# EJERCICIOS ARPWATCH

EJERCICIOS SENCILLOS OBLIGATORIOS

**Ejercicio 1 — Instalar arpwatch**

**Objetivo:** tener la herramienta lista.

sudo apt update

sudo apt install -y arpwatch

✅ **Qué comprobar:** que la instalación termina sin errores.

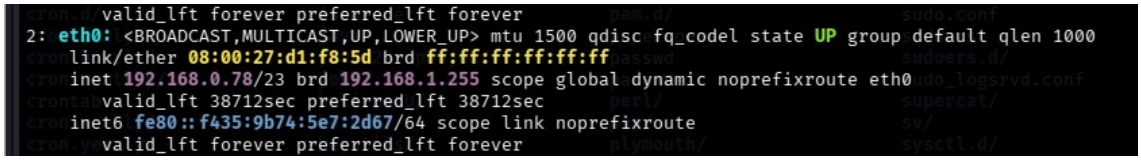
---

🔹 **Ejercicio 2 — Ver la interfaz de red**

**Objetivo:** identificar la interfaz que se va a vigilar.

ip addr show

✅ **Qué anotar:** el nombre de la interfaz (ej.: eth0, enp0s3, wlan0).




---

🔹 **Ejercicio 3 — Arrancar arpwatch**

**Objetivo:** poner en marcha el programa.

sudo arpwatch -i eth0 -d

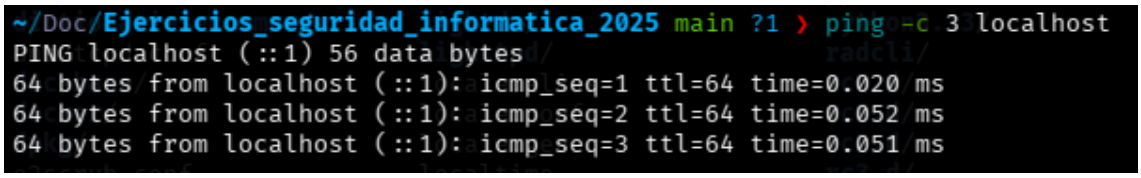
(reemplaza eth0 por la interfaz que hayas visto en el Ejercicio 2).
✅ **Qué verás:** la consola queda “escuchando” la red.


---

🔹 **Ejercicio 4 — Generar un evento**

**Objetivo:** que arpwatch detecte algo nuevo.

- Abre **otra terminal** y haz ping a cualquier dirección de tu red:
- ping -c 3 192.168.1.1

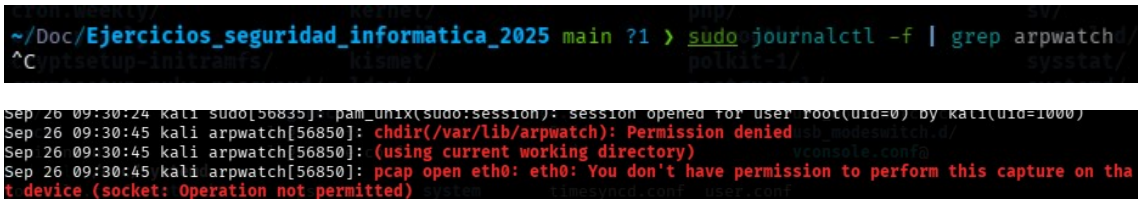


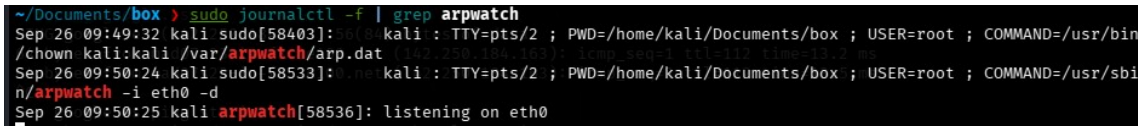

✅ **Qué verás:** en la terminal de arpwatch aparecerá una línea con new station (IP + MAC).

