LABORATORIO 7 TECH

JESUS DAVID DE LA HOZ PEÑA

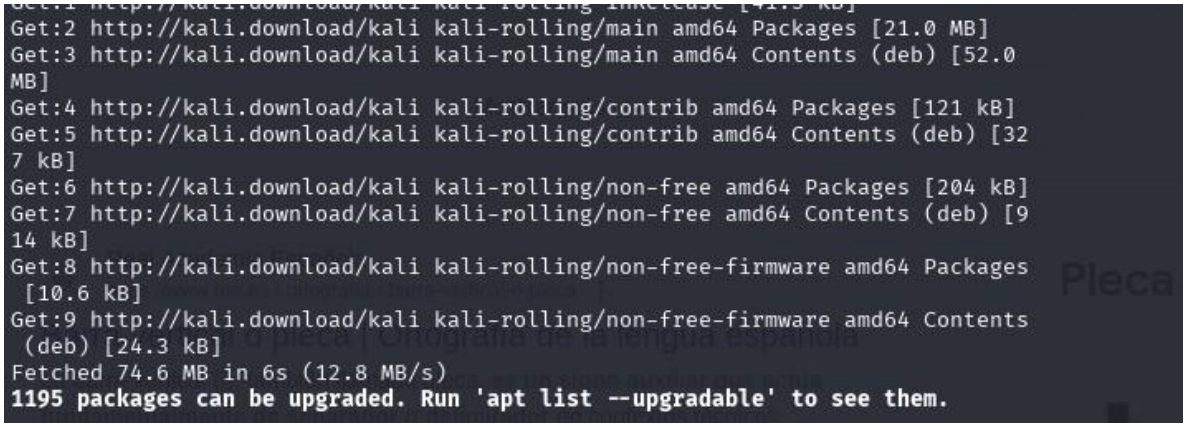
UNIVERSIDAD POPULAR DEL CESAR

VALLEDUPAR

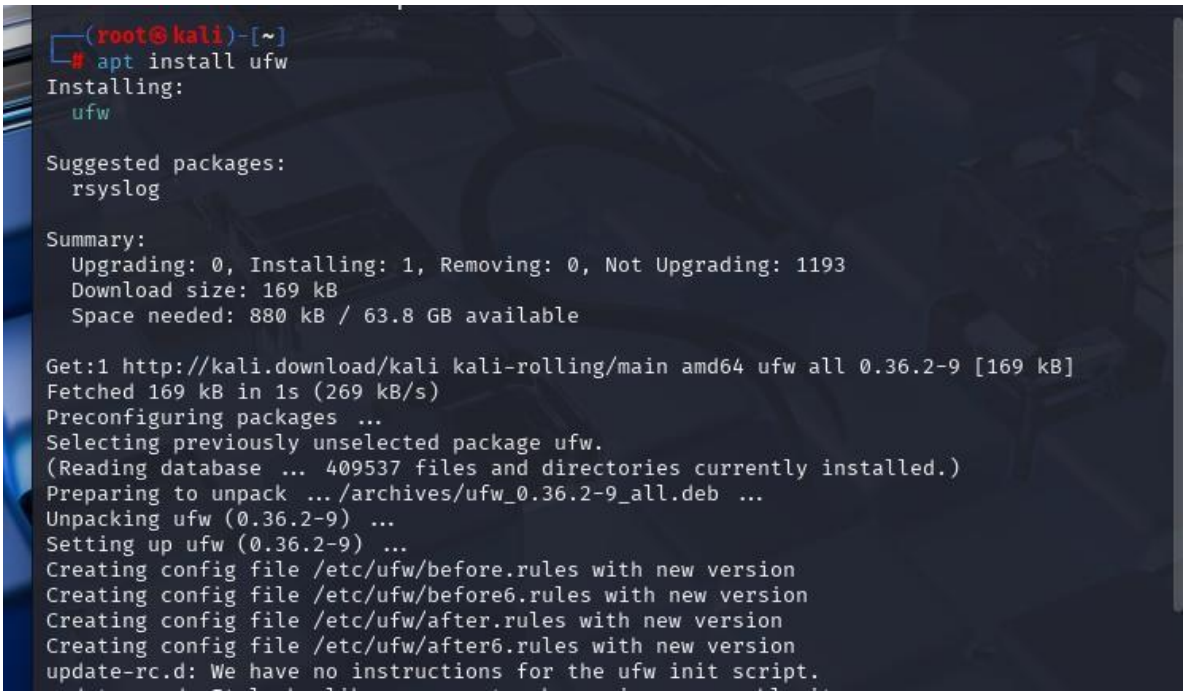
2025

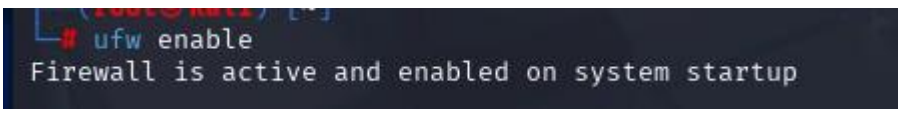
INSTALACION SISTEMA

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

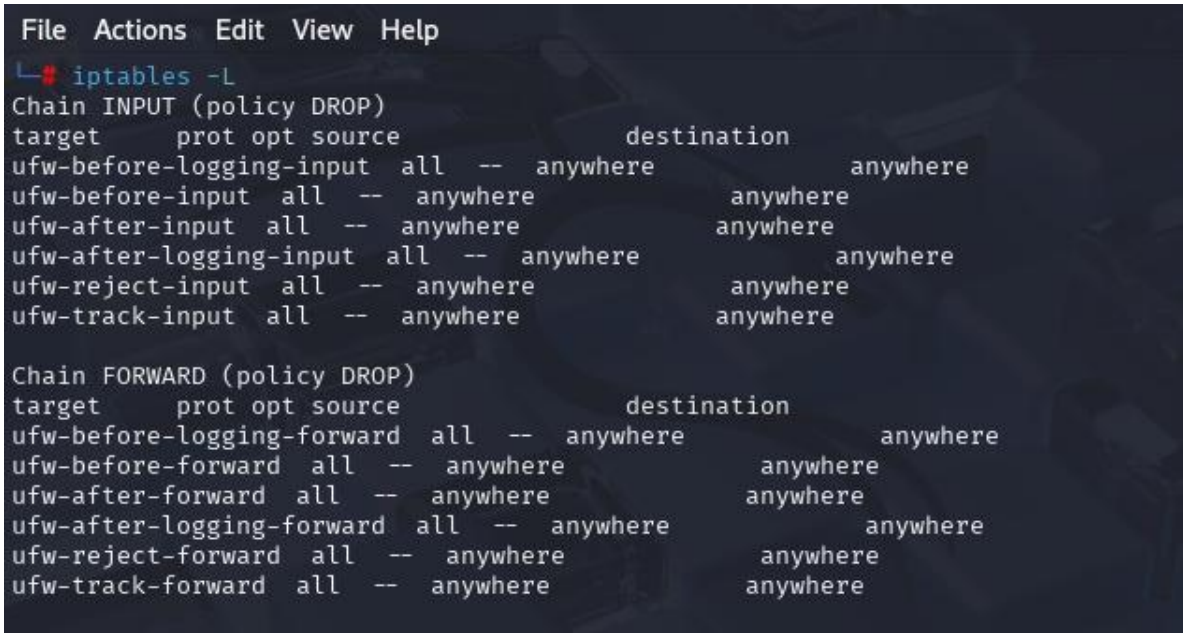


Siguiente a esto instalamos UFW y lo activamos con UFW enable

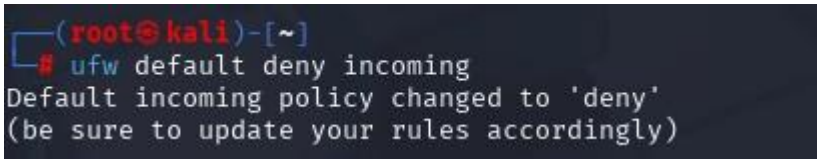




Ahora veremos las reglas actuales del cortafuego con iptables -L

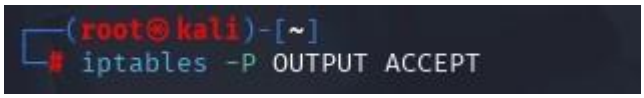


Ahora configuraremos la política para bloquear todo el tráfico entrante

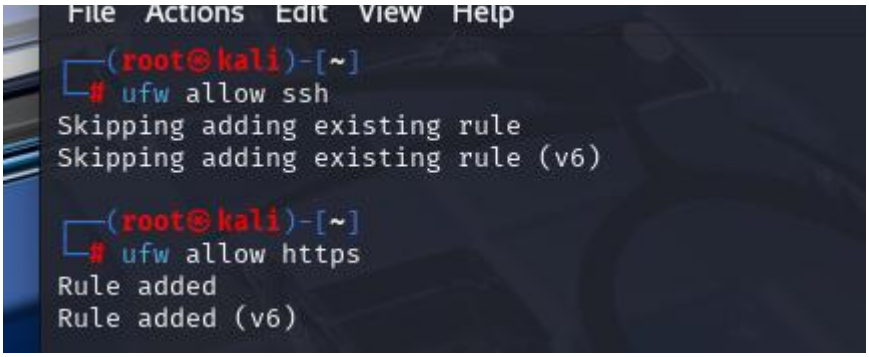


Ahora permitiremos que todo el trafico de mi dispositivo pueda llegar otros dispositivos

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, https y Ssh entré también



