



JESUÏTES El Clot
Escola del Clot

M011-SEGURETAT INFORMÀTICA i ALTA SEGURETAT

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

PRÀCTICA 2 : DE TALLAFOCS

Curs: 2018-19

CFGs: ASIX2

Alumne : Arnau Subirós Puigarnau

Data : 17-02-2019

Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

PRACTICA 2 :

De Tallafocs

En aquesta pràctica provarem el filtratge de paquets utilitzant l'aplicació ufw – Uncomplicated Firewall, que és l'eina per defecte de configuració del firewall en sistemes Ubuntu. Es va desenvolupar amb la idea de fer fàcil la configuració de les iptables. ufw proporciona una manera amigable de crear un servidor firewall IPv4 o IPv6.

EXERCICI 1 – 80%

L'objectiu és provar diferents regles del firewall i realitzar filtratge de paquets. Es pot treballar per parelles: una màquina té diferents serveis (ssh, https, telnet, mysql, i altres serveis que heu estudiat en el cicle); i l'altra màquina farà de prova).

Activa el logging. Després instal·la gufw i veuràs com de forma gràfica i senzilla també podem fer les mateixes accions.

S'ha d'entregar la documentació de les proves realitzades, amb les captures de pantalla necessàries i suficients per demostrar la realització de la pràctica.

Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

COMPROVACIONS PREVIES

1. Host **SERVIDOR: kali-anonymous (Kali Linux)**

Abans de fer proves amb el UFW actiu, revisem la IP del SERVIDOR.

- He creat una IP estàtica : 192.168.1.130/24 amb xarxa interna

```
uruloki@kali-anonymous: /etc/ufw
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/etc/ufw$ clear
uruloki@kali-anonymous:/etc/ufw$ ip a | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    inet 192.168.1.130/24 brd 192.168.1.255 scope global noprefixroute eth0
uruloki@kali-anonymous:/etc/ufw$
```

- A continuació en aquesta màquina hi ha instal·lats varies servidors que utilitzarà el host client. Revisem que tots els serveis estiguin actius(i en cas contrari,activar-los)
 - SSH (port 22)
 - FTP (port 21)
 - APACHE (port 80 i 443)
 - CUPS(port 631)

❖ El servidor apache està actiu

```
uruloki@kali-anonymous: /var/www/html/m011
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/var/www/html/m011$ sudo systemctl status apache2
[sudo] contrasenya per a uruloki:
● apache2.service - The Apache HTTP Server
   loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2019-02-15 18:44:22 CET; 21min ago
     Process: 12010 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
     Process: 12015 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 12019 (apache2)
      Tasks: 8 (limit: 2352)
   ..

```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

❖ El servidor FTP està actiu

```
uruloki@kali-anonymous: /var/www/html/m011
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/var/www/html/m011$ sudo systemctl status vsftpd.service
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2019-02-15 13:15:33 CET; 5h 51min ago
     Main PID: 7769 (vsftpd)
        Tasks: 1 (limit: 2352)
       Memory: 528.0K
      CGroup: /system.slice/vsftpd.service
              └─7769 /usr/sbin/vsftpd /etc/vsftpd.conf

de febr. 15 13:15:33 kali-anonymous systemd[1]: Starting vsftpd FTP server...
de febr. 15 13:15:33 kali-anonymous systemd[1]: Started vsftpd FTP server.
uruloki@kali-anonymous:/var/www/html/m011$
```

❖ El servidor SSH està actiu

```
uruloki@kali-anonymous: /var/www/html/m011
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/var/www/html/m011$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2019-02-15 13:08:35 CET; 6h ago
     Docs: man:sshd(8)
           man:ssh_config(5)
    Process: 11288 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
    Process: 11282 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
     Main PID: 7050 (sshd)
        Tasks: 1 (limit: 2352)
```

❖ El servidor CUPS està actiu

```
uruloki@kali-anonymous: /var/www/html/m011
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/var/www/html/m011$ sudo systemctl status cups
● cups.service - CUPS Scheduler
   Loaded: loaded (/lib/systemd/system/cups.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2019-02-15 13:18:35 CET; 5h 54min ago
     Docs: man:cupsd(8)
    Main PID: 10492 (cupsd)
        Tasks: 1 (limit: 2352)
       Memory: 2.6M
      CGroup: /system.slice/cups.service
              └─10492 /usr/sbin/cupsd -l

de febr. 15 13:18:35 kali-anonymous systemd[1]: Started CUPS Scheduler.
uruloki@kali-anonymous:/var/www/html/m011$
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

- I revisem que aquests serveis tinguin correctament oberts els ports abans comentats

```
uruloki@kali-anonymous: /var/www/html/m011
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/var/www/html/m011$ 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      7050/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      10492/cupsd
tcp6       0      0 :::80                  :::*                   LISTEN      12019/apache2
tcp6       0      0 :::21                  :::*                   LISTEN      7769/vsftpd
tcp6       0      0 :::22                  :::*                   LISTEN      7050/sshd
tcp6       0      0 :::1:631               :::*                   LISTEN      10492/cupsd
tcp6       0      0 :::443                 :::*                   LISTEN      12019/apache2
uruloki@kali-anonymous:/var/www/html/m011$
```

2. Host CLIENT: ubuntu-asix2 (Ubuntu)

Revisem les configuracions amb el host Client

- He creat una IP estàtica : 192.168.1.4/24 amb xarxa interna

```
arsupu@ubuntu-asix2: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~$ ip a | grep enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    inet 192.168.1.4/24 brd 192.168.1.255 scope global noprefixroute enp0s3
arsupu@ubuntu-asix2:~$
```

- Revisem l'arxiu hosts i afegim la IP del servidor i el nom del host i la pagina web

```
arsupu@ubuntu-asix2: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
GNU nano 2.9.3 /etc/hosts Modificat
127.0.0.1    localhost
127.0.1.1    ubuntu-asix2

# 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

192.168.1.130 kali-anonymous www.m011-uf3-firewall
```

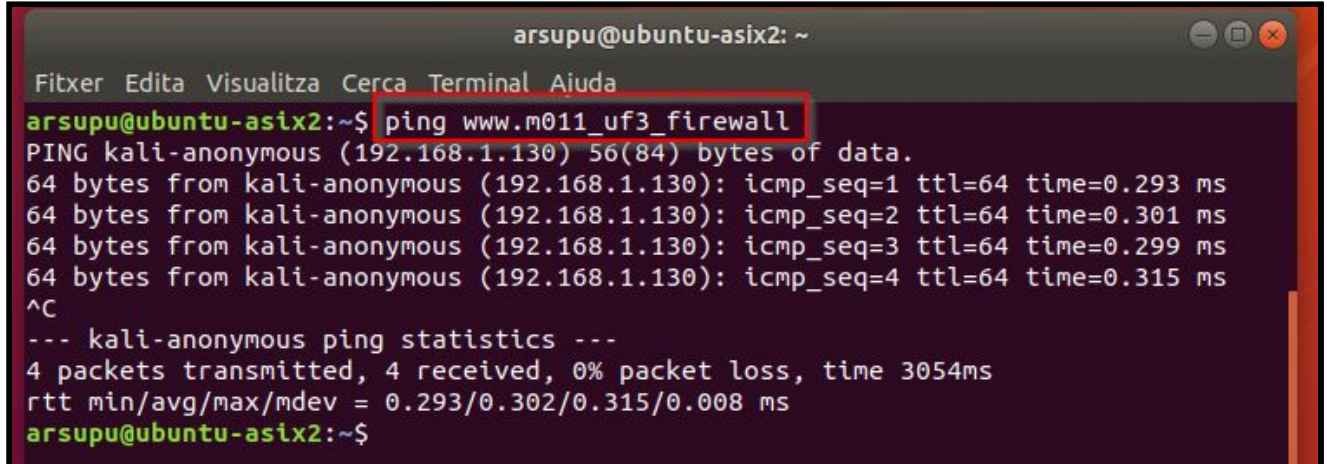

Nom i Cognoms

Arnau Subirós Puigarnau

Data

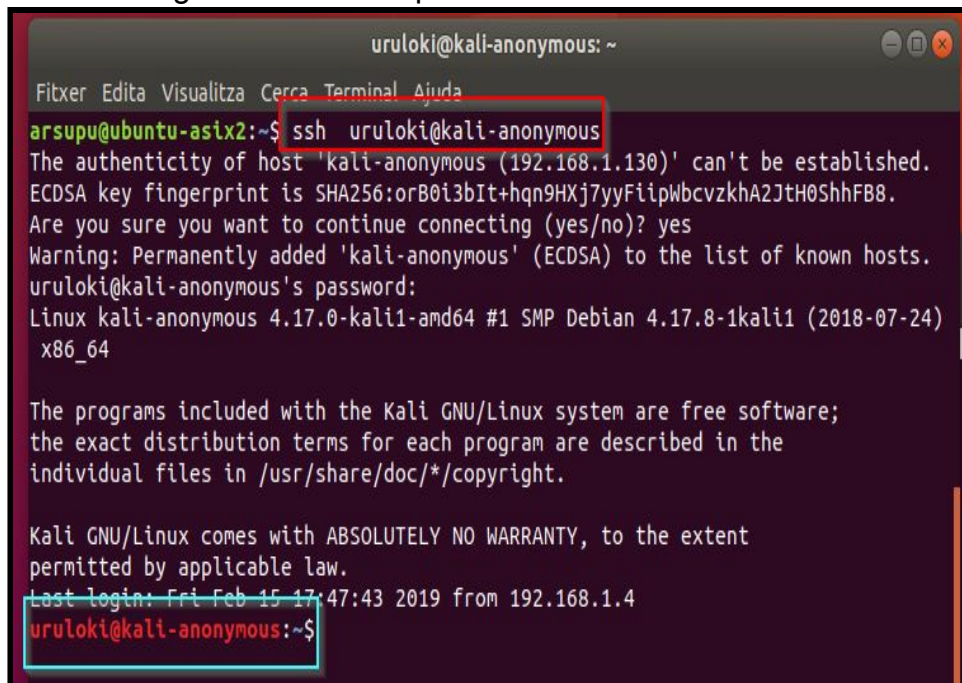
17-02-2019

- Farem ping al nom de la pàgina web del servidor.