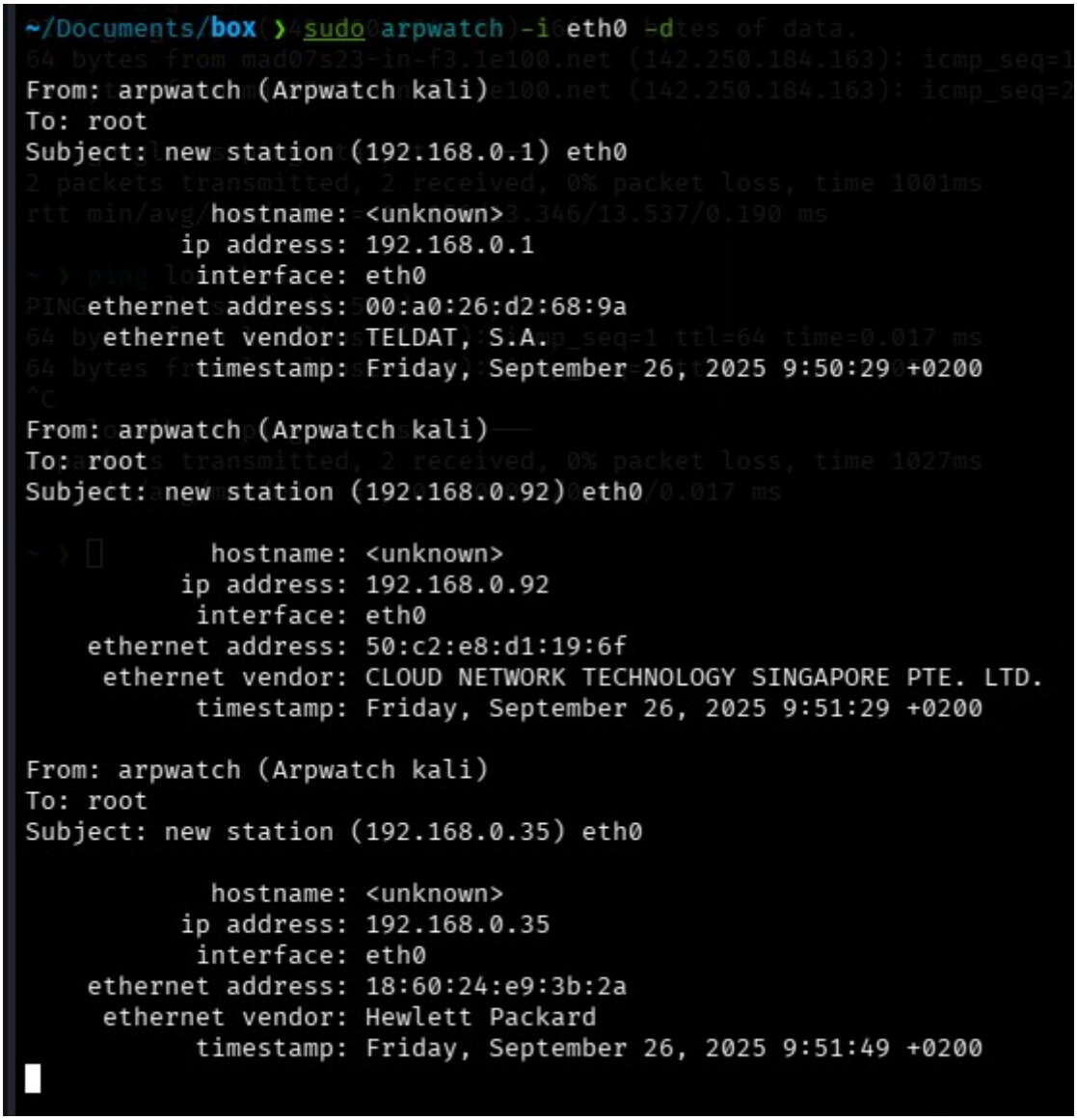
---

**Objetivo:** comprobar que queda registrado el evento.

sudo journalctl -f | grep arpwatch






## EJERCICIOS AVANZADOS OPCIONALES

### Ejercicio 1 — Instalar arpwatch

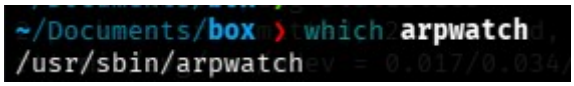
**Objetivo: tener la herramienta disponible.**

