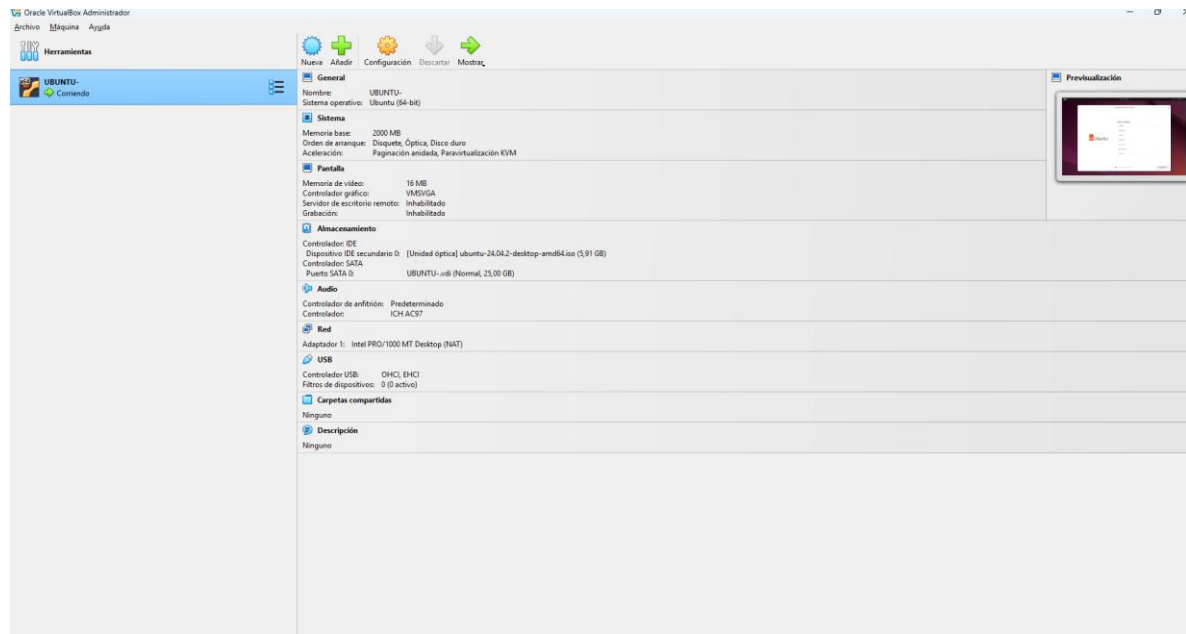


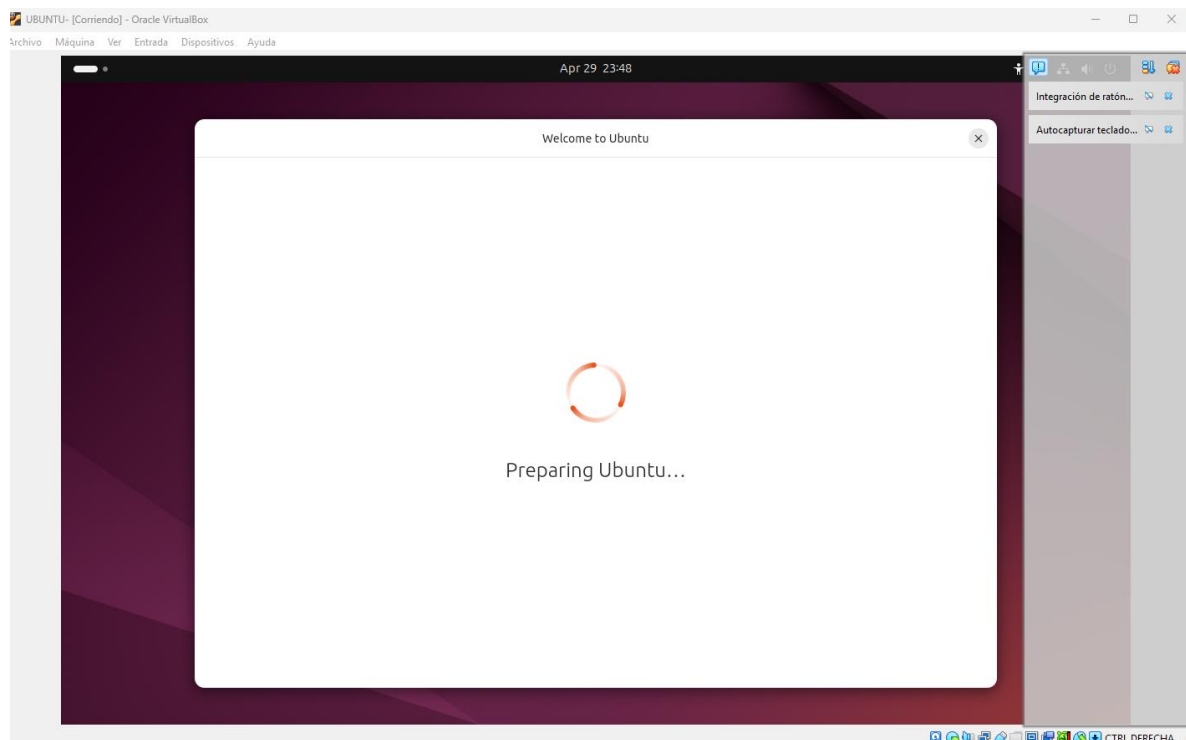
Laboratorio 6,7 - Rigoberto Márquez

C:\Users\ADM\VirtualBox VMs

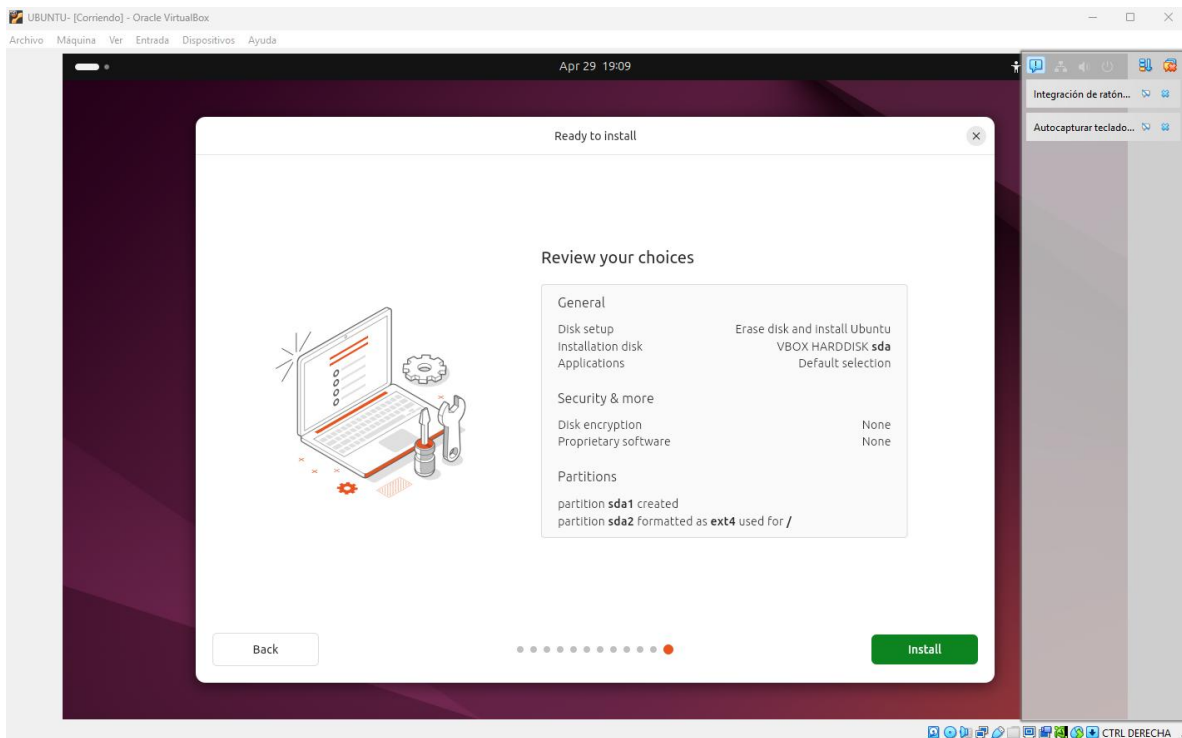
Instalando la VM



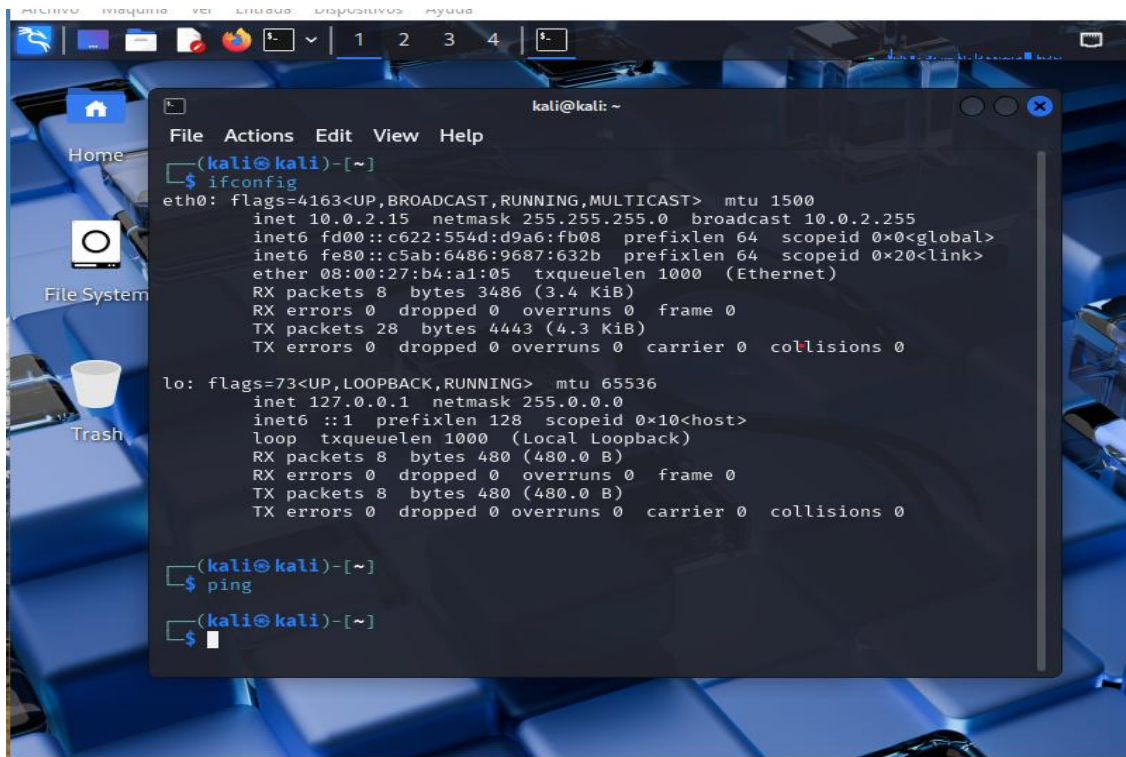
Inicializando la VM



Iniciar instalación:



Comandos:



Los firewalls nos van a proteger contra accesos no autorizados. Monitorean el tráfico de red, lo que entra y sale. Decide si puede entrar o lo bloquear según las reglas (políticas) de seguridad predefinidas.

Los firewalls pueden ser elementos hardware y software. Incluso, híbridos.

Dominio de colisiones: no tener switches que saturen la red, tener segmentada la red.

Dominio de broadcast: dominio de ip.

