



JESUÏTES El Clot
Escola del Clot

M011-SEGURETAT INFORMÀTICA i ALTA SEGURETAT

UF3- Instal·lació i Configuració d'un servidor intermediari

PRÀCTICA 4 : IPTables

Curs: 2018-19

CFGs: ASIX2

Alumne : Arnau Subirós Puigarnau

Data : 22-03-2019

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

PRACTICA 4 : IPTables

Descripció

Per aquesta pràctica treballarem amb dos ordinadors: un farà de firewall i serà on hi haurà disponibles diferents serveis; i l'altre farà de màquina que vol connectar-s'hi, per accedir a aquests serveis. En aquest tutorial l'ordinador servidor-firewall del professor és el 192.168.1.141, i ho hauràs de substituir per la teva IP. Treballareu per parelles i s'aniran fent les proves que es comenten en aquest tutorial. Tots dos membres de la parella haureu de treballar en les dues parts de la pràctica.

Si algun membre de la parella no assisteix a classe durant la realització d'aquesta pràctica, podeu treballar telemàticament, o a distància. En cas que un dels membres de la parella no pugui treballar en aquesta pràctica, feu-m'ho saber enviant-me un correu electrònic, i feu la pràctica de manera individual, treballant amb màquines virtuals.

Enunciat

Podeu dur a terme una pràctica lliure, on simplement el que heu de fer és demostrar l'habilitat adquirida amb iptables i el domini del màxim de les comandes i opcions d'iptables (algunes de les quals es descriuen breument a continuació) que considereu que poden ser més útils i rellevants. Podeu utilitzar totes les explicacions que trobareu a continuació per dur a terme la vostra idea per aquesta pràctica.

És important que detalleu amb claredat i que sigueu concisos quan expliqueu el cas que heu decidit implementar per a la demostració del vostre domini d'iptables.

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

1. Introducció de les màquines Client-Servidor :

En aquesta pràctica utilitzaré 2 màquines virtuals:

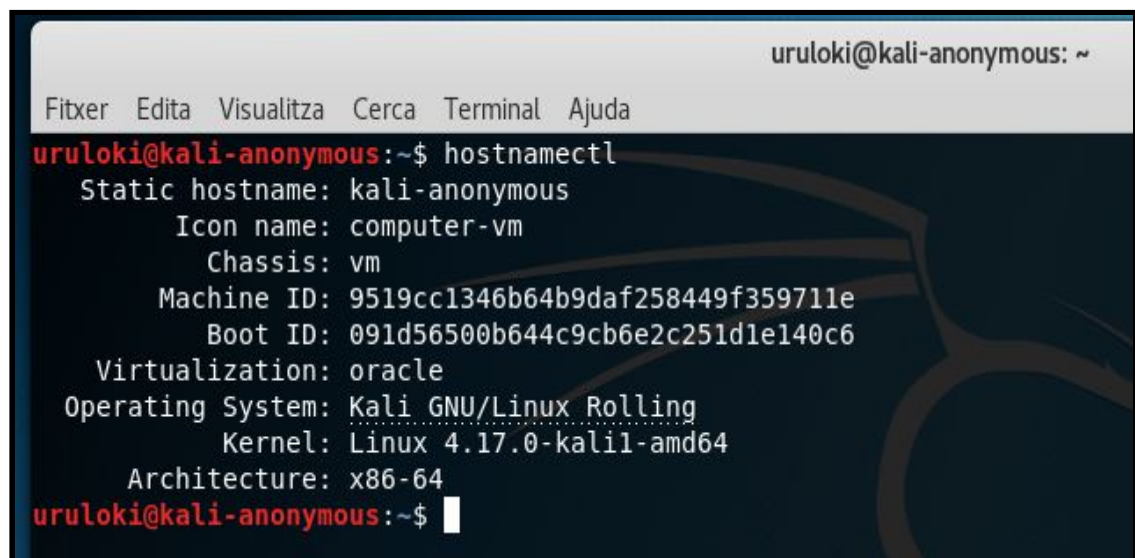
SERVIDOR LINUX

- Nom del host: kali-anonymous
- Sistema Operatiu : Kali GNU/Linux Rolling
- connexió amb adaptador pont (ethernet)
- metode IPv4 automàtic (dhcp)

on tindrà :

- servidor web (port 80 i 443)
- servidor ssh (port 22)
- servidor ftp (port 21)

★ Mostro la versió de la distribució Linux instal·lada



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ hostnamectl  
Static hostname: kali-anonymous  
Icon name: computer-vm  
Chassis: vm  
Machine ID: 9519cc1346b64b9daf258449f359711e  
Boot ID: 091d56500b644c9cb6e2c251d1e140c6  
Virtualization: oracle  
Operating System: Kali GNU/Linux Rolling  
Kernel: Linux 4.17.0-kali1-amd64  
Architecture: x86-64  
uruloki@kali-anonymous:~$
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

★ Mostro l'interfície de xarxa utilitzada i la seva IP

```
uruloki@kali-anonymous: ~/Documents
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~/Documents$ ip a | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    inet 192.168.1.52/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
uruloki@kali-anonymous:~/Documents$
```

★ El nom del host i la seva IP

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ hostname
kali-anonymous
uruloki@kali-anonymous:~$ hostname -I
192.168.1.53
uruloki@kali-anonymous:~$
```

★ Com que hem iniciat la màquina virtual, i no he configurat perquè s'activen al iniciar (per seguretat). Procedeixo a engegar tots els serveis

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo systemctl start ssh
uruloki@kali-anonymous:~$ sudo systemctl start apache2
uruloki@kali-anonymous:~$
uruloki@kali-anonymous:~$ sudo systemctl start vsftpd.service
uruloki@kali-anonymous:~$
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

- ★ Reviso l'estat de tots els serveis, confirmem que estan actius.