```
arsupu@ubuntu-asix2: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
arsupu@ubuntu-asix2:~$ ping www.m011_uf3_firewall  
PING kali-anonymous (192.168.1.130) 56(84) bytes of data.  
64 bytes from kali-anonymous (192.168.1.130): icmp_seq=1 ttl=64 time=0.293 ms  
64 bytes from kali-anonymous (192.168.1.130): icmp_seq=2 ttl=64 time=0.301 ms  
64 bytes from kali-anonymous (192.168.1.130): icmp_seq=3 ttl=64 time=0.299 ms  
64 bytes from kali-anonymous (192.168.1.130): icmp_seq=4 ttl=64 time=0.315 ms  
^C  
--- kali-anonymous ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3054ms  
rtt min/avg/max/mdev = 0.293/0.302/0.315/0.008 ms  
arsupu@ubuntu-asix2:~$
```

- Un cop això abans d'activar el FIREWALL farem un parell de comprovacions:
 - Desde el host client confirmem que podem establir una connexió segura utilitzant el protocol SSH



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
arsupu@ubuntu-asix2:~$ ssh uruloki@kali-anonymous  
The authenticity of host 'kali-anonymous (192.168.1.130)' can't be established.  
ECDSA key fingerprint is SHA256:orB0i3bIt+hqn9HXj7yyFiipWbcvzkha2JtH0ShhFB8.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'kali-anonymous' (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 Feb 15 17:47:43 2019 from 192.168.1.4  
uruloki@kali-anonymous:~$
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

- Desde el host client confirmem que podem accedir a la pàgina web de prova del servidor.



Nom i Cognoms

Arnau Subirós Puigarnau

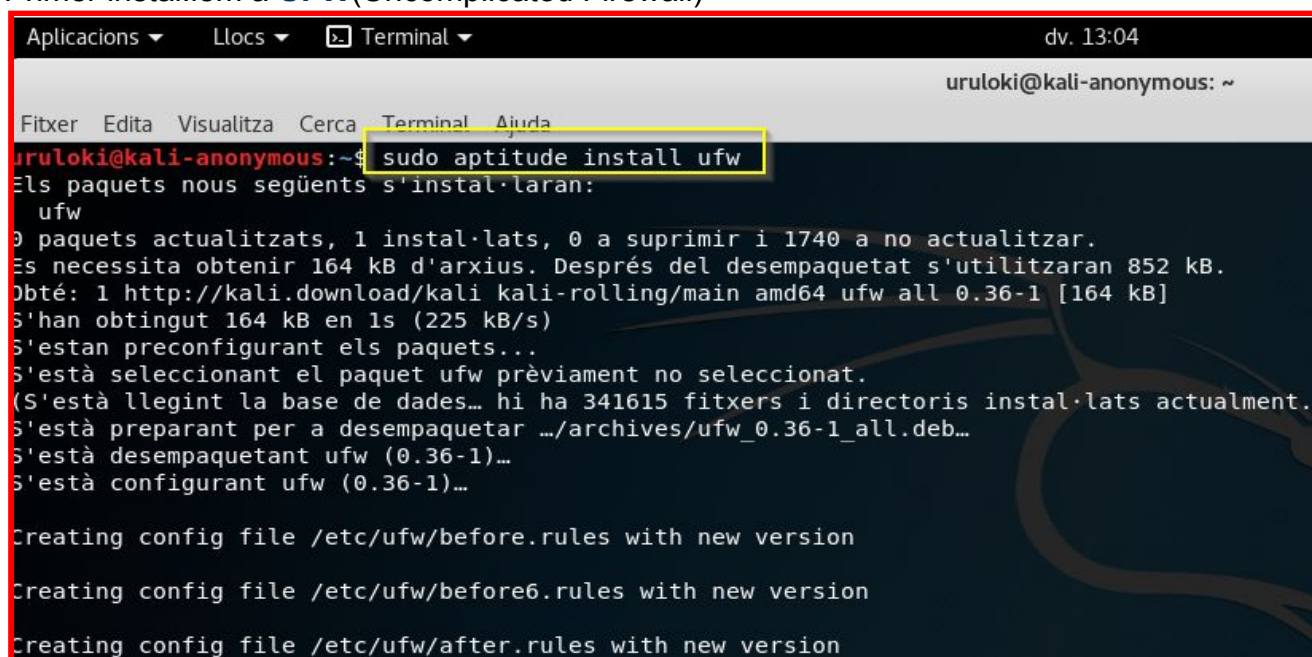
Data

17-02-2019

REALITZACIÓ DE LA PRÀCTICA

SERVIDOR (màquina Kali Linux): On instal·larem el firewall i tindrà instal·lats tots els serveis

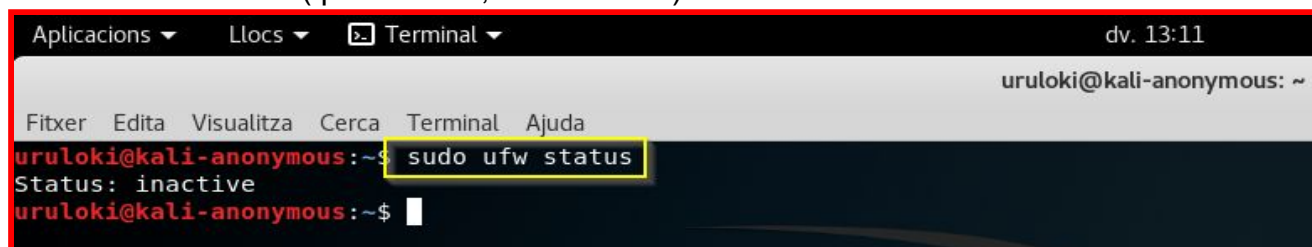
Primer instal·lem a **UFW**(Uncomplicated Firewall)



```
uruloki@kali-anonymous:~$ sudo aptitude install ufw
Els paquets nous següents s'instal·laran:
  ufw
0 paquets actualitzats, 1 instal·lats, 0 a suprimir i 1740 a no actualitzar.
Es necessita obtenir 164 kB d'arxius. Després del desempaquetat s'utilitzaran 852 kB.
Obté: 1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36-1 [164 kB]
S'han obtingut 164 kB en 1s (225 kB/s)
S'estan preconfigurant els paquets...
S'està seleccionant el paquet ufw prèviament no seleccionat.
(S'està llegint la base de dades... hi ha 341615 fitxers i directoris instal·lats actualment...)
S'està preparant per a desempaquetar ../archives/ufw_0.36-1_all.deb...
S'està desempaquetant ufw (0.36-1)...
S'està configurant ufw (0.36-1)...

Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
```

Revisem el seu estat(per defecte, estar inactiu)



```
uruloki@kali-anonymous:~$ sudo ufw status
Status: inactive
uruloki@kali-anonymous:~$
```

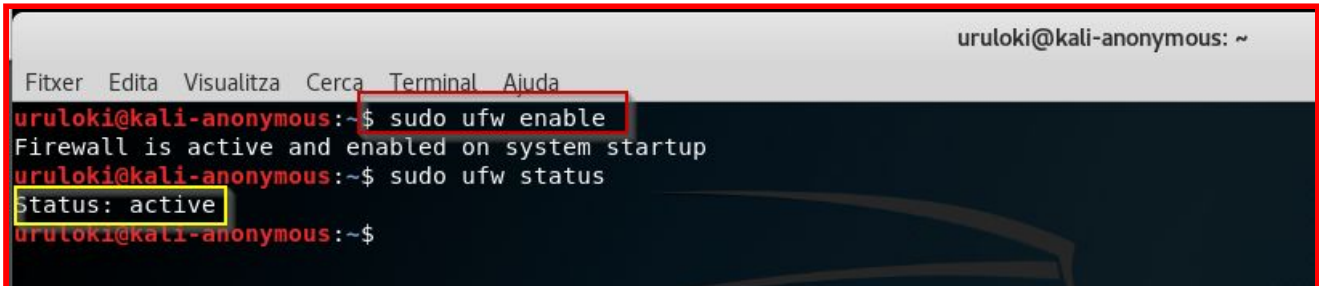

Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

Activem **UFW**(Uncomplicated Firewall) i seguidament revisem el seu status.

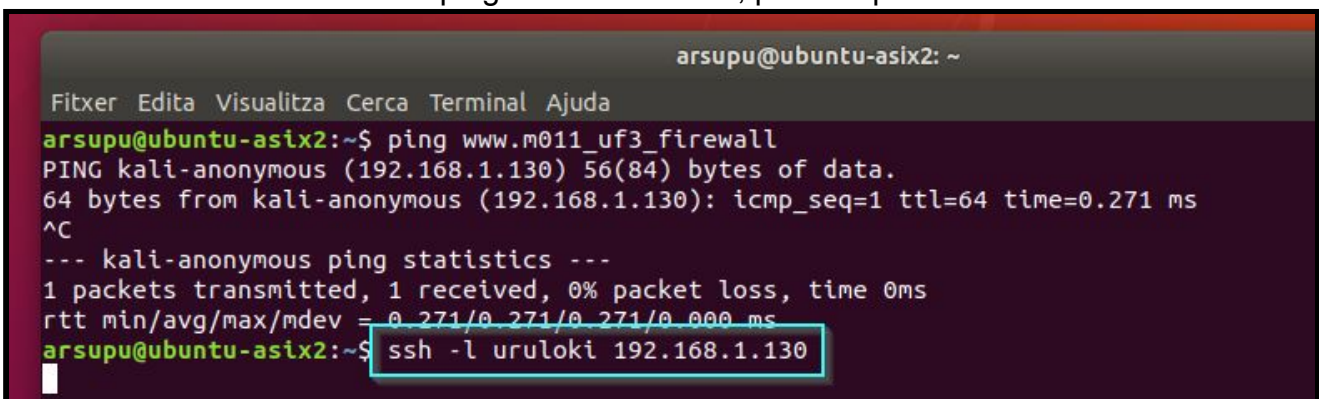