Comandos:

ping google.com

sudo su

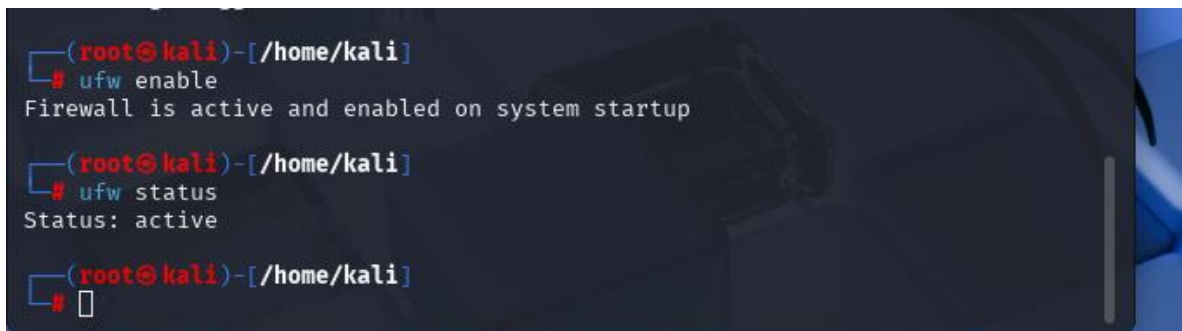
Instalar el firewall descomplicado: apt install ufw -y

ufw enable

ufw es para crear reglas de firewall

ufw status

acciones de reglas: Allow permitir el ingreso, Deny para denegar.

A screenshot of a terminal window with a dark background. The prompt is (root@kali)-[/home/kali]. The first command is # ufw enable, followed by the output 'Firewall is active and enabled on system startup'. The second command is # ufw status, followed by the output 'Status: active'. The third command is #, followed by a cursor. The terminal window is overlaid on a blurred image of a person's hand holding a smartphone.

```
(root@kali)-[/home/kali]
# ufw enable
Firewall is active and enabled on system startup

(root@kali)-[/home/kali]
# ufw status
Status: active

(root@kali)-[/home/kali]
#
```

iptables:

apt install iptable -y

iptables -L dictar como están las reglas.

```
(root@kali)-[/home/kali]
# sudo apt install iptables -y

iptables is already the newest version (1.8.11-2).
iptables set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1238

(root@kali)-[/home/kali]
# iptables -y
iptables v1.8.11 (nf_tables): unknown option "-y"
Try 'iptables -h' or 'iptables --help' for more information.

(root@kali)-[/home/kali]
# iptables -L
Chain INPUT (policy DROP)
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

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

ls y ls -i... Para listar

```
(root@kali)-[/home/kali]
# ls
Desktop Documents Downloads Music Pictures Public Templates Videos

(root@kali)-[/home/kali]
# ls -i
1703987 Desktop 1703988 Downloads 1703993 Pictures 1703989 Templates
1703991 Documents 1703992 Music 1703990 Public 1703994 Videos

(root@kali)-[/home/kali]
#
```

ufw default deny incoming : denegar todas las comunicaciones.

¿Por qué es útil?

- **Protege tu sistema:** evita que alguien desde Internet intente conectarse sin permiso.
- Es un buen **primer paso de seguridad** antes de permitir solo lo necesario.

El comando ufw default deny incoming protege solo *tu equipo (PC)*, no toda tu red.

¿Qué significa esto?

- **Tu PC** dejará de aceptar conexiones **desde afuera** (por ejemplo, desde Internet o desde otro dispositivo en la misma red local).
- Pero **otros dispositivos de tu red (como otro PC, una impresora o un router)** **no están protegidos** por este comando. Tendrían que tener su propio firewall configurado.

```

(root@kali)-[/home/kali]
# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

(root@kali)-[/home/kali]

```

- ufw default allow outgoing : Todo el trafico permitido, Tu sistema **puede iniciar conexiones hacia fuera sin restricciones**, por ejemplo:
 - Navegar por internet
 - Actualizar el sistema
 - Conectarse a APIs externas
 - Enviar correos salientes (si tienes un servidor SMTP, por ejemplo)

```

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

(root@kali)-[/home/kali]
#

```

CON IPTABLE

Iptable -P INPUT DROP: COMO EL DENY. No mira el trafico que viene, solo niega y niega.

Iptable -P OUTPUT ACCEPT: **Permitir todo el tráfico saliente desde tu sistema hacia otros destinos**, a menos que haya reglas explícitas que digan lo contrario.