```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo systemctl status ssh | grep active  
Active: active (running) since Sat 2019-03-16 12:32:26 CET; 2min 32s ago  
uruloki@kali-anonymous:~$ sudo systemctl status apache2 | grep active  
Active: active (running) since Sat 2019-03-16 12:32:34 CET; 2min 33s ago  
uruloki@kali-anonymous:~$ sudo systemctl status vsftpd.service | grep active  
Active: active (running) since Sat 2019-03-16 12:32:42 CET; 2min 35s ago  
uruloki@kali-anonymous:~$
```

- ★ Reviso que els ports dels serveis activats estan oberts

```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo netstat -atupn  
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      1611/sshd  
tcp6       0      0 :::80                  :::*                    LISTEN      1626/apache2  
tcp6       0      0 :::21                  :::*                    LISTEN      1654/vsftpd  
tcp6       0      0 :::22                  :::*                    LISTEN      1611/sshd  
tcp6       0      0 :::443                 :::*                    LISTEN      1626/apache2  
udp        0      0 0.0.0.0:68             0.0.0.0:*               LISTEN      572/dhclient  
uruloki@kali-anonymous:~$
```

Nom i Cognoms

Arnau Subirós Puigarnau

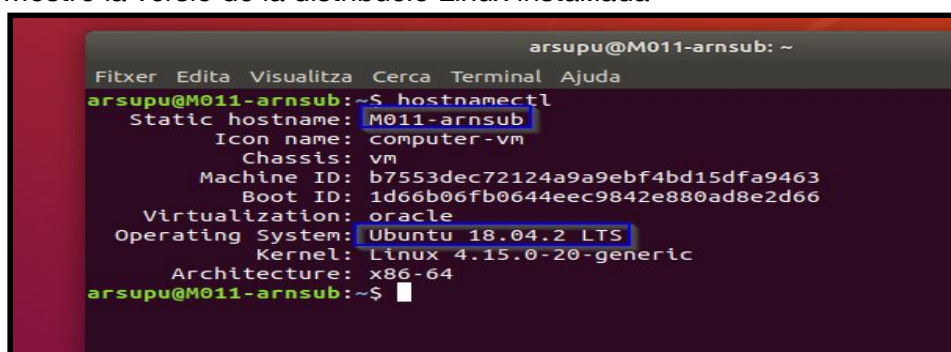
Data

22-03-2019

CLIENT LINUX

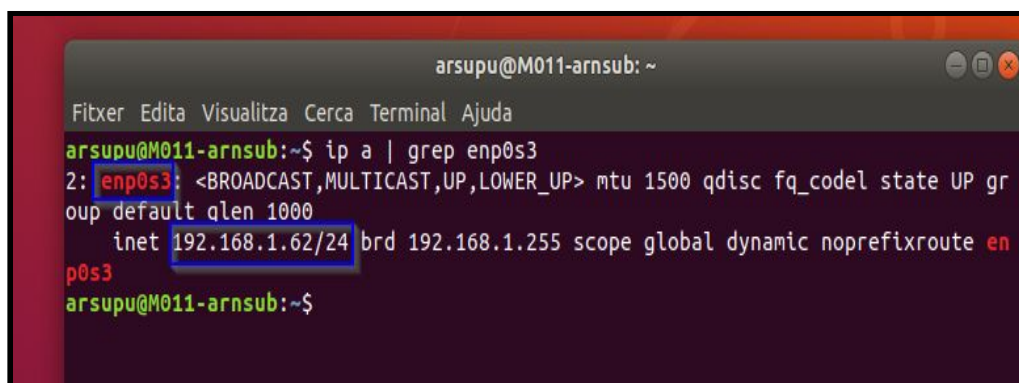
- Nom del host: M011-arnsub
- Sistema Operatiu : Ubuntu 18.04.2 LTS
- connexió amb adaptador pont (ethernet)
- metode IPv4 automàtic (dhcp)

★ Mostro la versió de la distribució Linux instal·lada



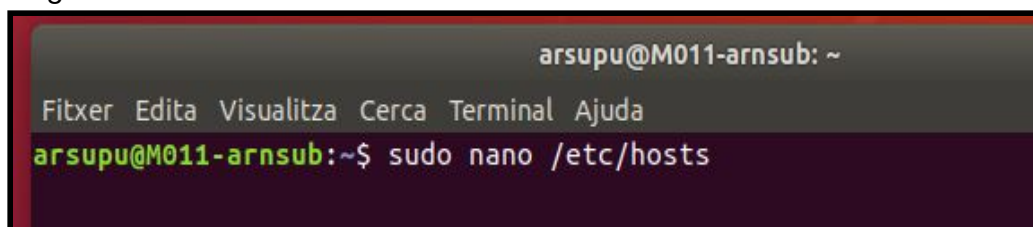
```
arsupu@M011-arnsub: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
arsupu@M011-arnsub:~$ hostnamectl  
Static hostname: M011-arnsub  
Icon name: computer-vm  
Chassis: vm  
Machine ID: b7553dec72124a9a9ebf4bd15dfa9463  
Boot ID: 1d66b06fb0644eec9842e880ad8e2d66  
Virtualization: oracle  
Operating System: Ubuntu 18.04.2 LTS  
Kernel: Linux 4.15.0-20-generic  
Architecture: x86_64  
arsupu@M011-arnsub:~$
```

★ Mostro l'interfície de xarxa utilitzada i la seva IP



```
arsupu@M011-arnsub: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
arsupu@M011-arnsub:~$ ip a | grep enp0s3  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr  
oup default qlen 1000  
    inet 192.168.1.62/24 brd 192.168.1.255 scope global dynamic noprefixroute en  
p0s3  
arsupu@M011-arnsub:~$
```

★ Afegeixo la IP i el nom del host del servidor en l'arxiu /etc/hosts