```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
uruloki@kali-anonymous:~$ sudo ufw status  
Status: active  
uruloki@kali-anonymous:~$
```

Al activar UFW s'activen les regles predefinides . Revisem amb el host client si ara podem establir connexio amb el servidor amb el protocol SSH i si podem accedir a la seva pagina web.

CLIENT (màquina Ubuntu)

- Fem correctament ping amb el servidor , però no podem establir-hi connexió SSH



```
arsupu@ubuntu-asix2: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
arsupu@ubuntu-asix2:~$ ping www.m011_uf3_firewall  
PING kali-anonymous (192.168.1.130) 56(84) bytes of data.  
64 bytes from kali-anonymous (192.168.1.130): icmp_seq=1 ttl=64 time=0.271 ms  
^C  
--- kali-anonymous ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.271/0.271/0.271/0.000 ms  
arsupu@ubuntu-asix2:~$ ssh -l uruloki 192.168.1.130
```

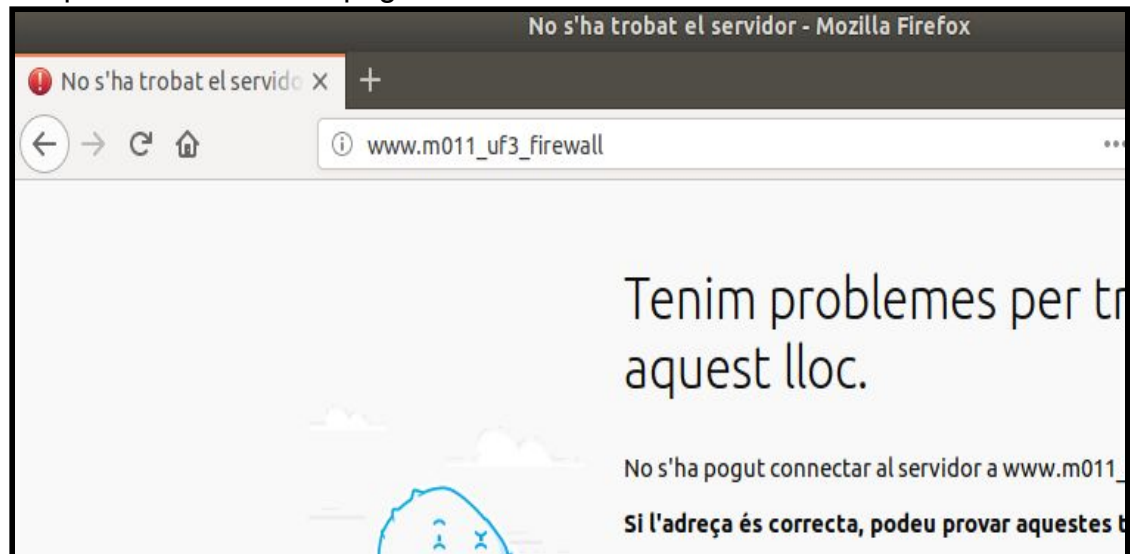
Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

- No podem accedir a la pàgina web del servidor



SERVIDOR (màquina Kali Linux):

- Habilitem l'accés al port 22 (SSH)

```
uruloki@kali-anonymous: ~  
Fitxer  Editar  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo ufw allow 22  
Rule added  
Rule added (v6)  
uruloki@kali-anonymous:~$
```

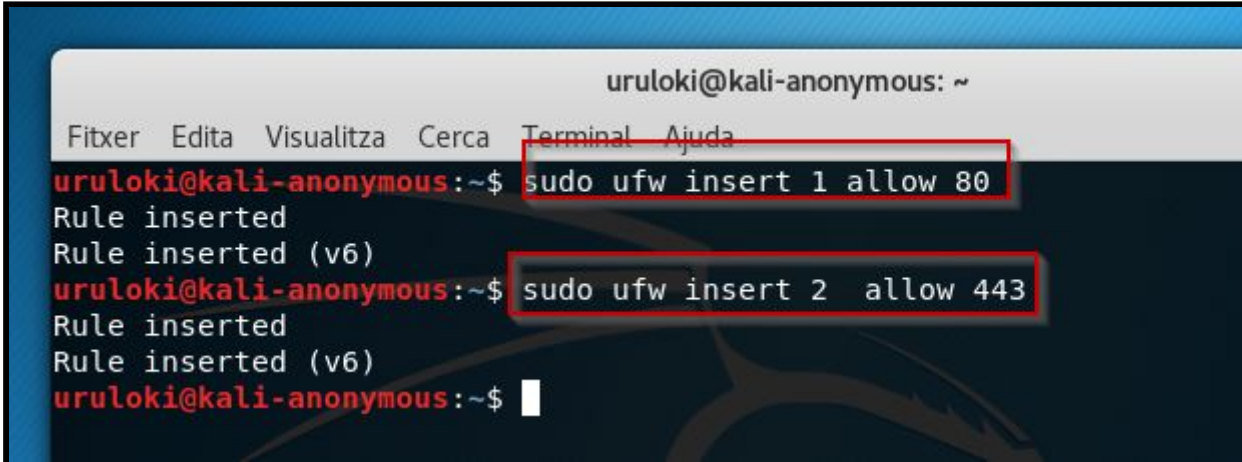
Nom i Cognoms

Arnau Subirós Puigarnau

Data

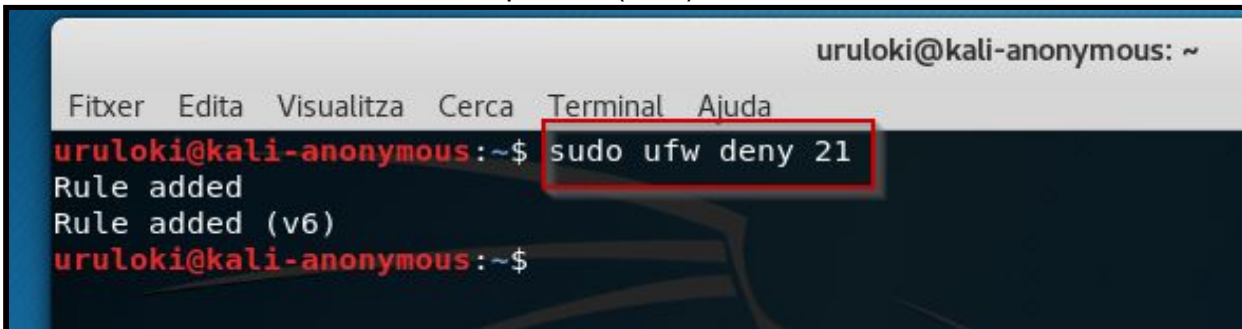
17-02-2019

- Habilitem el port 80 i el port 443(HTTP i HTTPS) utilitzant regles predefinides



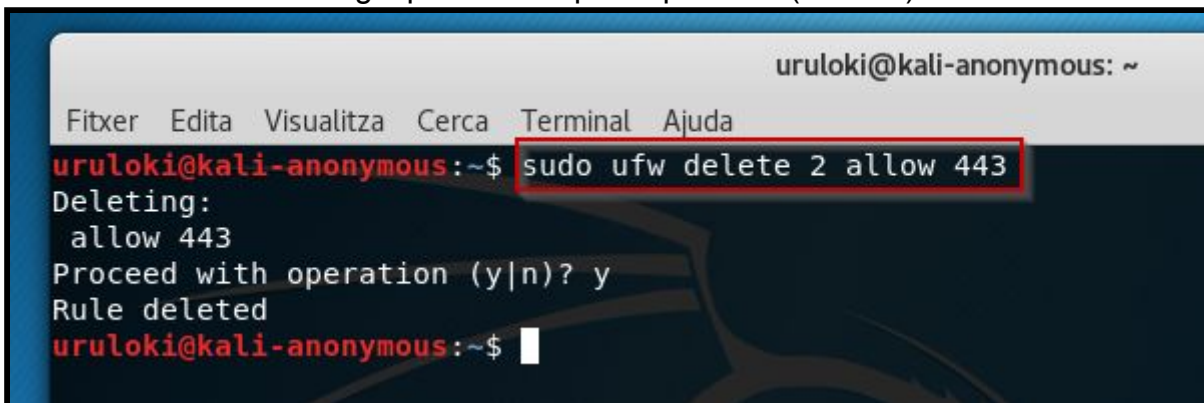
```
uruloki@kali-anonymous: ~  
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo ufw insert 1 allow 80  
Rule inserted  
Rule inserted (v6)  
uruloki@kali-anonymous:~$ sudo ufw insert 2 allow 443  
Rule inserted  
Rule inserted (v6)  
uruloki@kali-anonymous:~$
```

- Deshabilitem l'accés al port 21 (FTP)



