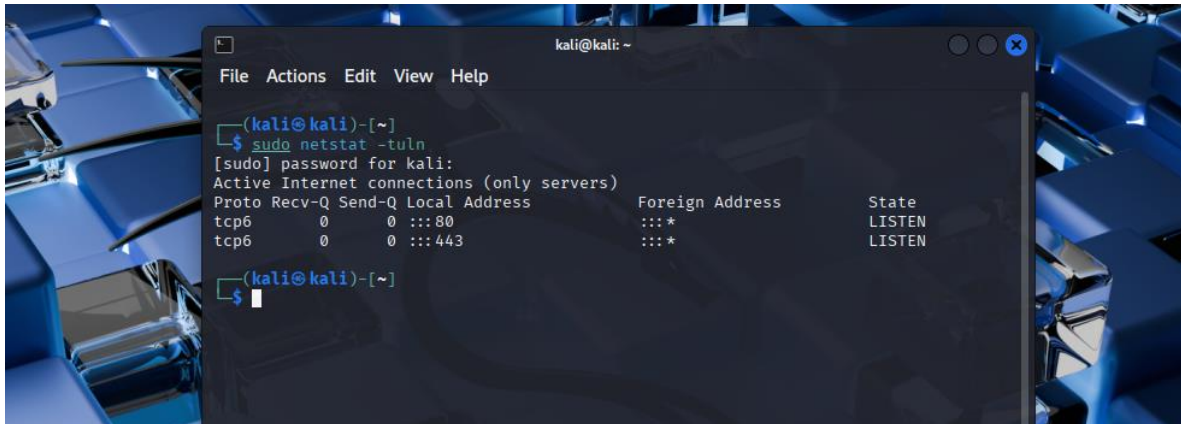
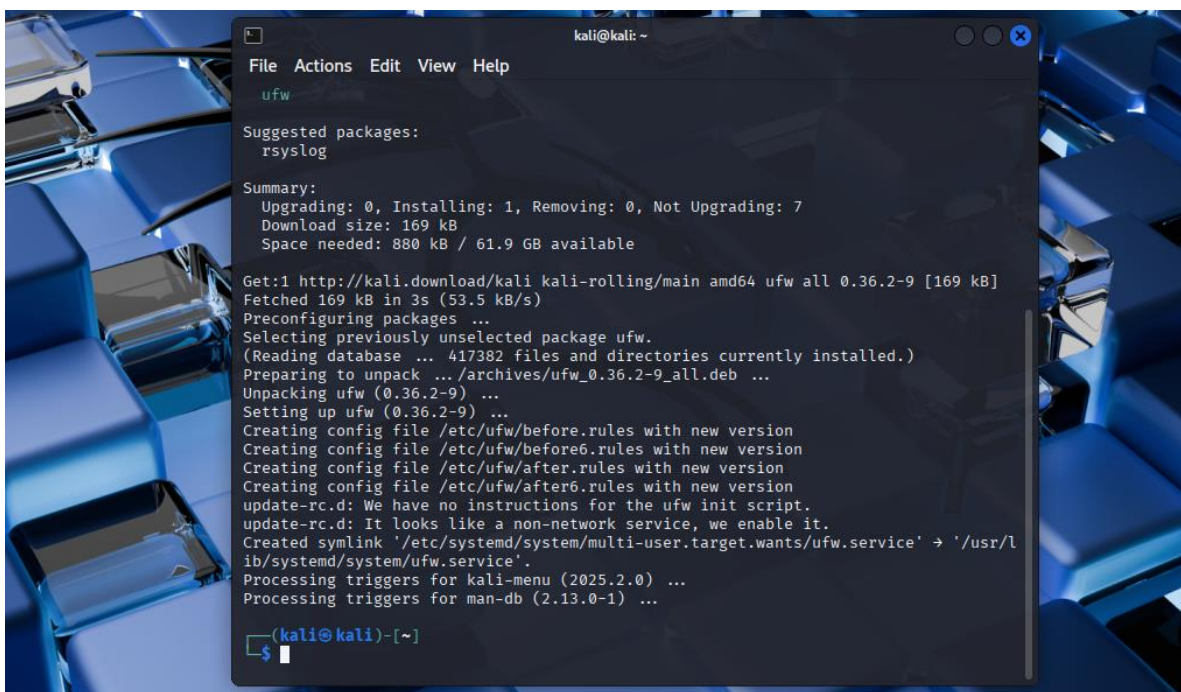


Configuración de un Firewall en un Entorno de Red

Introducción al Firewall y Entorno de Configuración

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The user has entered the command 'sudo netstat -tuln'. The output shows active Internet connections for servers. The terminal text is as follows:

```
(kali@kali)-[~]  
$ sudo netstat -tuln  
[sudo] password for kali:  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp6      0      0 :::80                  :::*                    LISTEN  
tcp6      0      0 :::443                  :::*                    LISTEN  
  
(kali@kali)-[~]  
$
```