```
arsupu@M011-arnsub: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
arsupu@M011-arnsub:~$ sudo nano /etc/hosts
```

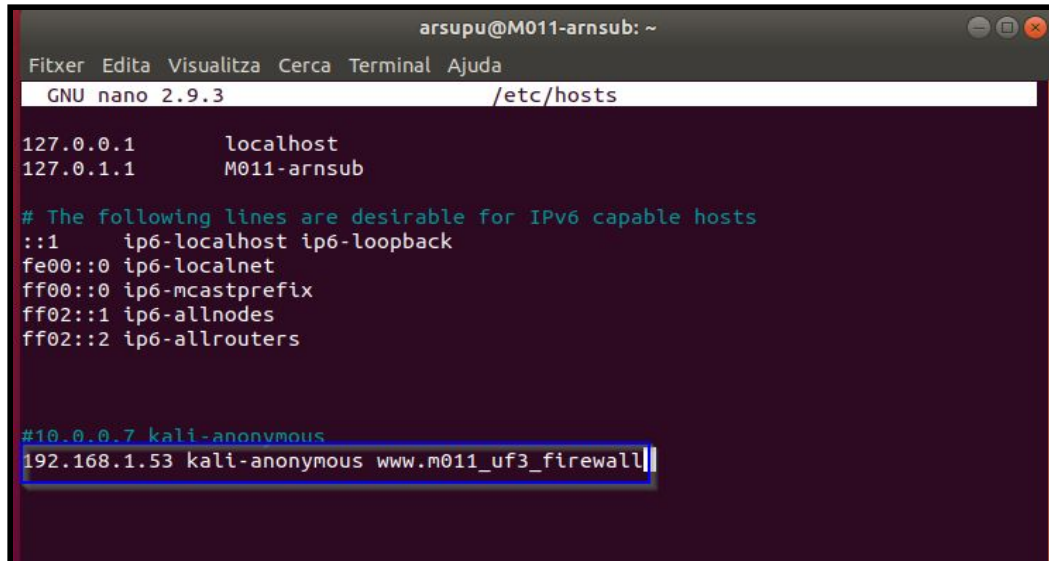

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

He afegit el nom de la pàgina web del servidor



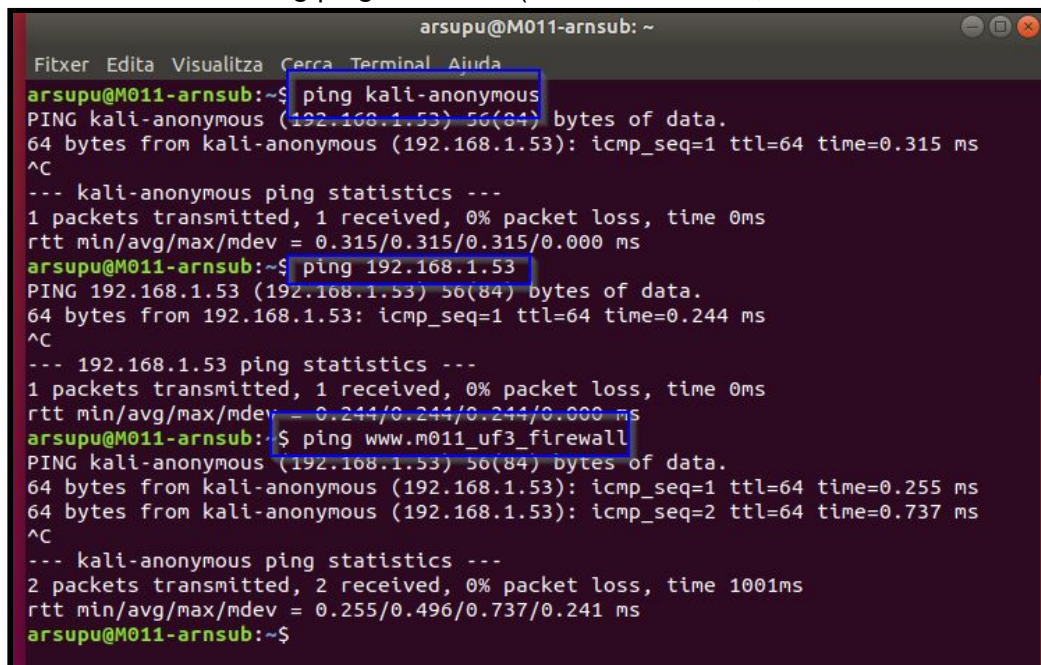
```
arsupu@M011-arndsub: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
GNU nano 2.9.3 /etc/hosts

127.0.0.1    localhost
127.0.1.1    M011-arndsub

# The following lines are desirable for IPv6 capable hosts
::1        ip6-localhost ip6-loopback
fe00::0    ip6-localnet
ff00::0    ip6-mcastprefix
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

#10.0.0.7 kali-anonymous
192.168.1.53 kali-anonymous www.m011_uf3_firewall
```

★ Guardo els canvis i faig ping al servidor(utilitzant : el nom, la seva IP i el seu alias)



```
arsupu@M011-arndsub: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@M011-arndsub:~$ ping kali-anonymous
PING kali-anonymous (192.168.1.53) 56(84) bytes of data.
64 bytes from kali-anonymous (192.168.1.53): icmp_seq=1 ttl=64 time=0.315 ms
^C
--- kali-anonymous ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.315/0.315/0.315/0.000 ms
arsupu@M011-arndsub:~$ ping 192.168.1.53
PING 192.168.1.53 (192.168.1.53) 56(84) bytes of data.
64 bytes from 192.168.1.53: icmp_seq=1 ttl=64 time=0.244 ms
^C
--- 192.168.1.53 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.244/0.244/0.244/0.000 ms
arsupu@M011-arndsub:~$ ping www.m011_uf3_firewall
PING kali-anonymous (192.168.1.53) 56(84) bytes of data.
64 bytes from kali-anonymous (192.168.1.53): icmp_seq=1 ttl=64 time=0.255 ms
64 bytes from kali-anonymous (192.168.1.53): icmp_seq=2 ttl=64 time=0.737 ms
^C
--- kali-anonymous ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.255/0.496/0.737/0.241 ms
arsupu@M011-arndsub:~$
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