```
uruloki@kali-anonymous: ~  
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo ufw deny 21  
Rule added  
Rule added (v6)  
uruloki@kali-anonymous:~$
```

- Eliminem la regla per accedir per el port 443 (HTTPS)



```
uruloki@kali-anonymous: ~  
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo ufw delete 2 allow 443  
Deleting:  
allow 443  
Proceed with operation (y|n)? y  
Rule deleted  
uruloki@kali-anonymous:~$
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

- Eliminem la regla per accedir per el port 22 (SSH)

```
uruloki@kali-anonymous: ~  
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo ufw delete 1 deny 22  
Deleting:  
  allow 22  
Proceed with operation (y|n)? y  
Rule deleted  
uruloki@kali-anonymous:~$
```

- Hem eliminat la regla anterior ja que la volem personalitzar només amb l'IP del host client (Ubuntu)

```
uruloki@kali-anonymous: ~  
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo ufw allow proto tcp from 192.168.1.4 to any port 22  
Rule added  
uruloki@kali-anonymous:~$
```

- Mirem l'estat de les regles actives de UFW

```
uruloki@kali-anonymous: ~  
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo ufw status  
Status: active  
  
To Action From  
-- -- --  
21 DENY Anywhere  
80 ALLOW Anywhere  
22/tcp ALLOW 192.168.1.4  
80 (v6) ALLOW Anywhere (v6)  
443 (v6) ALLOW Anywhere (v6)  
22 (v6) ALLOW Anywhere (v6)  
21 (v6) DENY Anywhere (v6)  
  
uruloki@kali-anonymous:~$
```

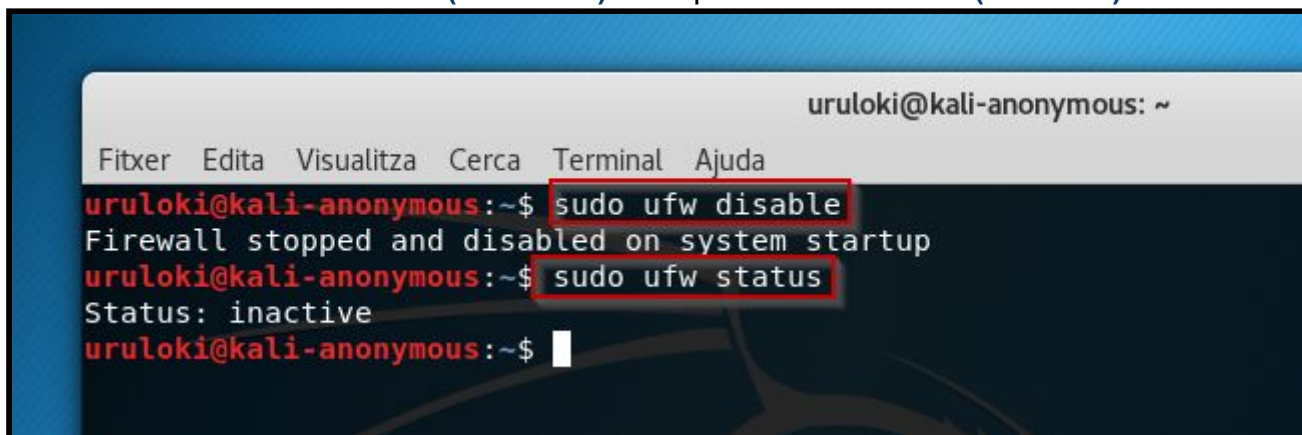

Nom i Cognoms

Arnau Subirós Puigarnau

Data

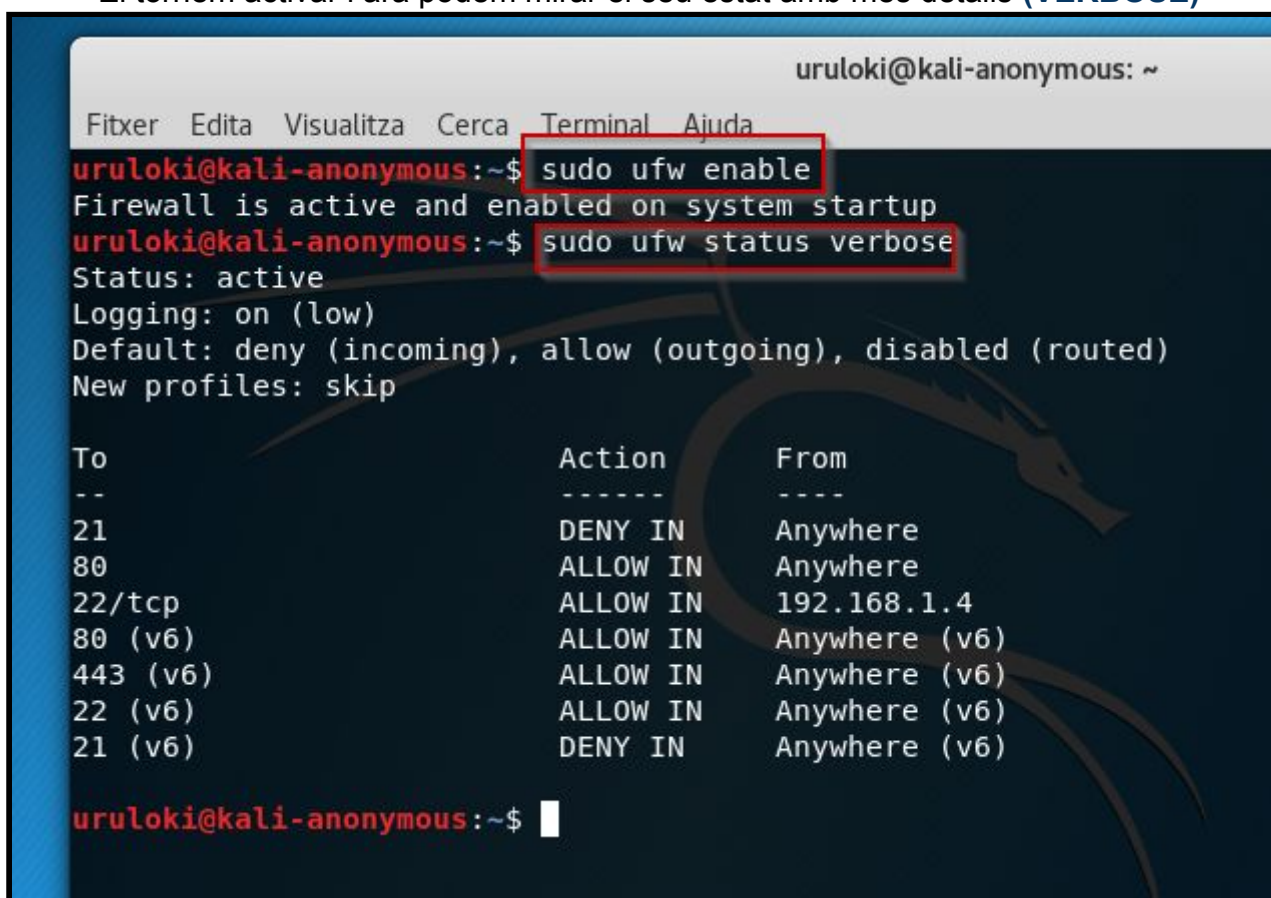
17-02-2019

- Podem desactivar-lo(**DISABLE**) i comprovant el seu estat(**STATUS**)



```
uruloki@kali-anonymous: ~  
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo ufw disable  
Firewall stopped and disabled on system startup  
uruloki@kali-anonymous:~$ sudo ufw status  
Status: inactive  
uruloki@kali-anonymous:~$
```

- El tornem activar i ara podem mirar el seu estat amb més detalls (**VERBOSE**)



```
uruloki@kali-anonymous: ~  
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda  
uruloki@kali-anonymous:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
uruloki@kali-anonymous:~$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
  
To Action From  
--  
21 DENY IN Anywhere  
80 ALLOW IN Anywhere  
22/tcp ALLOW IN 192.168.1.4  
80 (v6) ALLOW IN Anywhere (v6)  
443 (v6) ALLOW IN Anywhere (v6)  
22 (v6) ALLOW IN Anywhere (v6)  
21 (v6) DENY IN Anywhere (v6)  
  
uruloki@kali-anonymous:~$
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

- Podem veure el seu status amb el format numerat (**NUMBERED**)

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo ufw status numbered
Status: active

      To Action From
      --
[ 1] 21 DENY IN Anywhere
[ 2] 80 ALLOW IN Anywhere
[ 3] 22/tcp ALLOW IN 192.168.1.4
[ 4] 80 (v6) ALLOW IN Anywhere (v6)
[ 5] 443 (v6) ALLOW IN Anywhere (v6)
[ 6] 22 (v6) ALLOW IN Anywhere (v6)
[ 7] 21 (v6) DENY IN Anywhere (v6)

uruloki@kali-anonymous:~$
```

- En aquests exemples, els ports els conec però n'hi ha molts, però això en cas de dubte es pot recórrer a l'arxiu `/etc/services` on estan els ports assignats per la IANA

```
uruloki@kali-anonymous: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~$ sudo cat /etc/services more
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from http://www.iana.org/assignments/port-numbers and other
# sources like http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services .
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux      1/tcp          # TCP port service multiplexer
echo        7/tcp
echo        7/udp
discard     9/tcp          sink null
discard     9/udp          sink null
sysstat     11/tcp
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
qotd        17/tcp          quote
msp         18/tcp          # message send protocol
msp         18/udp
chargen     19/tcp          ttytst source

--More--
```

