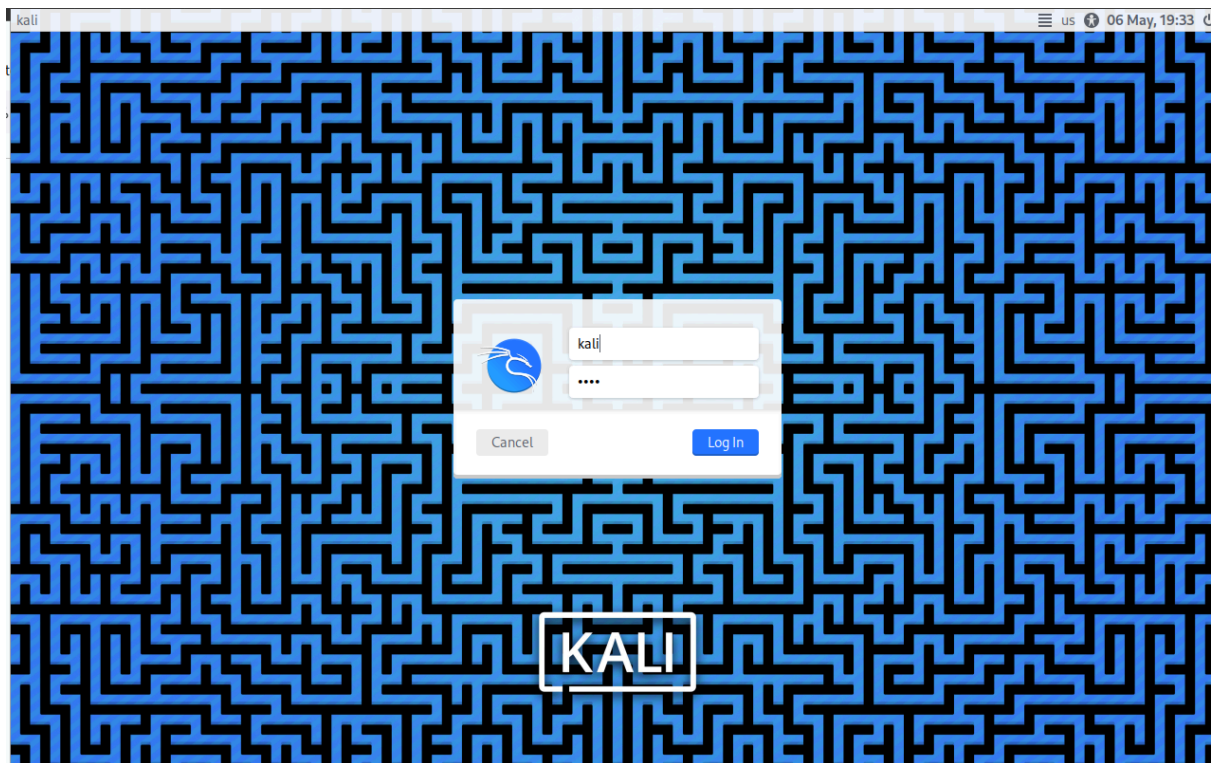


Estudiante: Hector Rincon

Primero entramos a nuestra máquina virtual usando kali linux:



Paso 1: Revisión de la Configuración de Red Actual

Comando para ver interfaces de red:

`ip a`

```
root@kali: ~
zsh: corrupt history file /root/.zsh_history
(root@kali)-[~]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1
    link/ether 08:00:27:c1:c9:eb brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 86207sec preferred_lft 86207sec
    inet6 fd17:625c:f037:2:e6c1:cd16:5e5e:5eb3/64 scope global dynamic noprefixroute
        valid_lft 86209sec preferred_lft 14209sec
    inet6 fe80::d71a:8904:8114:e0f1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Comando para ver la tabla de rutas:

`ip route`

```
(root@kali)-[~]
# ip route
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100
```

Ver puertos y servicios en escucha:

```
ss -tuln
```

```
(root@kali)-[~]
# ss -tuln
```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port

Paso 2: Instalación y Verificación del Firewall

Para sistemas basados en Debian/Ubuntu:

