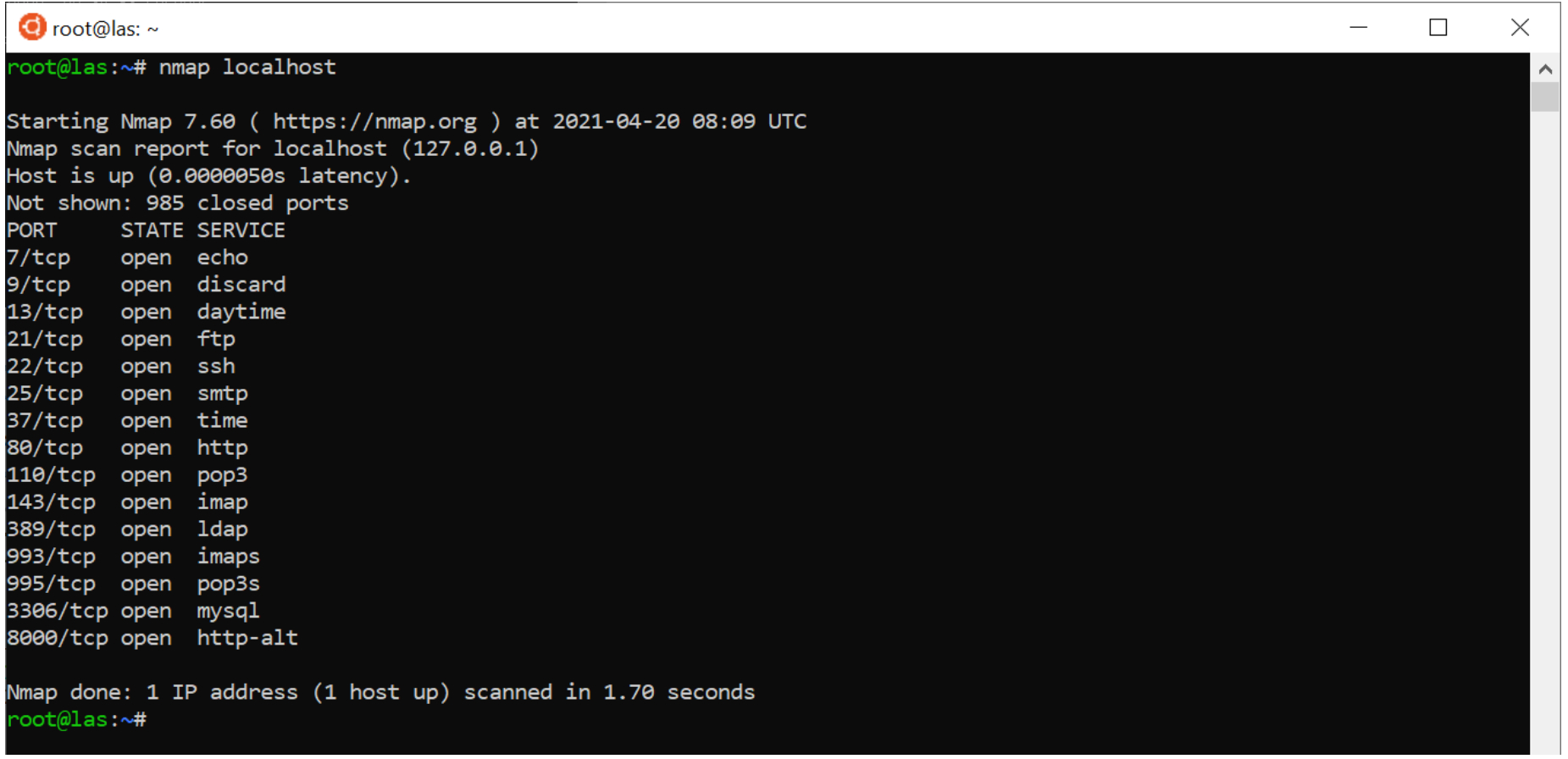
Scansione delle porte

Come vedere i servizi attivi di una macchina remota, o perché no anche della nostra macchina?

```
# nmap 192.168.100.xx
# nmap las.local
# nmap localhost
# nmap 192.168.100.1
# nmap 192.168.100.10
```

- `nmap` è un tool utilizzato per effettuare la scansione delle porte di host remoti. Lo vedrete al corso di sicurezza. Per saperne di più `man nmap` o https://nmap.org/
- Per installarlo: `sudo apt install nmap`

Scansione delle porte



IPTABLES

- Vi ricordate? Un firewall **iptables** è descritto da uno script di shell bash:

```
# cat fw0.sh
#!/bin/bash
echo 1 > /proc/sys/net/ipv4/ip_forward # abilita ip_forward
IPTABLES=$(which iptables)
# definizione di altre variabili utili
 . . . . . .
# istruzioni del firewall, iniziamo svuotando le catene.
$IPTABLES -F
$IPTABLES -X
$IPTABLES -Z
$IPTABLES -t nat -Z
```