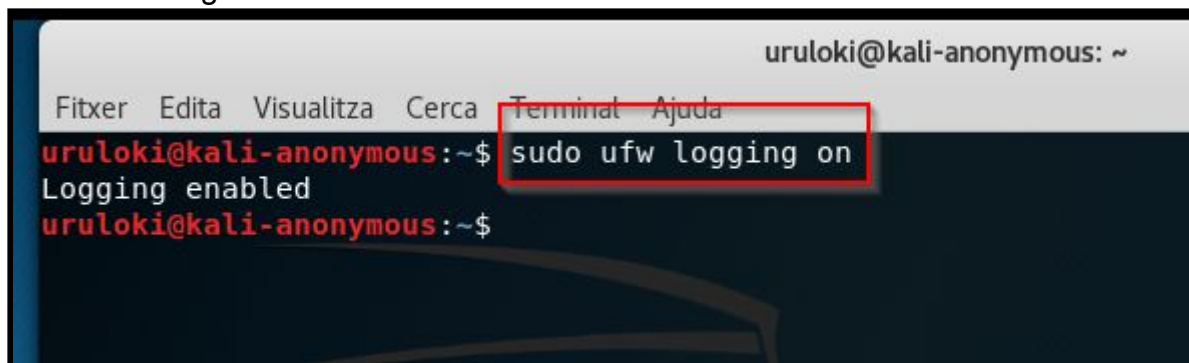
Nom i Cognoms

Arnau Subirós Puigarnau

Data

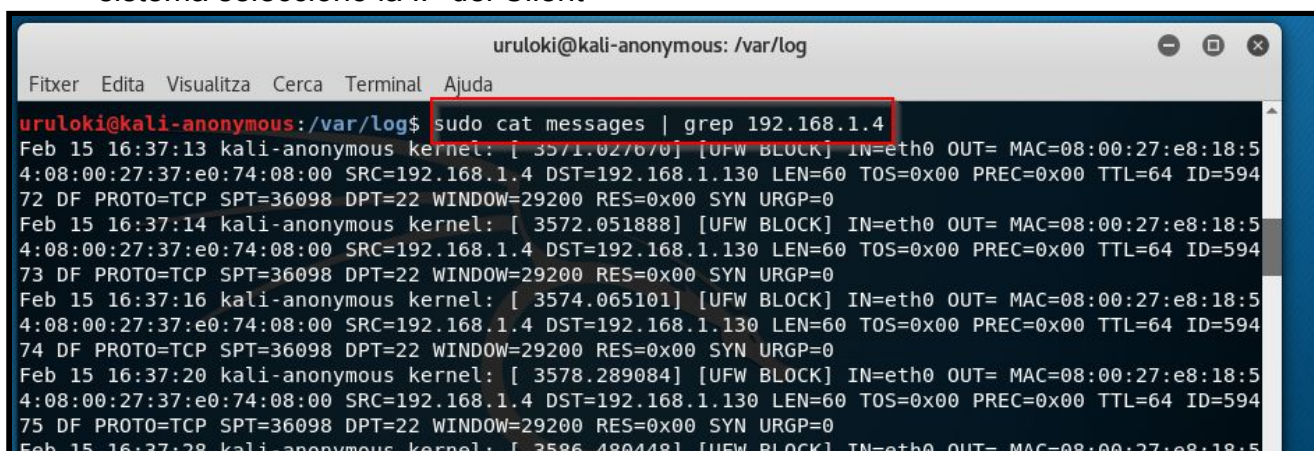
17-02-2019

- Activem els logs de UFW



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo ufw logging on  
Logging enabled  
uruloki@kali-anonymous:~$
```

- En l'arxiu `/var/logs` hi han els logs del UFW, en el meu cas per filtrar dels del sistema selecciono la IP del Client



```
uruloki@kali-anonymous: /var/log  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:/var/log$ sudo cat messages | grep 192.168.1.4  
Feb 15 16:37:13 kali-anonymous kernel: [ 3571.027670] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5  
4:08:00:27:37:e0:74:08:00 SRC=192.168.1.4 DST=192.168.1.130 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=594  
72 DF PROTO=TCP SPT=36098 DPT=22 WINDOW=29200 RES=0x00 SYN URGP=0  
Feb 15 16:37:14 kali-anonymous kernel: [ 3572.051888] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5  
4:08:00:27:37:e0:74:08:00 SRC=192.168.1.4 DST=192.168.1.130 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=594  
73 DF PROTO=TCP SPT=36098 DPT=22 WINDOW=29200 RES=0x00 SYN URGP=0  
Feb 15 16:37:16 kali-anonymous kernel: [ 3574.065101] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5  
4:08:00:27:37:e0:74:08:00 SRC=192.168.1.4 DST=192.168.1.130 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=594  
74 DF PROTO=TCP SPT=36098 DPT=22 WINDOW=29200 RES=0x00 SYN URGP=0  
Feb 15 16:37:20 kali-anonymous kernel: [ 3578.289084] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5  
4:08:00:27:37:e0:74:08:00 SRC=192.168.1.4 DST=192.168.1.130 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=594  
75 DF PROTO=TCP SPT=36098 DPT=22 WINDOW=29200 RES=0x00 SYN URGP=0  
Feb 15 16:37:28 kali-anonymous kernel: [ 3586.480418] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5
```


Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

- En l'arxiu **/var/syslog** hi han els logs del UFW, en el meu cas per filtrar dels del sistema selecciono la IP del Client

```
uruloki@kali-anonymous: /var/log
Fitxer Edita Visualitza Cerca Terminal Ajuda

uruloki@kali-anonymous:/var/log$ sudo cat syslog | grep 192.168.1.4
Feb 15 16:37:13 kali-anonymous kernel: [ 3571.027670] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5
4:08:00:27:37:e0:74:08:00 SRC=192.168.1.4 DST=192.168.1.130 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=594
72 DF PROTO=TCP SPT=36098 DPT=22 WINDOW=29200 RES=0x00 SYN URGP=0
Feb 15 16:37:14 kali-anonymous kernel: [ 3572.051888] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5
4:08:00:27:37:e0:74:08:00 SRC=192.168.1.4 DST=192.168.1.130 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=594
73 DF PROTO=TCP SPT=36098 DPT=22 WINDOW=29200 RES=0x00 SYN URGP=0
Feb 15 16:37:16 kali-anonymous kernel: [ 3574.065101] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5
4:08:00:27:37:e0:74:08:00 SRC=192.168.1.4 DST=192.168.1.130 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=594
74 DF PROTO=TCP SPT=36098 DPT=22 WINDOW=29200 RES=0x00 SYN URGP=0
```

- En l'arxiu **/var/kern.log** hi han els logs del UFW, en el meu cas per filtrar dels del sistema selecciono la IP del Client

```
uruloki@kali-anonymous: /var/log
Fitxer Edita Visualitza Cerca Terminal Ajuda

uruloki@kali-anonymous:/var/log$ sudo cat kern.log | grep 192.168.1.4
Feb 15 16:37:13 kali-anonymous kernel: [ 3571.027670] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5
4:08:00:27:37:e0:74:08:00 SRC=192.168.1.4 DST=192.168.1.130 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=594
72 DF PROTO=TCP SPT=36098 DPT=22 WINDOW=29200 RES=0x00 SYN URGP=0
Feb 15 16:37:14 kali-anonymous kernel: [ 3572.051888] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5
4:08:00:27:37:e0:74:08:00 SRC=192.168.1.4 DST=192.168.1.130 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=594
73 DF PROTO=TCP SPT=36098 DPT=22 WINDOW=29200 RES=0x00 SYN URGP=0
Feb 15 16:37:16 kali-anonymous kernel: [ 3574.065101] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5
4:08:00:27:37:e0:74:08:00 SRC=192.168.1.4 DST=192.168.1.130 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=594
74 DF PROTO=TCP SPT=36098 DPT=22 WINDOW=29200 RES=0x00 SYN URGP=0
Feb 15 16:37:20 kali-anonymous kernel: [ 3578.289084] [UFW BLOCK] IN=eth0 OUT= MAC=08:00:27:e8:18:5
4:08:00:27:37:e0:74:08:00 SRC=192.168.1.4 DST=192.168.1.130 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=594
```

- I en l'arxiu **/var/ufw.log** hi han els logs del UFW