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The user has entered the command 'ufw'. The output shows the installation of the ufw package. The terminal text is as follows:

```
ufw  
  
Suggested packages:  
  rsyslog  
  
Summary:  
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 7  
  Download size: 169 kB  
  Space needed: 880 kB / 61.9 GB available  
  
Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]  
Fetched 169 kB in 3s (53.5 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package ufw.  
(Reading database ... 417382 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.  
update-rc.d: It looks like a non-network service, we enable it.  
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' -> '/usr/lib/systemd/system/ufw.service'.  
Processing triggers for kali-menu (2025.2.0) ...  
Processing triggers for man-db (2.13.0-1) ...  
  
(kali@kali)-[~]  
$
```

```
(kali@kali)-[~]
$ sudo iptables -L
[sudo] password for kali:
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
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
```

Configuración Básica del Firewall

```
(kali@kali)-[~]
$ sudo ufw enable
Firewall is active and enabled on system startup

(kali@kali)-[~]
$ sudo ufw status
Status: active

(kali@kali)-[~]
$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

(kali@kali)-[~]
$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

(kali@kali)-[~]
$
```

Esta configuración hace que el tráfico entrante sea bloqueado, solo se permite el que este autorizado

```
(kali@kali)-[~]
$ sudo ufw allow ssh
$ sudo ufw allow http
$ sudo ufw allow https
Rule added
Rule added (v6)
Rule added
Rule added (v6)
Rule added
Rule added (v6)

(kali@kali)-[~]
$ sudo 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)

(kali@kali)-[~]
$
```

Configuración Avanzada del Firewall

```
(kali@kali)-[~]
$ sudo ufw allow from 192.168.1.100
Rule added

(kali@kali)-[~]
$ sudo ufw deny from 192.168.1.100
Rule updated

(kali@kali)-[~]
$
```

Denegar o permitir una ip especifica.

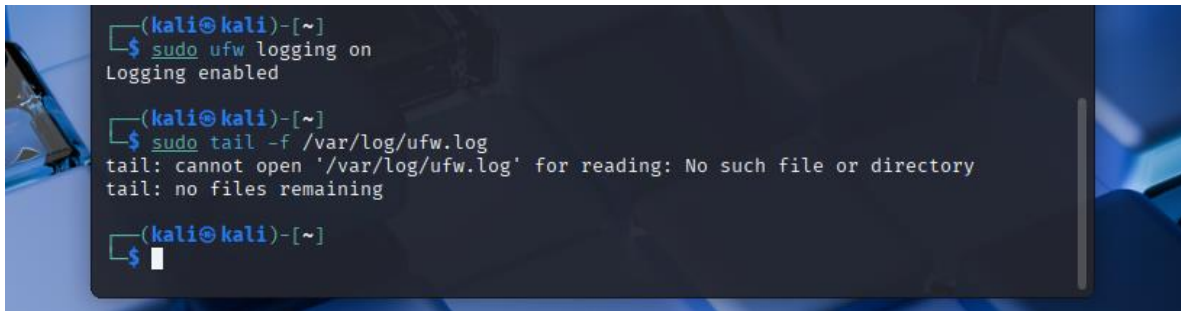
```
(kali@kali)-[~]
$ sudo ufw allow from 192.168.1.0/24
Rule added

(kali@kali)-[~]
$ sudo ufw deny from any to any port 8080
Rule added
Rule added (v6)

(kali@kali)-[~]
$
```

1. permitir todo el tráfico dentro de la red interna
2. denegar tráfico externo a puertos no esenciales

Monitoreo y Ajustes del Firewall

A terminal window on a Kali Linux system. The prompt is (kali@kali)-[~]. The user enters 'sudo ufw logging on' and the output is 'Logging enabled'. The user then enters 'sudo tail -f /var/log/ufw.log' and the output is 'tail: cannot open '/var/log/ufw.log' for reading: No such file or directory' followed by 'tail: no files remaining'. The prompt returns to (kali@kali)-[~].

```
(kali@kali)-[~]  
$ sudo ufw logging on  
Logging enabled  
  
(kali@kali)-[~]  
$ sudo tail -f /var/log/ufw.log  
tail: cannot open '/var/log/ufw.log' for reading: No such file or directory  
tail: no files remaining  
  
(kali@kali)-[~]  
$
```

La configuración de un firewall en Linux representó un proceso desafiante, especialmente al momento de entender cómo funcionan las reglas y políticas predeterminadas del sistema. Durante el desarrollo del laboratorio, se exploraron herramientas como ufw e iptables, lo que permitió tener un mayor control sobre el tráfico entrante y saliente del sistema. A pesar de algunos errores iniciales que bloquearon ciertos servicios por accidente, con pruebas y ajustes progresivos se consiguió establecer una configuración funcional y segura. Esta actividad reforzó la importancia de aplicar filtros adecuados en la red y permitió adquirir habilidades prácticas en la administración de la seguridad a nivel de sistema operativo.