2. Realitzem algunes proves desde el Client per confirmar que els serveis funcionen (abans d'utilitzar les IPTables)

- ★ HTTP: Accedeixo a una pàgina web del servidor utilitzant el port 80



- ★ HTTPS: Accedeixo a una pàgina web del servidor utilitzant el port 443



Nom i Cognoms

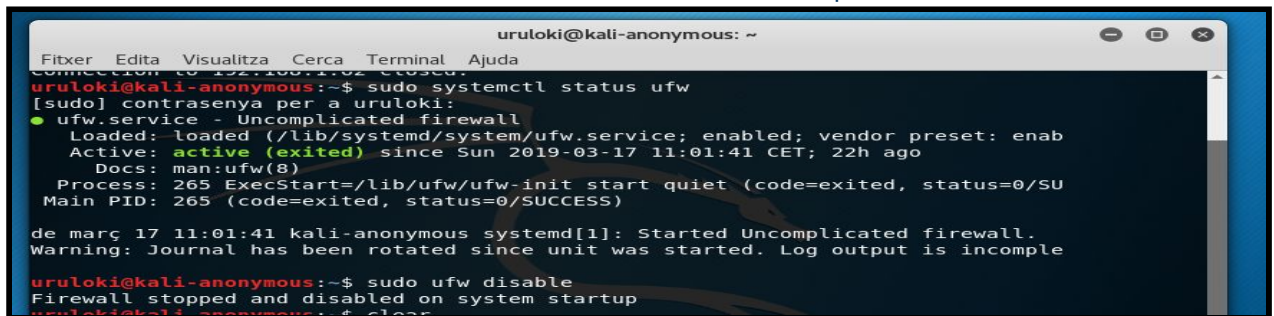
Arnau Subirós Puigarnau

Data

22-03-2019

- ★ SSH: Desde el Client no puc accedir al servidor mitjançant SSH (confirmo que el servei estigui instal·lat. Desde el servidor, si que funciona la connexió SSH al client).

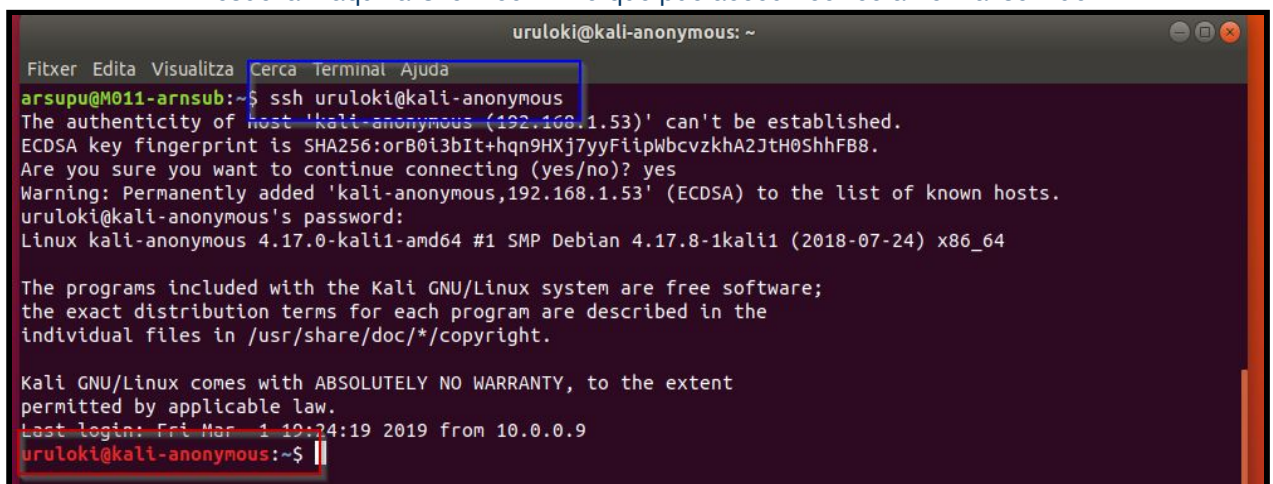
- ☐ Desde el servidor Linux reviso l'estat de UFW i com que està actiu, el desactivo.



```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo systemctl status ufw
[sudo] contrasenya per a uruloki:
● ufw.service - Uncomplicated firewall
   Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enab
   Active: active (exited) since Sun 2019-03-17 11:01:41 CET; 22h ago
     Docs: man:ufw(8)
   Process: 265 ExecStart=/lib/ufw/ufw-init start quiet (code=exited, status=0/SU
   Main PID: 265 (code=exited, status=0/SUCCESS)

de març 17 11:01:41 kali-anonymous systemd[1]: Started Uncomplicated firewall.
Warning: Journal has been rotated since unit was started. Log output is incomple
uruloki@kali-anonymous:~$ sudo ufw disable
Firewall stopped and disabled on system startup
uruloki@kali-anonymous:~$
```

- ☐ Desde la màquina Client confirmo que puc accedir correctament al servidor



```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@M011-arnsub:~$ ssh uruloki@kali-anonymous
The authenticity of host 'kali-anonymous (192.168.1.53)' can't be established.
ECDSA key fingerprint is SHA256:orB0i3bIt+hqn9HXj7yyFilpWbcvzkha2JtH0ShhFB8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'kali-anonymous,192.168.1.53' (ECDSA) to the list of known hosts.
uruloki@kali-anonymous's password:
Linux kali-anonymous 4.17.0-kali1-amd64 #1 SMP Debian 4.17.8-1kali1 (2018-07-24) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Mar 1 10:24:19 2019 from 10.0.0.9
uruloki@kali-anonymous:~$
```