```
uruloki@kali-anonymous: /var/log
Fitxer Edita Visualitza Cerca Terminal Ajuda

uruloki@kali-anonymous:/var/log$ sudo cat ufw.log | more
Feb 15 16:25:19 kali-anonymous kernel: [ 2857.132646] [UFW BLOCK] IN=eth0 OUT= MAC=33:33:00:00:00:0
1:08:00:27:5d:2f:09:86:dd SRC=fe80:0000:0000:0000:0a00:27ff:fe5d:2f09 DST=ff02:0000:0000:0000:0000:0000:0001 LEN=64 TC=0 HOPLIMIT=1 FLOWLBL=601201 PROTO=UDP SPT=8612 DPT=8612 LEN=24
Feb 15 16:25:19 kali-anonymous kernel: [ 2857.132702] [UFW BLOCK] IN=eth0 OUT= MAC=33:33:00:00:00:0
1:08:00:27:5d:2f:09:86:dd SRC=fe80:0000:0000:0000:0a00:27ff:fe5d:2f09 DST=ff02:0000:0000:0000:0000:0000:0001 LEN=64 TC=0 HOPLIMIT=1 FLOWLBL=237779 PROTO=UDP SPT=8612 DPT=8610 LEN=24
Feb 15 16:25:19 kali-anonymous kernel: [ 2857.143121] [UFW BLOCK] IN=eth0 OUT= MAC=33:33:00:00:00:0
1:08:00:27:5d:2f:09:86:dd SRC=fe80:0000:0000:0000:0a00:27ff:fe5d:2f09 DST=ff02:0000:0000:0000:0000:0000:0001 LEN=64 TC=0 HOPLIMIT=1 FLOWLBL=601201 PROTO=UDP SPT=8612 DPT=8612 LEN=24
Feb 15 16:25:19 kali-anonymous kernel: [ 2857.143179] [UFW BLOCK] IN=eth0 OUT= MAC=33:33:00:00:00:0
```


Nom i Cognoms

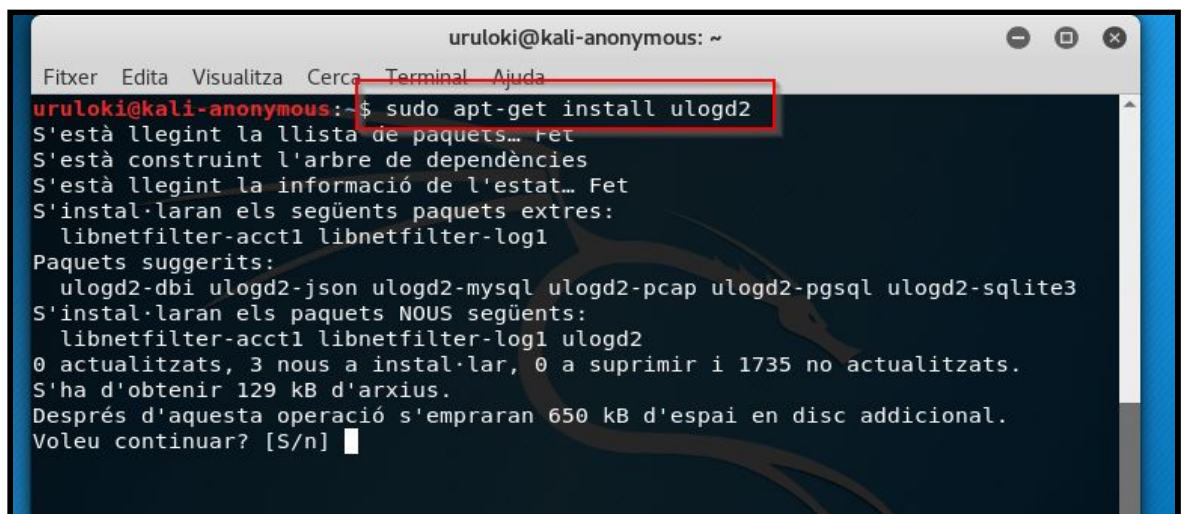
Arnau Subirós Puigarnau

Data

17-02-2019

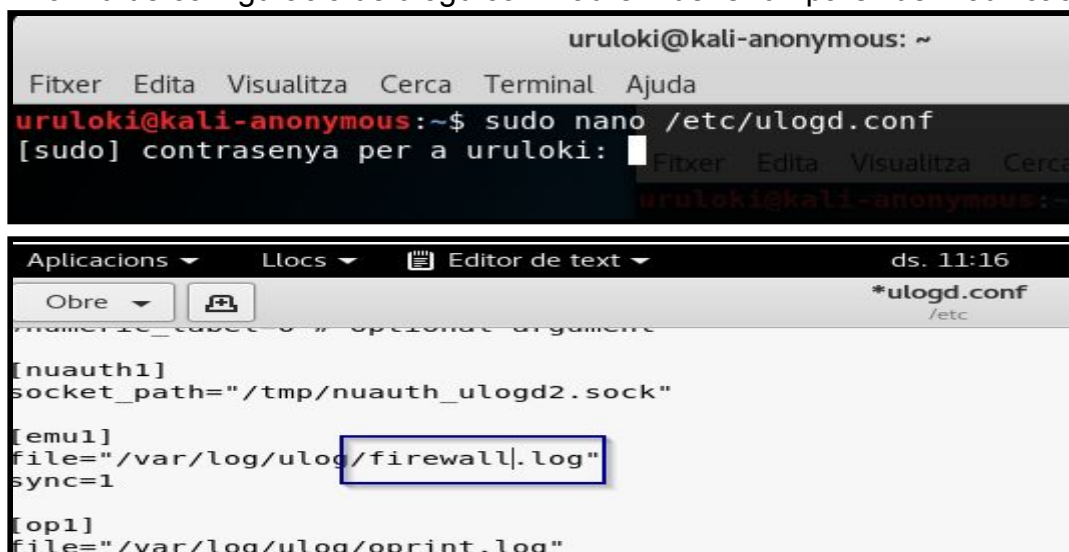
Això vol dir que es barregen missatges generals del sistema, com missatges del nucli o altres serveis. (en **/var/log/messages** , **var/log/syslog**, **/var/log/kern.log**)

Per diferenciar els esdeveniments del tallafocs, es recomana instal·lar el programa **ulogd2**, el qual s'encarrega de rebre els missatges del tallafocs, millor dit, els missatges de registre de LOG del tallafocs i els envia a un arxiu individual, per exemple: **/var/log/firewall.log** el qual serà mantingut de forma independent a registre del dimoni syslog.



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo apt-get install ulogd2  
S'està llegint la llista de paquets... Fet  
S'està construint l'arbre de dependències  
S'està llegint la informació de l'estat... Fet  
S'instal·laran els següents paquets extres:  
  libnetfilter-acct1 libnetfilter-log1  
Paquets suggerits:  
  ulogd2-dbi ulogd2-json ulogd2-mysql ulogd2-pcap ulogd2-pgsql ulogd2-sqlite3  
S'instal·laran els paquets NOUS següents:  
  libnetfilter-acct1 libnetfilter-log1 ulogd2  
0 actualitzats, 3 nous a instal·lar, 0 a suprimir i 1735 no actualitzats.  
S'ha d'obtenir 129 kB d'arxius.  
Després d'aquesta operació s'empraran 650 kB d'espai en disc addicional.  
Voleu continuar? [S/n]
```

- A l'arxiu de configuració de ulogd.conf haurem de fer un parell de modificacions



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo nano /etc/ulogd.conf  
[sudo] contrasenya per a uruloki:  
uruloki@kali-anonymous: ~  
Aplicacions ▾ Llocs ▾ Editor de text ▾ ds. 11:16  
*ulogd.conf /etc  
#numeric_label=0 # optional argument  
[nuauth1]  
socket_path="/tmp/nuauth_ulogd2.sock"  
[emu1]  
file="/var/log/ulog/firewall.log"  
sync=1  
[op1]  
file="/var/log/ulog/oprint.log"
```

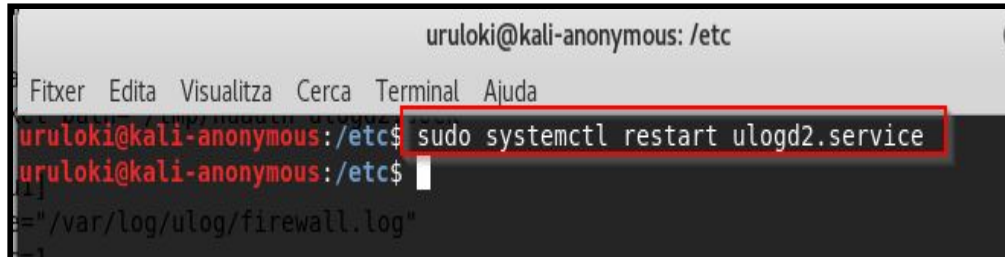
Nom i Cognoms

Arnau Subirós Puigarnau

Data

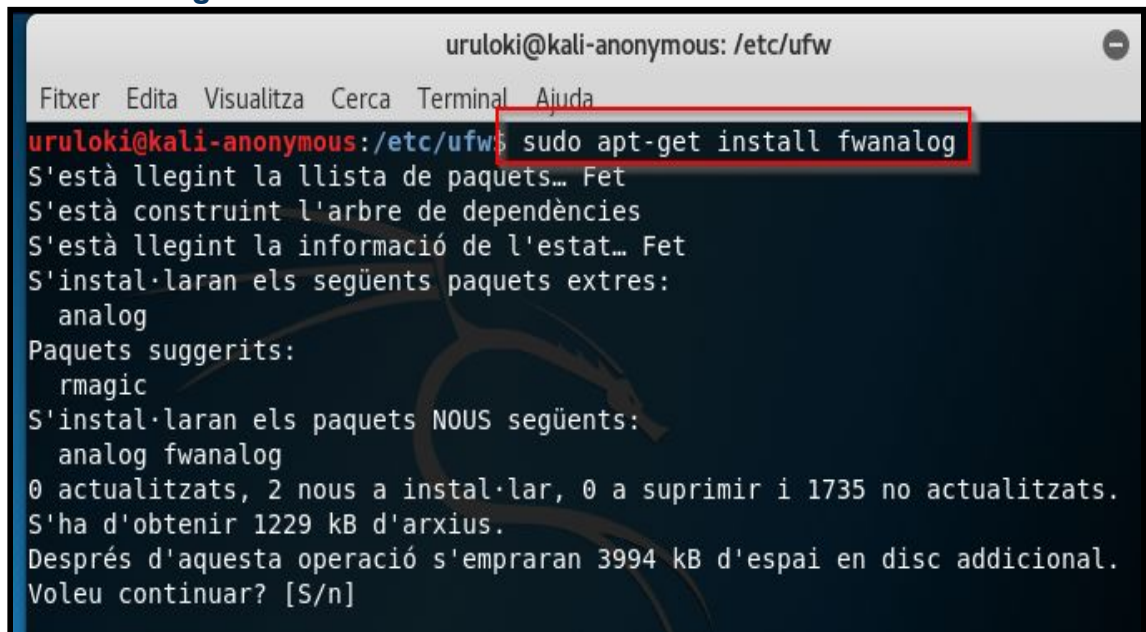
17-02-2019

- Reiniciem el servei ulogd2 perquè guardi els canvis



