LABORATORIO 6 TECH

JESUS DAVID DE LA HOZ PEÑA

UNIVERSIDAD POPULAR DEL CESAR

VALLEDUPAR

2025

INSTALACION SISTEMA

El primer paso que hemos realizado es actualizar el sistema mediante “sudo apt update && sudo apt upgrade -y”

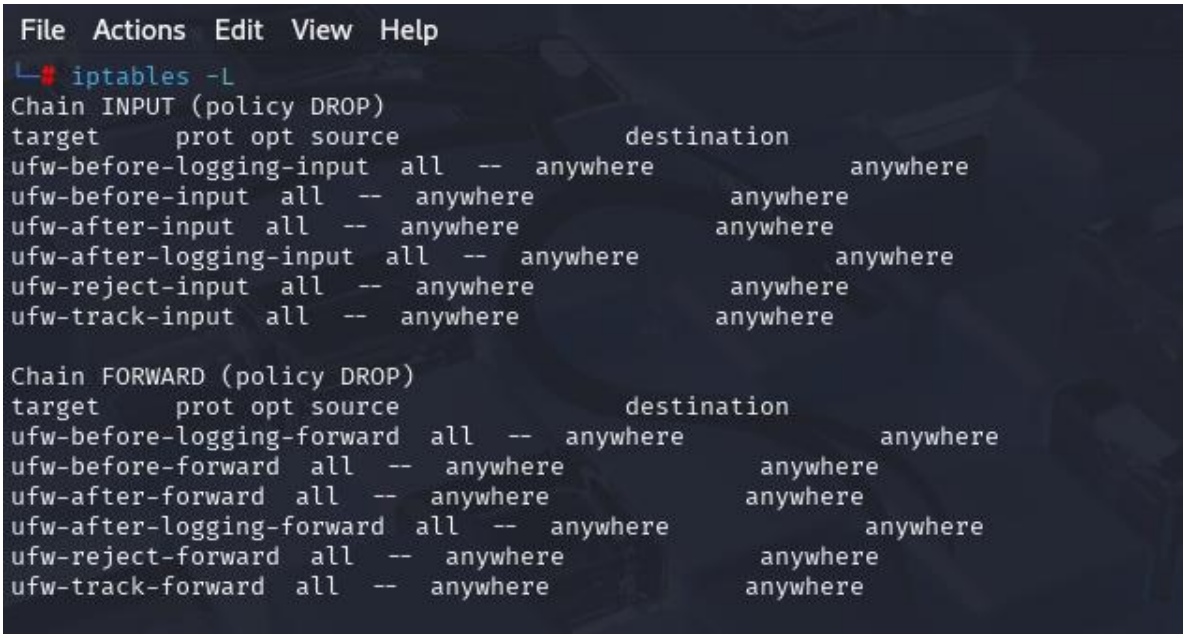
```
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.0
MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [121 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [32
7 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [204 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [9
14 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages
 [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents
 (deb) [24.3 kB]
Fetched 74.6 MB in 6s (12.8 MB/s)
1195 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Siguiente a esto instalamos UFW y lo activamos con UFW enable

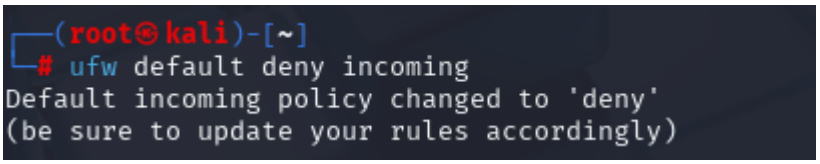
```
┌──(root㉿kali)-[~]
└─# apt install ufw
Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1193
  Download size: 169 kB
  Space needed: 880 kB / 63.8 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 1s (269 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 409537 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
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
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
```