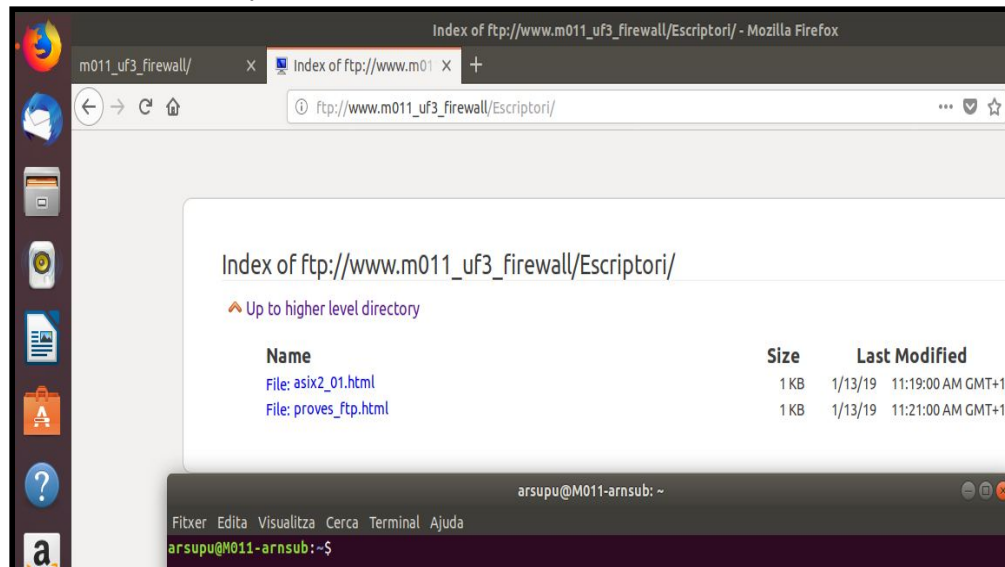
Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

★ FTP: Desde la màquina Client accedeixo al servidor via FTP



Nom i Cognoms

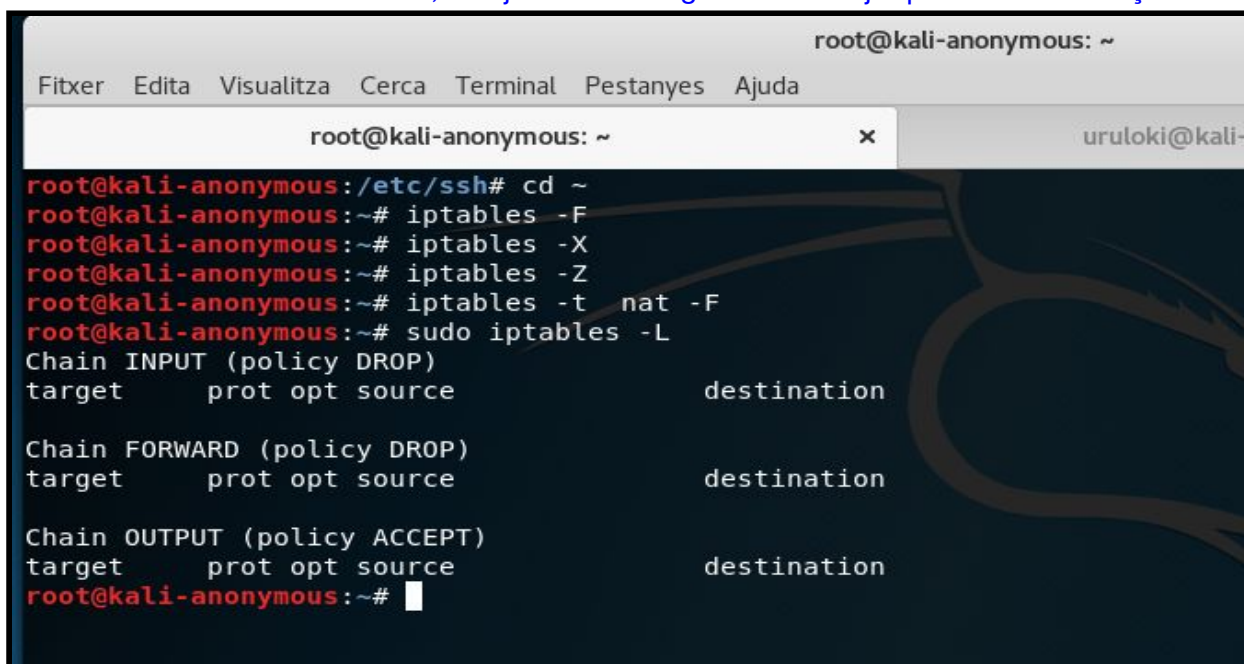
Arnau Subirós Puigarnau

Data

22-03-2019

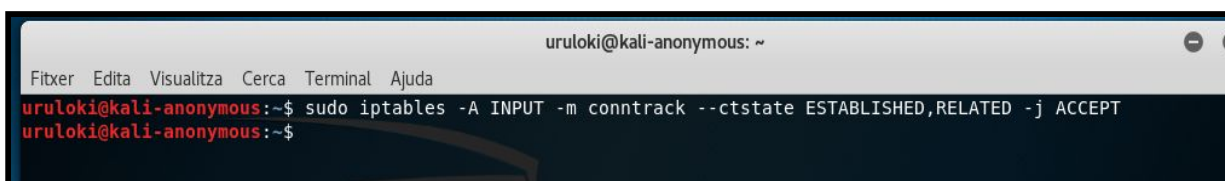
3. Servidor Linux - Configuració de les IPTables:

- **SERVIDOR:** Primer de tot, netejo totes les regles anteriors ja que volem començar de 0.



```
root@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Pestanyes Ajuda  
root@kali-anonymous: ~  
root@kali-anonymous:/etc/ssh# cd ~  
root@kali-anonymous:~# iptables -F  
root@kali-anonymous:~# iptables -X  
root@kali-anonymous:~# iptables -Z  
root@kali-anonymous:~# iptables -t nat -F  
root@kali-anonymous:~# sudo iptables -L  
Chain INPUT (policy DROP)  
target      prot opt source                destination  
  
Chain FORWARD (policy DROP)  
target      prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source                destination  
root@kali-anonymous:~#
```

- **SERVIDOR:** Estableixo una regla per permetre sessions establertes, per tal de permetre la rebuda de trànsit



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  
uruloki@kali-anonymous:~$
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

- **SERVIDOR:** Estableixo una regla per permetre el trànsit d'entrada en el port per defecte de SSH (22) amb connexió TCP

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
uruloki@kali-anonymous:~$
```

- **CLIENT:** Confirmo que puc accedir via SSH

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@M011-arnsub:~$ ssh uruloki@kali-anonymous
uruloki@kali-anonymous's password:
Linux kali-anonymous 4.17.0-kali1-amd64 #1 SMP Debian 4.17.8-1kali1 (2018-07-24) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Mar 18 09:54:06 2019 from 192.168.1.37
uruloki@kali-anonymous:~$
```

