

**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”

```
Get:1 http://kali.download/kali kali-rolling InRelease [41.3 kB]
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) [327 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) [914 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.
```

```
(root@kali)~# ufw enable
Firewall is active and enabled on system startup
```

Ahora veremos las reglas actuales del cortafuego con iptables -L

```
File Actions Edit View Help
└─# 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
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
```

Ahora configuraremos la política para bloquear todo el tráfico entrante

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

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

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

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

```
(root@kali)-[~]
└─# iptables -P OUTPUT ACCEPT
```

Ahora permitiremos que el tráfico http, https y Ssh entré también

```
(root@kali)~# ufw allow http
Rule added
Rule added (v6)

File Actions Edit View Help
(root@kali)~# ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)

(root@kali)~# ufw allow https
Rule added
Rule added (v6)
```

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

```
(root@kali)~# iptables -A INPUT -p tcp --dport 22 -j ACCEPT

(root@kali)~# iptables -A INPUT -p tcp --dport 80 -j ACCEPT

(root@kali)~# iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

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

```
(root@kali)~# ufw status numbered
Status: active

    To Action From
    --
[ 1] 22/tcp ALLOW IN Anywhere
[ 2] 80/tcp ALLOW IN Anywhere
[ 3] 443/tcp ALLOW IN Anywhere
[ 4] Anywhere ALLOW IN 192.168.1.9
[ 5] 443 ALLOW IN Anywhere
[ 6] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 7] 80/tcp (v6) ALLOW IN Anywhere (v6)
[ 8] 443/tcp (v6) ALLOW IN Anywhere (v6)
[ 9] 443 (v6) ALLOW IN Anywhere (v6)
```

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:

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

Para denegar el trafico externo a puertos no esenciales:

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

```
(root@kali)-[~]  
# iptables -A INPUT -p tcp --dport 8080 -j DROP
```

## MONITOREO Y AJUSTES DE FIREWALL

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

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

Ahora revisamos los logs

```
(root@kali)-[~]  
# sudo journalctl -f | grep UFW
```

Si queremos habilitar los logs por iptable:

```
(root@kali)-[~]  
# sudo iptables -A INPUT -j LOG --log-prefix "IPTables-Dropped: " --log-level 4
```

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

```
(root@kali)-[~]  
# sudo journalctl -f | grep UFW
```