```

(root@kali)-[/home/kali]
# iptables -P INPUT DROP

(root@kali)-[/home/kali]
# iptables -P OUTPUT ACCEPT

(root@kali)-[/home/kali]
#

```

CREAR POLITICAS PARA EL PUERTO 22, HTTP, HTTPS

ufw allow ssh, ufw allow http, ufw allow https

iptables -A INPUT -p tcp -dport 22 -j ACCEPT

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

```
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

```
(root@kali)-[/home/kali]
# ufw allow ssh
Rule added
Rule added (v6)

(root@kali)-[/home/kali]
# ufw allow http
Rule added
Rule added (v6)

(root@kali)-[/home/kali]
# ufw allow https
Rule added
Rule added (v6)
```

```
(root@kali)-[/home/kali]
# iptables -A INPUT -p tcp --dport 22 -j ACCEPT

(root@kali)-[/home/kali]
# iptables -A INPUT -p tcp --dport 80 -j ACCEPT

(root@kali)-[/home/kali]
# iptables -A INPUT -p tcp --dport 443 -j ACCEPT

(root@kali)-[/home/kali]
```

enumerar las políticas creadas:

ufw status numbered

```
(root@kali)-[/home/kali]
# ufw status numbered
Status: active

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

(root@kali)-[/home/kali]
```

iptables -L, para ver las reglas


```

(root@kali)-[/home/kali]
# iptables -L
Chain INPUT (policy DROP)
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     tcp -- anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp -- anywhere             anywhere             tcp dpt:http
ACCEPT     tcp -- anywhere             anywhere             tcp dpt:https

Chain FORWARD (policy DROP)
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
ufw-track-forward all -- anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ufw-before-logging-output all -- anywhere             anywhere
ufw-before-output all -- anywhere             anywhere
ufw-after-output all -- anywhere             anywhere
ufw-after-logging-output all -- anywhere             anywhere
ufw-reject-output all -- anywhere             anywhere
ufw-track-output all -- anywhere             anywhere

Chain ufw-after-forward (1 references)
target     prot opt source                destination

```

ufw allow from 192.168.1.20

Explicación:

¿Qué hace?

Este comando le dice al **firewall (ufw)**:

“Permite que este equipo (mi PC) reciba conexiones desde la dirección IP 192.168.1.20”.

Es como decir:

“Confío en el dispositivo con IP 192.168.1.20 (por ejemplo, otro computador, una impresora o un servidor en tu red), y le dejo pasar por mi firewall.”

```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# ufw allow from 192.168.1.20
Rule added

(root@kali)-[/home/kali]
# ufw status numbered
Status: active

      To Action From
      --
[ 1] 22/tcp ALLOW IN Anywhere
[ 2] 80/tcp ALLOW IN Anywhere
[ 3] 443 ALLOW IN Anywhere
[ 4] Anywhere ALLOW IN 192.168.1.20
[ 5] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 6] 80/tcp (v6) ALLOW IN Anywhere (v6)
[ 7] 443 (v6) ALLOW IN Anywhere (v6)

(root@kali)-[/home/kali]
#
```

ufw deny from 192.168.1.20

```
root@kali: /home/kali
File Actions Edit View Help
[ 3] 443 ALLOW IN Anywhere
[ 4] Anywhere ALLOW IN 192.168.1.20
[ 5] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 6] 80/tcp (v6) ALLOW IN Anywhere (v6)
[ 7] 443 (v6) ALLOW IN Anywhere (v6)

(root@kali)-[/home/kali]
# ufw deny from 192.168.1.20
Rule updated

(root@kali)-[/home/kali]
# ufw status numbered
Status: active

      To Action From
      --
[ 1] 22/tcp ALLOW IN Anywhere
[ 2] 80/tcp ALLOW IN Anywhere
[ 3] 443 ALLOW IN Anywhere
[ 4] Anywhere DENY IN 192.168.1.20
[ 5] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 6] 80/tcp (v6) ALLOW IN Anywhere (v6)
[ 7] 443 (v6) ALLOW IN Anywhere (v6)

(root@kali)-[/home/kali]
#
```

iptables -A INPUT -s 192.168.1.45 -j ACCEPT (A DE APPEND, -s es source, origen. -j, jump, salto que da la regla) (hace lo mismo que ufw allow)