- **SERVIDOR :** Reviso les regles actuals

```
uruloki@kali-anonymous:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ufw-before-logging-input all -- anywhere anywhere
ufw-before-input all -- anywhere anywhere
ufw-after-input all -- anywhere anywhere
ufw-after-logging-input all -- anywhere anywhere
ufw-reject-input all -- anywhere anywhere
ufw-track-input all -- anywhere anywhere
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
ACCEPT tcp -- anywhere anywhere tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target prot opt source destination
ufw-before-logging-forward all -- anywhere anywhere
ufw-before-forward all -- anywhere anywhere
```

Nom i Cognoms

Arnau Subirós Puigarnau

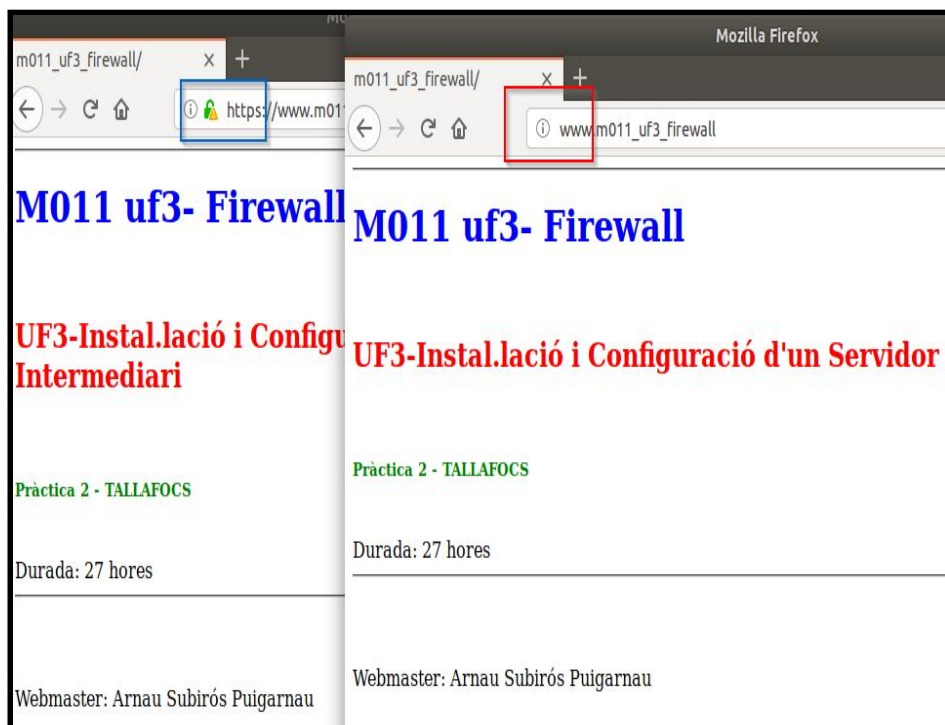
Data

22-03-2019

- **SERVIDOR:** Estableixo unes regles per a habilitar tot el trànsit web HTTP (port 80) i HTTPS (mode segur, port 443):

```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
uruloki@kali-anonymous:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT  
uruloki@kali-anonymous:~$
```

- **CLIENT:** Confirmo que puc accedir a la pàgina web utilitzant el protocol HTTP i HTTPS.



Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

- **SERVIDOR :Reviso les regles actuals**

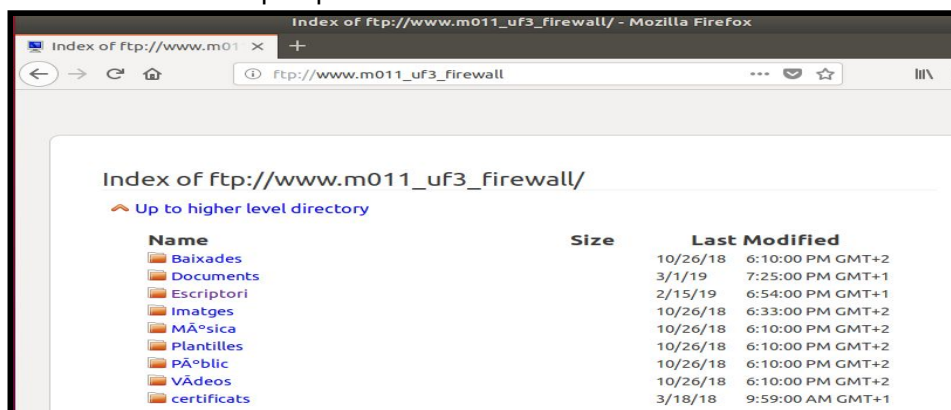
```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ufw-before-logging-input all -- anywhere anywhere
ufw-before-input all -- anywhere anywhere
ufw-after-input all -- anywhere anywhere
ufw-after-logging-input all -- anywhere anywhere
ufw-reject-input all -- anywhere anywhere
ufw-track-input all -- anywhere anywhere
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
ACCEPT tcp -- anywhere anywhere tcp dpt:ssh
ACCEPT tcp -- anywhere anywhere tcp dpt:http
ACCEPT tcp -- anywhere anywhere tcp dpt:https

Chain FORWARD (policy ACCEPT)
target prot opt source destination
ufw-before-logging-forward all -- anywhere anywhere
ufw-before-forward all -- anywhere anywhere
ufw-after-forward all -- anywhere anywhere
ufw-after-logging-forward all -- anywhere anywhere
ufw-reject-forward all -- anywhere anywhere
```

- **SERVIDOR: Estableixo una regla per permetre el trànsit d'entrada en el port per defecte de FTP (21) amb connexió TCP**