```
sudo apt update
sudo apt install ufw
```

```
(root@kali)-[~]
# sudo apt update
sudo apt install ufw
```

Verificar el estado:

```
sudo ufw status # o sudo firewall-cmd --state
```

```
(root@kali)-[~]
# sudo ufw status
Status: inactive
```

Parte 2: Configuración Básica del Firewall

Paso 3: Configuración de Políticas por Defecto

UFW:

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
```

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

Paso 4: Permitir Tráfico para Servicios Específicos

```
sudo ufw allow ssh
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
```

```
(root@kali)-[~]
# sudo ufw allow ssh
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
```

Parte 3: Configuración Avanzada del Firewall en Kali Linux (UFW)

✓ Paso 5: Crear Reglas de Filtrado por IP

Permitir tráfico **solo desde una IP específica** al puerto SSH (22):

```
sudo ufw allow from 192.168.1.100 to any port 22
```

```
(root@kali)-[~]
# sudo ufw allow from 192.168.1.100 to any port 22
sudo ufw deny from 10.0.0.0/8
Rules updated
Rules updated
```

Denegar tráfico de una red completa (por ejemplo, red privada 10.0.0.0/8):

```
sudo ufw deny from 10.0.0.0/8
```

```
(root@kali)-[~]  
# sudo ufw deny from 10.0.0.0/8  
Skipping adding existing rule
```

Permitir tráfico desde una IP a un puerto específico (por ejemplo, 80):

```
sudo ufw allow from 192.168.1.50 to any port 80 proto tcp
```

```
(root@kali)-[~]  
# sudo ufw allow from 192.168.1.50 to any port 80 proto tcp  
Rules updated
```

✓ Paso 6: Configuración de Reglas para Redes Internas y Externas

Kali no maneja zonas como `firewalld`, pero puedes simular la separación interna/externa usando interfaces y reglas personalizadas.

1. Ver interfaces de red disponibles:

```
ip link show
```

```
(root@kali)-[~]  
# ip link show  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000  
    link/ether 08:00:27:c1:c9:eb brd ff:ff:ff:ff:ff:ff
```

2. Permitir servicios solo en interfaces específicas (usando `ufw` y reglas avanzadas de `iptables` si es necesario):

UFW por sí solo no soporta reglas por interfaz directamente, pero puedes hacer esto:

```
sudo ufw allow in on eth1 to any port 22
```

```
(root@kali)-[~]  
# sudo ufw allow in on eth1 to any port 22  
Rules updated  
Rules updated (v6)
```

Esto permite el puerto 22 **solo** si entra por la interfaz `eth1`.



Parte 4: Monitoreo y Ajustes del Firewall

✓ Paso 7: Monitoreo de Logs del Firewall

1. Habilitar logs de UFW:

```
sudo ufw logging on
```

```
(root@kali)-[~]  
# sudo ufw logging on  
Logging enabled
```

2. Ver logs en tiempo real:

```
sudo tail -f /var/log/ufw.log
```

```
(root@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
```

3. Buscar eventos específicos:

```
grep 'BLOCK' /var/log/ufw.log
```

```
(root@kali)-[~]  
# grep 'BLOCK' /var/log/ufw.log  
grep: /var/log/ufw.log: No such file or directory
```

✓ Paso 8: Ajuste de Reglas Basado en Monitoreo

1. Ver todas las reglas actuales:

```
sudo ufw status numbered
```

```
(root@kali)-[~]  
# sudo ufw status numbered  
Status: inactive
```

2. Eliminar una regla específica por número:

```
sudo ufw delete 2
```

```
(root@kali)-[~]
# sudo ufw delete 2
Deleting:
  allow 80/tcp
Proceed with operation (y|n)? y
Rules updated
```

3. Permitir tráfico detectado como bloqueado (tras análisis del log):

```
sudo ufw allow from [IP] to any port [PORT]
```

```
(root@kali)-[~]
# sudo ufw allow from 192.168.1.70 to any port 443 proto tcp
Rules updated
```