IPTABLES

```
$IPTABLES -P INPUT DROP #definisce la politica della
                        #catena
$IPTABLES -A INPUT -i lo -j ACCEPT
$IPTABLES -I INPUT 1 -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

- Se questo script vi funziona provate a bloccare le porte di alcuni servizi che avete installato sulla vostra vm, li avete visti con `netstat` o `nmap`…. Per provare utilizzate `telnet` o `netcat` come abbiamo visto per la posta elettronica...
- Dovreste ottenere qualcosa di simile a quello che vedete nella slide successiva.
- PS: ricordatevi che lo script deve essere eseguibile (`chmod +x` …) e deve essere eseguito da root (`sudo`).

IPTABLES

```
# cat fw1.sh

#!/bin/bash
# Abilito ip forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward
# Carico i moduli necessari
modprobe ip_conntrack
modprobe iptable_nat
IPTABLES=$(which iptables)

# istruzioni del firewall, iniziamo svuotando le catene.
$IPTABLES -F
$IPTABLES -X
$IPTABLES -Z
$IPTABLES -t nat -Z
# Politica per la catena di INPUT
$IPTABLES -P INPUT DROP
# Abilitiamo l'accesso a localhost
$IPTABLES -A INPUT -i lo -j ACCEPT
# Abilitiamo la gestione degli stati per la catena di INPUT
$IPTABLES -I INPUT 1 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Abilitiamo l'accesso via ssh mantenendo la connessione esistente

$IPTABLES -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
# Abilitiamo i servizi installati nella nostra vm
###$IPTABLES -A INPUT -p tcp --dport 80 -j ACCEPT
###$IPTABLES -A INPUT -p tcp --dport 443 -j ACCEPT
###$IPTABLES -A INPUT -P tcp --dport 25 -j ACCEPT
# Abilitiamo la gestione degli stati per la catena di output
$IPTABLES -A OUTPUT -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
```

IPTABLES – router - facoltativo

- Con questo script di firewall permetteremo ad un secondo pc di uscire su internet:

```
# cat fw2.sh

#!/bin/bash
echo 1 > /proc/sys/net/ipv4/ip_forward
IPTABLES=$(which iptables)
ETH0="ens33"
ETH1="ens38"
$IPTABLES -F
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD DROP


# permette a tutto il traffico diretto alla rete locale di entrare
# $ETH1 e' la scheda di rete del server dove ho collegato il router wifi
# che permette ai client wifi di navigare in internet
$IPTABLES -A FORWARD -o $ETH1 -j ACCEPT
# permette a tutto il traffico diretto all'esterno di uscire
# $ETH0 e' la scheda di rete del server direttamente collegata ad internet
$IPTABLES -A FORWARD -o $ETH0 -j ACCEPT
# effettua il masquerade di tutto il traffico in uscita
$IPTABLES -t nat -A POSTROUTING -o $ETH0 -j MASQUERADE

#versione stateful
##$IPTABLES -t nat -A POSTROUTING -o $ETH0 -j MASQUERADE
##$IPTABLES -A FORWARD -i $ETH0 -o $ETH1 -m state --state RELATED,ESTABLISHED -j ACCEPT
##$IPTABLES -A FORWARD -i $ETH1 -o $ETH0 -j ACCEPT
```

NB: stiamo lavorando sulla catenal di forward!

IPTABLES – router e blocco servizi - facoltativo

- Realizzate una 3 macchina virtuale che utilizzeremo per testare il blocco dei servizi. Sul vostro server dovreste avere installati i servizi di http, daytime, echo, ftp, dhcp ecc.
- Vogliamo che alcuni di essi siano accessibili solo da determinati pc.

```
# cat fw3.sh

#!/bin/bash
echo 1 > /proc/sys/net/ipv4/ip_forward
IPTABLES=$(which iptables)
ETH0="ens33"
ETH1="ens38"
$IPTABLES -F
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD DROP

$IPTABLES -A INPUT -p udp -i $ETH1 –sport 68 --dport 67 -j ACCEPT
# Dovete trovare l’ip degli altri pc  e bloccare l’accesso ai
# servizi web ed ftp.

# Routing
$IPTABLES -A FORWARD -o $ETH1 -j ACCEPT
$IPTABLES -A FORWARD -o $ETH0 -j ACCEPT
$IPTABLES -t nat -A POSTROUTING -o $ETH0 -j MASQUERADE
##$IPTABLES -t nat -A POSTROUTING -o $ETH0 -j MASQUERADE
##$IPTABLES -A FORWARD -i $ETH0 -o $ETH1 -m state --state RELATED,ESTABLISHED -j ACCEPT
##$IPTABLES -A FORWARD -i $ETH1 -o $ETH0 -j ACCEPT
```