```
└─# ufw enable
Firewall is active and enabled on system startup
```

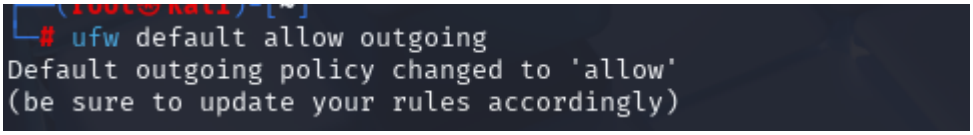
Ahora veremos las reglas actuales del cortafuego con iptables -L



Ahora configuraremos la política para bloquear todo el tráfico entrante

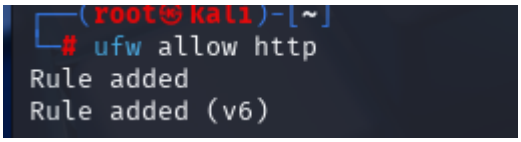


Ahora permitiremos que todo el trafico de mi dispositivo pueda llegar otros dispositivos

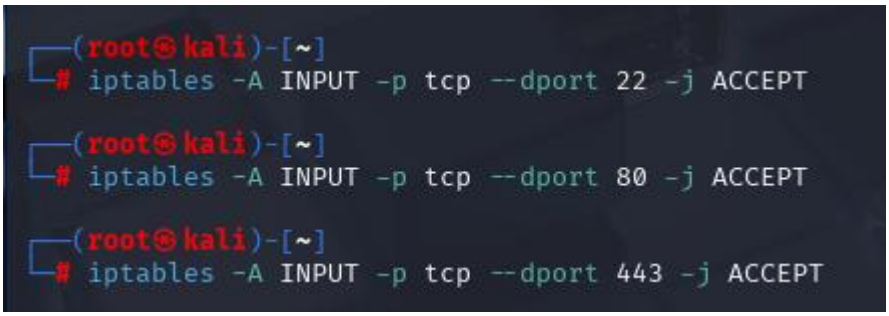


Ahora haremos que no pueda entrar el tráfico entrante, aunque se reinicie el dispositivo, es decir que se mantenga persistente

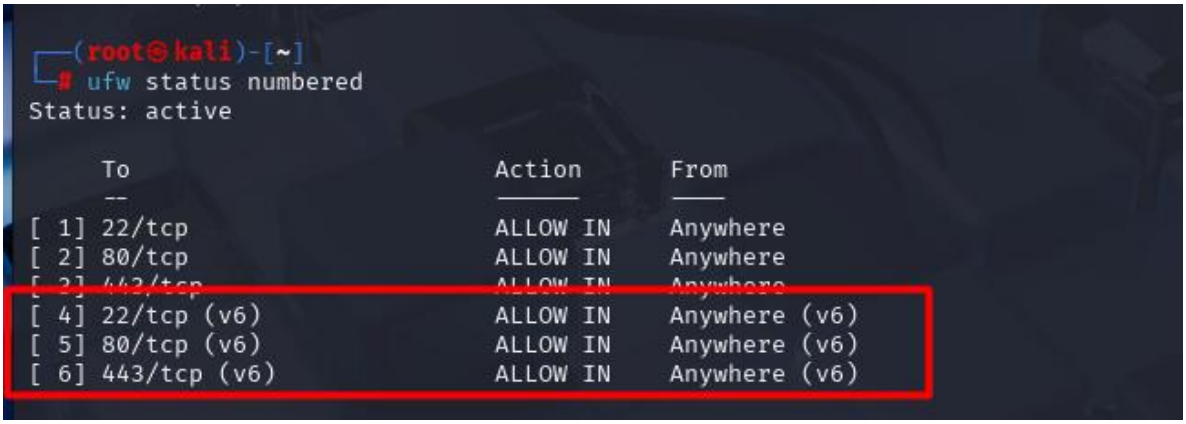
Ahora permitiremos que el tráfico http entré también



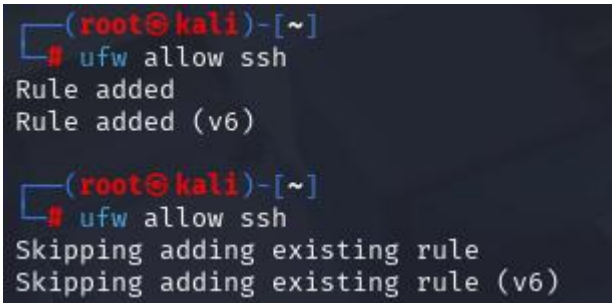
Ahora permitiremos que entre el trafico en los puertos “22” (SSH), “80” (HTTP) y 443 (HTTPS)



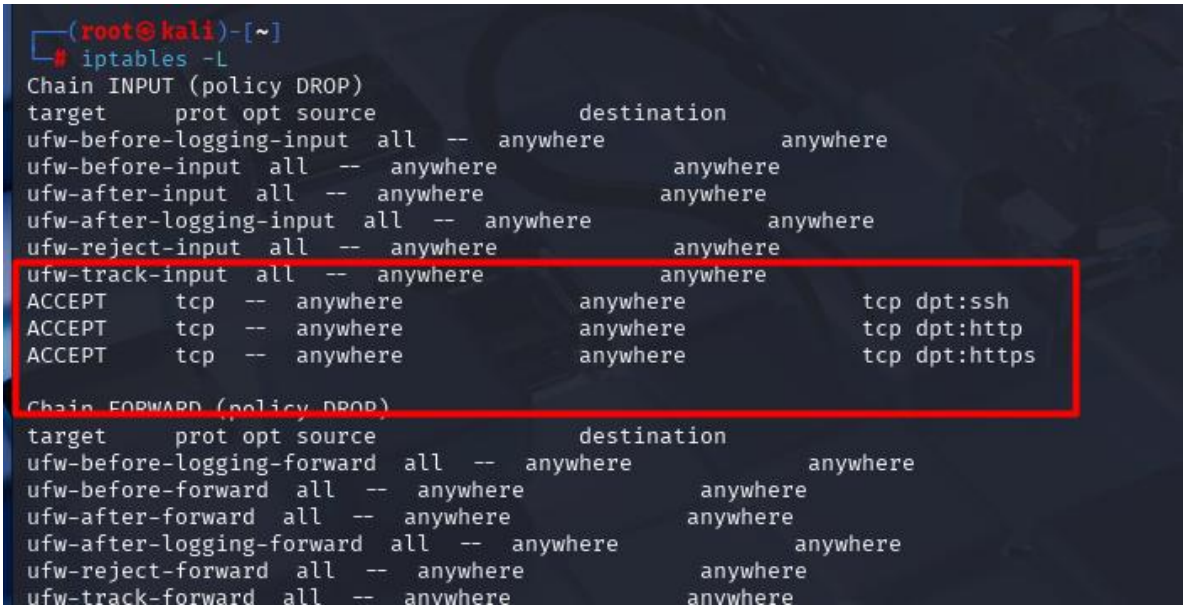
Ahora verificamos que ya estén habilitados:



Ahora para que otras maquinas se conecten al servidor habilitaremos SSH



Ahora verificaremos que las reglas se agregaron correctamente



Finalmente permitiremos que las maquinas con mi ip “192.168.1.9” puedan acceder a mi servidor desde cualquier puerto}