```
uruloki@kali-anonymous: /etc
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/etc$ sudo systemctl restart ulogd2.service
uruloki@kali-anonymous:/etc$
```

- Els logs del firewall es poden interpretar més fàcilment amb eines d'anàlisi de logs com **fwalog**



```
uruloki@kali-anonymous: /etc/ufw
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/etc/ufw$ sudo apt-get install fwalog
S'està llegint la llista de paquets... Fet
S'està construint l'arbre de dependències
S'està llegint la informació de l'estat... Fet
S'instal·laran els següents paquets extres:
  analog
Paquets suggerits:
  rmagic
S'instal·laran els paquets NOUS següents:
  analog fwalog
0 actualitzats, 2 nous a instal·lar, 0 a suprimir i 1735 no actualitzats.
S'ha d'obtenir 1229 kB d'arxius.
Després d'aquesta operació s'empraran 3994 kB d'espai en disc addicional.
Voleu continuar? [S/n]
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

- Ens descarreguem **GUFW**, per utilitzar l'interfície gràfica (en aquest cas, és el front-end del UFW)

```
uruloki@kali-anonymous: /etc/fwanaolog
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/etc/fwanaolog$ sudo apt-get install gufw
S'està llegint la llista de paquets... Fet
S'està construint l'arbre de dependències
S'està llegint la informació de l'estat... Fet
S'instal·laran els paquets NOUS següents:
  gufw
0 actualitzats, 1 nous a instal·lar, 0 a suprimir i 1735 no actualitzats.
S'ha d'obtenir 873 kB d'arxius.
Després d'aquesta operació s'empraran 3534 kB d'espai en disc addicional.
Bai:1 http://kali.download/kali kali-rolling/main amd64 gufw all 18.10.0-1 [873
kB]
S'ha baixat 873 kB en 1s (1161 kB/s)
S'està seleccionant el paquet gufw prèviament no seleccionat.
(S'està llegint la base de dades... hi ha 343850 fitxers i directoris instal·lats
actualment.)
S'està preparant per a desempaquetar .../gufw_18.10.0-1_all.deb...
S'està desempaquetant gufw (18.10.0-1)...
S'està configurant gufw (18.10.0-1)...
S'estan processant els activadors per a mime-support (3.61)...
S'estan processant els activadors per a desktop-file-utils (0.23-3)...
S'estan processant els activadors per a man-db (2.8.3-2)...
S'estan processant els activadors per a gnome-menus (3.13.3-11)
```



Nom i Cognoms

Arnau Subirós Puigarnau

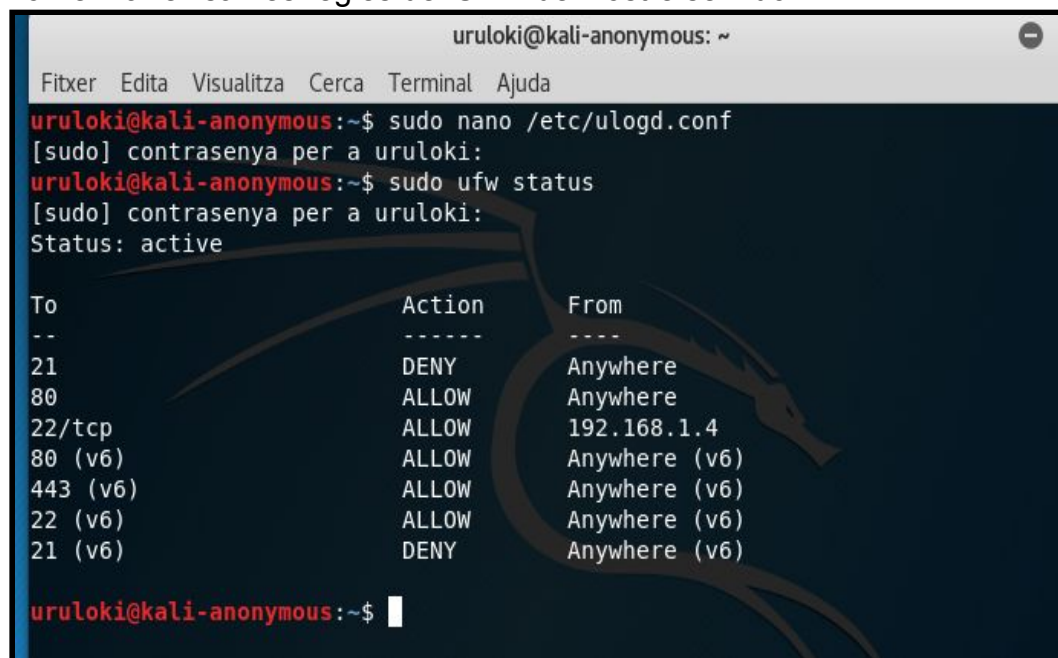
Data

17-02-2019

CLIENT (màquina Ubuntu)

- Per acabar amb la pràctica tenint en compte les regles que anteriorment he fet. Faré algunes proves amb el host client per comprovar que funcionen les regles establertes

Tornem a revisar les regles del UFW del nostre servidor.



```
uruloki@kali-anonymous: ~  
Fitxer Edita Visualitza Cerca Terminal Ajuda  
uruloki@kali-anonymous:~$ sudo nano /etc/ulogd.conf  
[sudo] contrasenya per a uruloki:  
uruloki@kali-anonymous:~$ sudo ufw status  
[sudo] contrasenya per a uruloki:  
Status: active  
  
To Action From  
--  
21 DENY Anywhere  
80 ALLOW Anywhere  
22/tcp ALLOW 192.168.1.4  
80 (v6) ALLOW Anywhere (v6)  
443 (v6) ALLOW Anywhere (v6)  
22 (v6) ALLOW Anywhere (v6)  
21 (v6) DENY Anywhere (v6)  
  
uruloki@kali-anonymous:~$
```

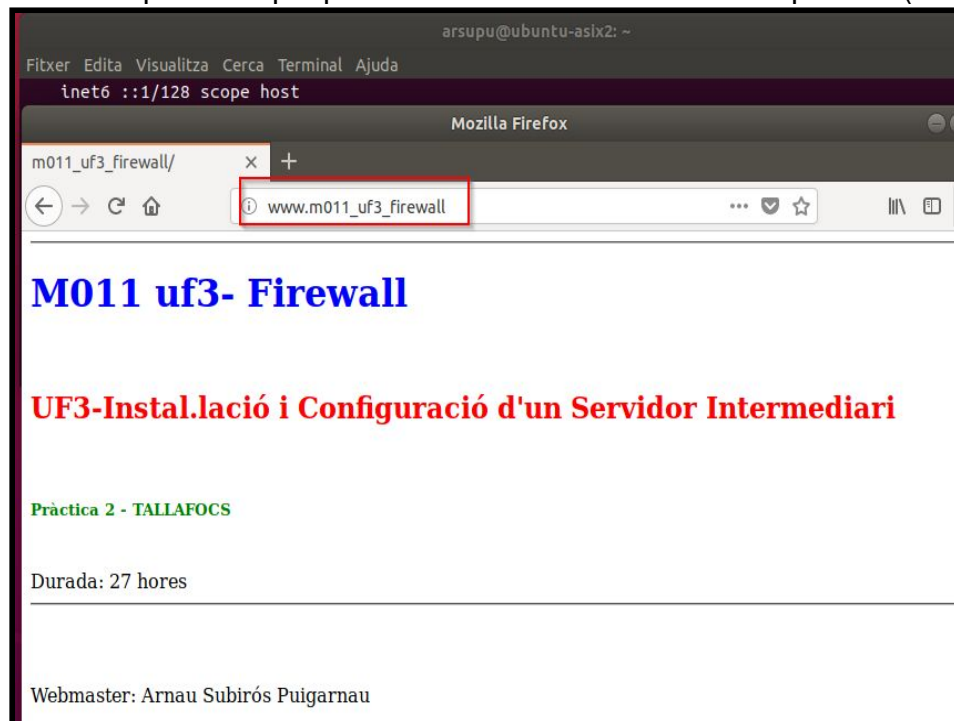

Nom i Cognoms

Arnau Subirós Puigarnau

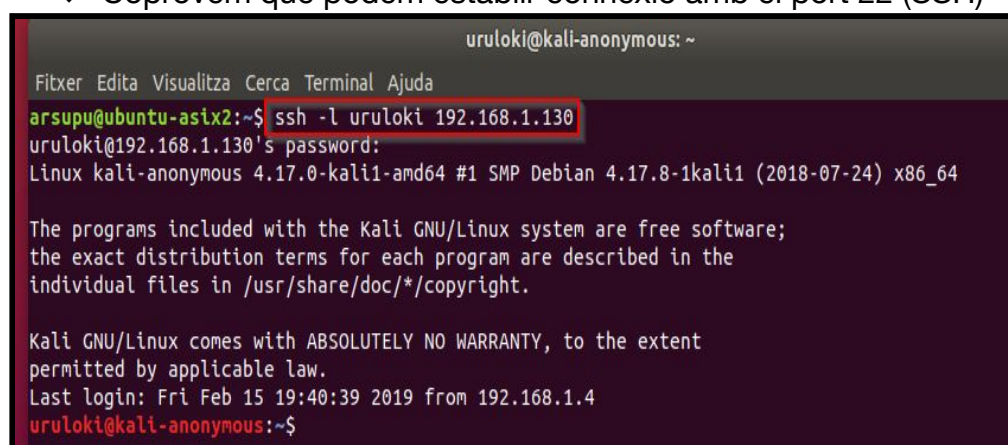
Data

17-02-2019

- ❖ Coproven que podem establir connexio amb el port 80 (HHTP)