Ahora configuramos reglas para habilitar el puerto 22 (SSH), el 80 (HTTP) y el 443 (HTTPS)

Ahora verificamos que se hayan colocado correctamente con “ufw status numbered”

Ahora configuraremos reglas para permitir o denegar trafico basado en ip especificas

```
┌──(root㉿kali)-[~]
└─# ufw allow from 192.168.1.100
Rule added
```

Si queremos denegar la ip especifica:

```
┌──(root㉿kali)-[~]
└─# ufw deny from 192.168.1.100
Rule updated
```

Si queremos permitir de una ip especifica desde iptables:

```
┌──(root㉿kali)-[~]
└─# iptables -A INPUT -s 192.168.1.100 -j ACCEPT
```

Si queremos denegar desde iptables:

```
┌──(root㉿kali)-[~]
└─# iptables -A INPUT -s 192.168.1.100 -j DROP
```

Ahora se configurará reglas para redes internas y externas

Para permitir todo el trafico dentro de la red interna colocamos lo siguiente:

```
└─# ufw allow from 192.168.1.0/24
Rule added
```

Para denegar el trafico externo a puertos no esenciales:

```
└─# ufw deny from any to any port 8080
Rule added
Rule added (v6)
```

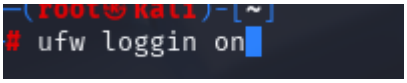
Para permitir todo el tráfico interno desde iptables:

```
┌──(root㉿kali)-[~]
└─# iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT
```

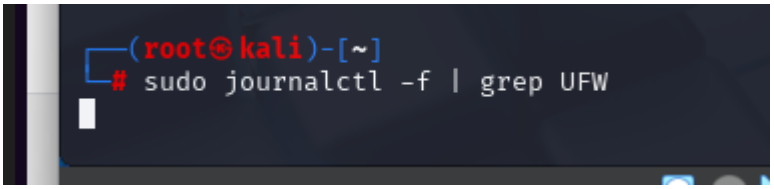
Para bloquear puertos no esenciales el trafico externo desde iptable

MONITOREO Y AJUSTES DE FIREWALL

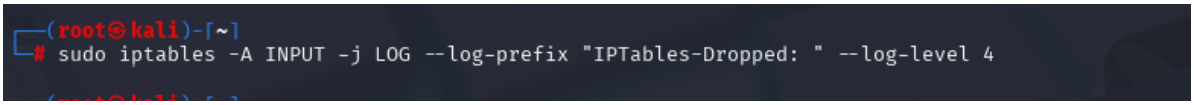
Ahora para habilitar los logs para identificar patrones sospechosos o intentos no autorizados habilitamos el registro (log)



Ahora revisamos los logs



Si queremos habilitar los logs por iptable:



Y finalmente revisamos el log en el cual actualmente no hay nada porque no se ha intentado ninguna violación de las reglas