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT
uruloki@kali-anonymous:~$
```

- **CLIENT :Confirmo que puc accedir al servidor via FTP**



Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

- **SERVIDOR :Reviso les regles actuals**

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ufw-before-logging-input all -- anywhere anywhere
ufw-before-input all -- anywhere anywhere
ufw-after-input all -- anywhere anywhere
ufw-after-logging-input all -- anywhere anywhere
ufw-reject-input all -- anywhere anywhere
ufw-track-input all -- anywhere anywhere
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
ACCEPT tcp -- anywhere anywhere tcp dpt:ssh
ACCEPT tcp -- anywhere anywhere tcp dpt:http
ACCEPT tcp -- anywhere anywhere tcp dpt:https
ACCEPT tcp -- anywhere anywhere tcp dpt:ftp
Chain FORWARD (policy ACCEPT)
target prot opt source destination
ufw-before-logging-forward all -- anywhere anywhere
ufw-before-forward all -- anywhere anywhere
```

- **SERVIDOR :Un cop s'ha pres la decisió d'acceptar un paquet, no hi ha altres regles que l'afectin. Les regles d'acceptar SSH i WEB són les primeres de totes, i la regla per bloquejar tota la resta de trànsit ha de venir després. A continuació haig de crear una regla per bloquejar-ho tot al final de tot (posteriorment confirmarem que no tenim accés via telnet)**

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo iptables -A INPUT -j DROP
uruloki@kali-anonymous:~$
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

- **SERVIDOR** : Intento establir connexió sense èxit amb el client via Telnet

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ telnet 192.168.1.62
Trying 192.168.1.62...
telnet: Unable to connect to remote host: Connection refused
uruloki@kali-anonymous:~$
```

- **CLIENT** : Intento establir connexió sense èxit amb el servidor via Telnet

```
arsupu@M011-arnsub: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@M011-arnsub:~$ telnet 192.168.1.53
Trying 192.168.1.53...
telnet: Unable to connect to remote host: Connection timed out
arsupu@M011-arnsub:~$ telnet 192.168.1.53
Trying 192.168.1.53...
GET /HTTP/1.1
Host:www.m011_uf3_firewall
User-Agent: telnet
```

- **SERVIDOR** :Reviso les regles actuals

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ufw-before-logging-input all -- anywhere anywhere
ufw-before-input all -- anywhere anywhere
ufw-after-input all -- anywhere anywhere
ufw-after-logging-input all -- anywhere anywhere
ufw-reject-input all -- anywhere anywhere
ufw-track-input all -- anywhere anywhere
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
ACCEPT tcp -- anywhere anywhere tcp dpt:ssh
ACCEPT tcp -- anywhere anywhere tcp dpt:http
ACCEPT tcp -- anywhere anywhere tcp dpt:https
ACCEPT tcp -- anywhere anywhere tcp dpt:ftp
DROP all -- anywhere anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination
ufw-before-logging-forward all -- anywhere anywhere
ufw-before-forward all -- anywhere anywhere
ufw-after-forward all -- anywhere anywhere
ufw-after-logging-forward all -- anywhere anywhere
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

- **SERVIDOR** : L'únic problema amb la nostra configuració fins al moment és que fins i tot el port de loopback està bloquejat. Una de les opcions seria afegir una regla pel loopback, però abans que el trànsit estic bloquejat, insertar-la com la primera regla i que sigui la primera en processar.

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo iptables -I INPUT 1 -i lo -j ACCEPT
[sudo] contrasenya per a uruloki:
uruloki@kali-anonymous:~$
```

- **SERVIDOR** :Reviso les regles actuals però afegirem *-v* per veure més detalls (interfície loopback)

```
uruloki@kali-anonymous:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source    destination
  0      0 ACCEPT     all  --  lo      any      anywhere  anywhere
14654  39M ufw-before-logging-input all  --  any     any     anywhere  anywhere
14654  39M ufw-before-input all  --  any     any     anywhere  anywhere
6993  9209K ufw-after-input all  --  any     any     anywhere  anywhere
6888  9200K ufw-after-logging-input all  --  any     any     anywhere  anywhere
6888  9200K ufw-reject-input all  --  any     any     anywhere  anywhere
6888  9200K ufw-track-input all  --  any     any     anywhere  anywhere
1181  6281K ACCEPT     all  --  any     any     anywhere  anywhere             ctstate RELATED,ESTABLISHED
  3    1264 ACCEPT     tcp  --  any     any     anywhere  anywhere             tcp dpt:ssh
  0      0 ACCEPT     tcp  --  any     any     anywhere  anywhere             tcp dpt:http
  0      0 ACCEPT     tcp  --  any     any     anywhere  anywhere             tcp dpt:https
  2    120 ACCEPT     tcp  --  any     any     anywhere  anywhere             tcp dpt:ftp
204  9416 DROP       all  --  any     any     anywhere  anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

- **SERVIDOR** Com que no utilitzem l'interfície eth0, podem configurar una regla(en la 2 posició) per bloquejar el transit en aquesta interfície.

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo iptables -I INPUT 2 -i eth0 -j DROP
uruloki@kali-anonymous:~$
```