iptables -L --line-numbers


```

(root@kali)-[/home/kali]
# iptables -L --line-numbers
Chain INPUT (policy DROP)
num target      prot opt source                destination
1  ufw-before-logging-input  all  --  anywhere                anywhere
2  ufw-before-input  all  --  anywhere                anywhere
3  ufw-after-input   all  --  anywhere                anywhere
4  ufw-after-logging-input  all  --  anywhere                anywhere
5  ufw-reject-input  all  --  anywhere                anywhere
6  ufw-track-input   all  --  anywhere                anywhere
7  ACCEPT          all  --  192.168.1.45            anywhere

Chain FORWARD (policy DROP)
num target      prot opt source                destination
1  ufw-before-logging-forward  all  --  anywhere                anywhere
2  ufw-before-forward  all  --  anywhere                anywhere
3  ufw-after-forward   all  --  anywhere                anywhere
4  ufw-after-logging-forward  all  --  anywhere                anywhere
5  ufw-reject-forward  all  --  anywhere                anywhere
6  ufw-track-forward   all  --  anywhere                anywhere

Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination
1  ufw-before-logging-output  all  --  anywhere                anywhere
2  ufw-before-output  all  --  anywhere                anywhere
3  ufw-after-output   all  --  anywhere                anywhere
4  ufw-after-logging-output  all  --  anywhere                anywhere
5  ufw-reject-output  all  --  anywhere                anywhere
6  ufw-track-output   all  --  anywhere                anywhere

Chain ufw-after-forward (1 references)
num target      prot opt source                destination

```

iptables -D INPUT 9 (Borrar reglas)

```

(root@kali)-[/home/kali]
# iptables -D INPUT 7

(root@kali)-[/home/kali]
#

```

BLOQUEAR PUERTOS NO ESENCIALES

ufw deny from any to any port 8080 : **Bloquear todo el tráfico dirigido al puerto 8080**, sin importar de qué dirección IP provenga o a qué IP de tu sistema esté destinado.

“Nadie puede usar la puerta número 8080 de mi computadora.”

¿Cuándo se usa esto?

El puerto 8080 suele usarse para servidores web alternativos (como aplicaciones en desarrollo). Este comando te sirve si **no quieres que nadie se conecte ahí** por razones de seguridad.

```

(root@kali)-[/home/kali]
# ufw deny from any to any port 8080
Rule added
Rule added (v6)

(root@kali)-[/home/kali]
# ufw status numbered
Status: active

      To Action From
      --
[ 1] 22/tcp ALLOW IN Anywhere
[ 2] 80/tcp ALLOW IN Anywhere
[ 3] 443 ALLOW IN Anywhere
[ 4] Anywhere DENY IN 192.168.1.20
[ 5] 8080 DENY IN Anywhere
[ 6] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 7] 80/tcp (v6) ALLOW IN Anywhere (v6)
[ 8] 443 (v6) ALLOW IN Anywhere (v6)
[ 9] 8080 (v6) DENY IN Anywhere (v6)

(root@kali)-[/home/kali]
#

```

iptables -A INPUT -p tcp --dport 8080 -j DROP (hace lo mismo que el anterior)

```

Chain ufw-user-input (1 references)
num target prot opt source destination tcp dpt:ssh
1 ACCEPT tcp -- anywhere anywhere tcp dpt:http
2 ACCEPT tcp -- anywhere anywhere tcp dpt:https
3 ACCEPT tcp -- anywhere anywhere udp dpt:https
4 ACCEPT udp -- anywhere anywhere
5 DROP all -- 192.168.1.20 anywhere
6 DROP tcp -- anywhere anywhere tcp dpt:http-alt
7 DROP udp -- anywhere anywhere udp dpt:8080

Chain ufw-user-limit (0 references)
num target prot opt source destination limit: avg 3/min bu
1 LOG all -- anywhere anywhere
rst 5 LOG level warn prefix "[UFW LIMIT BLOCK] "
2 REJECT all -- anywhere anywhere reject-with icmp-po
rt-unreachable

Chain ufw-user-limit-accept (0 references)
num target prot opt source destination
1 ACCEPT all -- anywhere anywhere

Chain ufw-user-logging-forward (0 references)
num target prot opt source destination

```