- ❖ Coproven que podem establir connexio amb el port 22 (SSH)



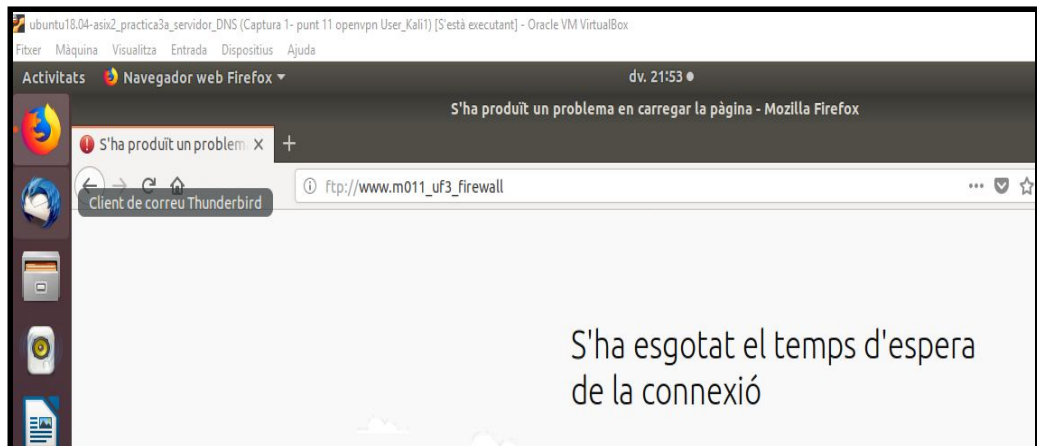
Nom i Cognoms

Arnau Subirós Puigarnau

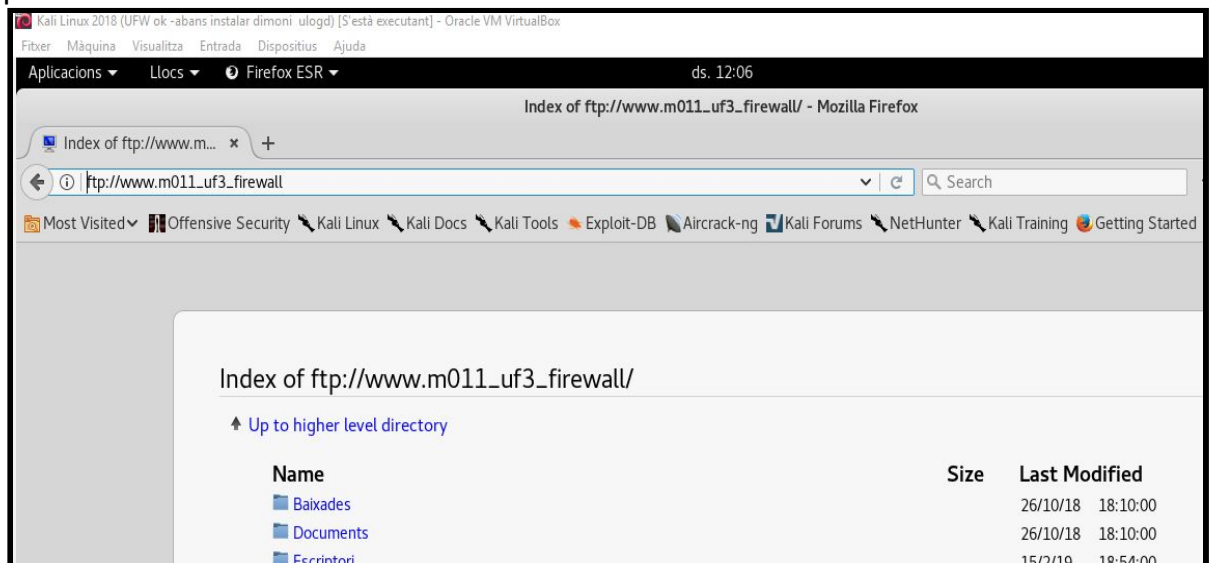
Data

17-02-2019

- ❖ Comprovem que no podem establir connexió amb el port 21 (FTP) desde el Host Client.



Revisem que tot i que en el client no pot accedir, desde el servidor si que podem.



Nom i Cognoms

Arnau Subirós Puigarnau

Data

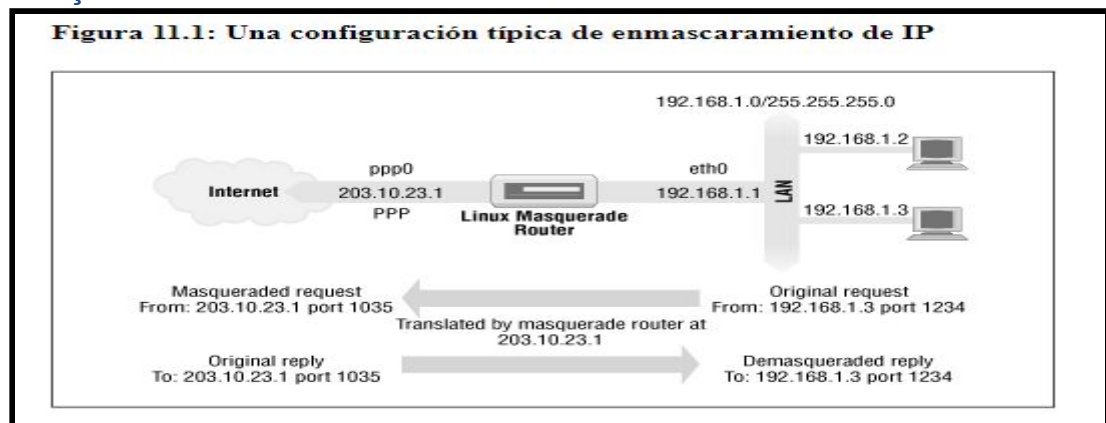
17-02-2019

EXERCICI 2 – 20%

Busca informació i explica amb les teves pròpies paraules, tot el que hagis entès sobre: *ip masquerading*

Molta gent disposa d'un sol compte per connexió telefònica per a connectar-se a Internet. Gairebé tots els que utilitzen aquesta configuració es veu limitat a una sola adreça IP que li dóna el Proveïdor de Serveis d'Internet (ISP), això normalment és bastant per a permetre un accés complet a la xarxa.

- IP-Masquerading possibilita la connexió de diversos ordinadors a internet usant una màquina Linux amb solo una IP pública. Això vol dir que pots connectar una xarxa privada a internet i el teu Proveïdor d'Internet(ISP) creurà que només tens un ordinador connectat
- IP-Masquerading tradueix adreces IP internes en direccions IP externes. Aquest procés es diu Traducció de Direccions de Xarxa (NAT) i Linux fa això mitjançant els anomenats números de port. Des de l'exterior, totes les connexions semblen haver-se originat des de la teva màquina Linux.
- Algunes de les principals distribucions de Linux (Redhat, Mandrake, Debian, Suse ...) el seu Kernel ve preparat per a usar IP-Masquerading.
- IP Masquerade és el nom que se li dóna a un tipus de traducció d'adreces de xarxa que permet que tots els hosts d'una xarxa privada usin Internet al preu d'una sola adreça IP.



Nom i Cognoms

Arnau Subirós Puigarnau

Data

17-02-2019

1. Avantatges

- Només necessita una adreça IP necessària (barata)
- No requereix suport d'aplicació especial
- Utilitza programari de firewall perquè la seva xarxa pugui convertir-se més segura

2. Desavantatges

- Requereix una caixa de Linux o un enrutador RDSI especial (encara que altres productes poden tenir això ...)
- El trànsit entrant no pot accedir al seu LAN intern
Tret que la LAN interna iniciï el trànsit o el programari específic de reexpedició de ports està instal·lat.
- Molts servidors NAT no poden proporcionar aquesta funcionalitat.
- Els protocols especials han de ser manejats de forma única per Redireccionadores de firewall, etc. Linux té suport complet per a aquesta capacitat (FTP, IRC, etc.) però molts enrutadores NO (NetGear ho fa).

3. Diferències entre servidors NAT i servidors PROXY

- Molts **NAT** són similars a un servidor **proxy** en el sentit que el servidor realitzarà la traducció de l'adreça IP i falsificarà el servidor remot **com si el servidor MASQ fes la sol·licitud en lloc d'un maquina interna**
- **La principal diferència entre un servidor MASQ i PROXY és que els servidors MASQ No necessita cap canvi de configuració en totes les màquines client.**
Només configurar per a usar la caixa de Linux com la seva porta d'enllaç predeterminada i tot funcionarà bé . S'haurà d'instal·lar mòduls especials de Linux per a coses com RealAudio, FTP, etc. per a treballar)
 - A més, molts usuaris operen IP MASQ per a TELNET, FTP, etc. * I * també configuren un proxy d'emmagatzematge en caixet en el mateix quadre de Linux per al trànsit WWW per a l'addicional actuació.