- **SERVIDOR** :Revisem les regles actuals

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 2 100 ACCEPT all -- lo any anywhere anywhere
23 1084 DROP all -- eth0 any anywhere anywhere
14726 40M ufw-before-logging-input all -- any any anywhere anywhere anywhere
14726 40M ufw-before-input all -- any any anywhere anywhere anywhere
7065 9212K ufw-after-input all -- any any anywhere anywhere anywhere
6960 9203K ufw-after-logging-input all -- any any anywhere anywhere anywhere
6960 9203K ufw-reject-input all -- any any anywhere anywhere anywhere
6960 9203K ufw-track-input all -- any any anywhere anywhere anywhere
1182 6281K ACCEPT all -- any any anywhere anywhere ctstate RELATED,ESTABLISHED
 3 1264 ACCEPT tcp -- any any anywhere anywhere tcp dpt:ssh
 0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:http
 0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:https
 2 120 ACCEPT tcp -- any any anywhere anywhere tcp dpt:ftp
275 12312 DROP all -- any any anywhere anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
```

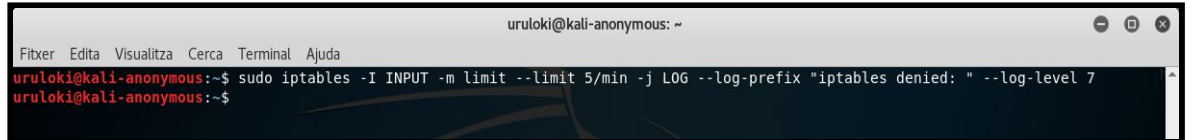

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

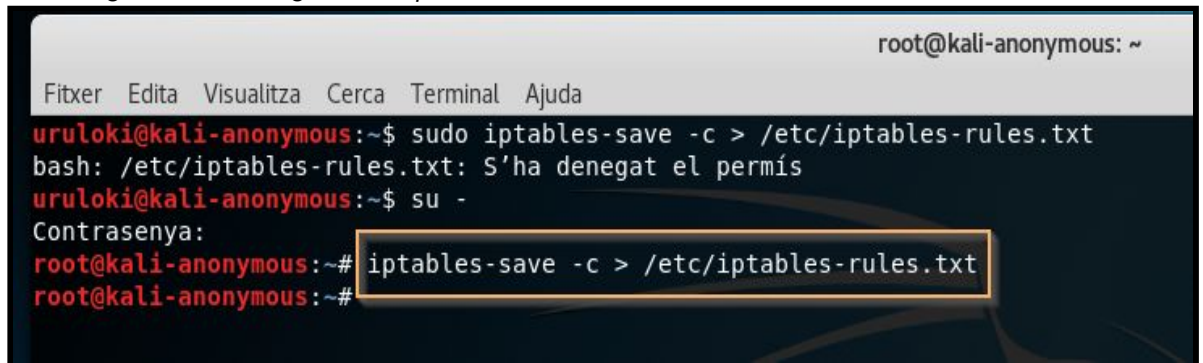
- **SERVIDOR** : Ara hauré d'emmagatzemar els paquets dropped en el syslog



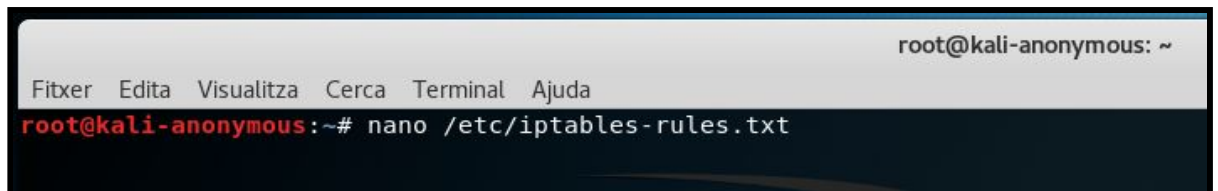
```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables -I INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7  
uruloki@kali-anonymous:~$
```

- **SERVIDOR** : Si hagués de reiniciar la màquina virtual , ara mateix, la configuració de les iptables desapareixeria, per tant es molt important guardar la configuració. Utilitzant iptables-save (guardar) i iptables-restore(restaurar)

si volem guardar la configuració d'iptables



```
root@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo iptables-save -c > /etc/iptables-rules.txt  
bash: /etc/iptables-rules.txt: S'ha denegat el permís  
uruloki@kali-anonymous:~$ su -  
Contrasenya:  
root@kali-anonymous:~# iptables-save -c > /etc/iptables-rules.txt  
root@kali-anonymous:~#
```



```
root@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
root@kali-anonymous:~# nano /etc/iptables-rules.txt
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

```

root@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
GNU nano 2.9.8 /etc/iptables-rules.txt

# Generated by iptables-save v1.6.2 on Mon Mar 18 11:51:26 2019
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [188:24266]
:ufw-after-forward - [0:0]
:ufw-after-input - [0:0]
:ufw-after-logging-forward - [0:0]
:ufw-after-logging-input - [0:0]
:ufw-after-logging-output - [0:0]
:ufw-after-output - [0:0]

```

```

root@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
GNU nano 2.9.8 /etc/iptables-rules.txt

:ufw-track-forward - [0:0]
:ufw-track-input - [0:0]
:ufw-track-output - [0:0]
[81:2948] -A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7
[2:100] -A INPUT -i lo -j ACCEPT
[102:4098] -A INPUT -i eth0 -j DROP
[15018:40569828] -A INPUT -j ufw-before-logging-input
[15018:40569828] -A INPUT -j ufw-before-input
[7357:10279892] -A INPUT -j ufw-after-input
[7252:10270312] -A INPUT -j ufw-after-logging-input
[7252:10270312] -A INPUT -j ufw-reject-input
[7252:10270312] -A INPUT -j ufw-track-input
[1395:7345413] -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
[3:1264] -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
[0:0] -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
[0:0] -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
[2:120] -A INPUT -p tcp -m tcp --dport 21 -j ACCEPT
[354:15326] -A INPUT -j DROP
[0:0] -A FORWARD -j ufw-before-logging-forward

```


Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

si volem restaurar la configuració d'iptables

```
root@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
root@kali-anonymous:~# iptables-restore -c < /etc/iptables-rules.txt
```

- **SERVIDOR** : Utilizo un dels mètodes perquè les regles que hem guardat estiguin disponibles al iniciar el sistema editant el fitxer /etc/network/interfaces.

```
root@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
Firefox ESR -anonymous:~# nano /etc/network/interfaces  
root@kali-anonymous:~#
```

```
root@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
GNU nano 2.9.8 /etc/network/interfaces  
  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
Fixers /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
iface eth1 inet dhcp  
    pre-up iptables-restore < /etc/iptables.rules  
    post-down iptables-restore < /etc/iptables.downrules
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

22-03-2019

- **SERVIDOR :** Utilitzo l'eina nmap per veure els ports oberts del client i del servidor.

```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo nmap -sS 192.168.1.53/24  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-18 12:21 CET  
█
```

```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
  
Nmap scan report for 192.168.1.62  
Host is up (0.00037s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
MAC Address: 08:00:27:A6:18:7D (Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 192.168.1.53  
Host is up (0.0000070s latency).  
Not shown: 996 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.60 seconds
```