**sudo apt update**

**sudo apt install -y arpwatch**

**which arpwatch**

**arpwatch -v**




**Observa: ruta del binario y versión. Si no aparece, revisa errores de instalación.**

---

## Ejercicio 2 — Identificar la interfaz de red

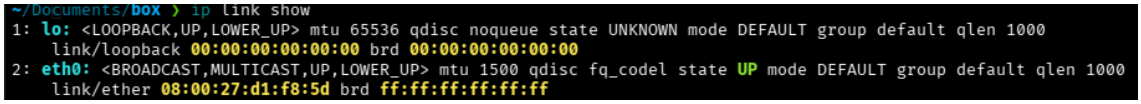
**Objetivo: saber qué interfaz monitorizar.**

**ip link show**

**# o**

**ip addr show**

**Observa: nombre de la interfaz (p. ej. eth0, enp0s3, wlan0). Usa ese nombre en los siguientes ejercicios.**




---

## Ejercicio 3 — Arrancar arpwatch en primer plano (modo debug)

**Objetivo: ver la salida directa para entender su funcionamiento.**

**sudo arpwatch -i eth0 -d**

**(Reemplaza eth0 por tu interfaz.)**
**Observa: mensajes en pantalla sobre nuevas estaciones o cambios ARP.**

---

## Ejercicio 4 — Ejecutar arpwatch como servicio y comprobar proceso

**Objetivo: poner como servicio y confirmarlo.**

**# systemd**

**sudo systemctl enable --now arpwatch**

**ps aux | grep arpwatch**

**# alternativa si no hay servicio:**

**sudo pkill -f arpwatch; sudo arpwatch -i eth0 -d &**

**Observa: la línea en ps con el proceso arpwatch y su PID.**

```
~/Documents/box ❯ ps aux | grep arpwatch
root       58533  0.0  0.1  22252  8280 pts/2    S+   09:50   0:00 sudo arpwatch -i eth0 -d
root       58535  0.0  0.0  22252  2708 pts/1    Ss   09:50   0:00 sudo arpwatch -i eth0 -d
root       58536  0.0  0.1  11432  6620 pts/1    S+   09:50   0:00 arpwatch -i eth0 -d
kali       58547  0.0  0.0   6660  2340 pts/0    S+   09:50   0:00 grep --color=auto arpwatch
kali       58784  0.0  0.0   6528  2268 pts/6    S+   09:56   0:00 grep --color=auto arpwatch
```

---

## Ejercicio 5 — Monitorizar logs en tiempo real

**Objetivo: ver las alertas que genera arpwatch.**

**# si tu sistema usa syslog**

**sudo tail -f /var/log/syslog | grep -i arpwatch**

**# si usa systemd/journal (Kali, etc.)**

**sudo journalctl -f | grep -i arpwatch**

**Observa: entradas tipo new station o changed ethernet address.**

---

## ~~Ejercicio 6 — Conectar un nuevo host (generar evento)~~

~~**Objetivo: provocar un evento de "nueva estación" y verlo en logs.**~~

- ~~**Levanta una VM extra o conecta un móvil a la misma red/segmento.**~~
- ~~**Observa los logs (usa el comando del ejercicio 5).**~~
  ~~**Observa: línea new station <IP> <MAC> en los logs.**~~

---

## Ejercicio 7 — Cambiar la MAC local y comprobar alerta

**Objetivo: cambiar temporalmente la MAC y ver la detección.**

**# bajar interfaz**

**sudo ip link set dev eth0 down**

**# cambiar MAC (ejemplo)**

**sudo ip link set dev eth0 address 02:11:22:33:44:55**

**# subir interfaz**

**sudo ip link set dev eth0 up**

**# observar logs**

**sudo journalctl -f | grep -i arpwatch**

**(Reemplaza eth0 y la MAC según tu caso.)**
**Observa: arpwatch registra changed ethernet address para la IP afectada.**

---

## Ejercicio 8 — Consultar la base de datos de arpwatch

**Objetivo: ver el historial que guarda arpwatch.**

**sudo ls -l /var/lib/arpwatch**

**sudo sed -n '1,80p' /var/lib/arpwatch/arp.dat**

**Observa: entradas con IP, MAC y marcas de tiempo.**

---

## Ejercicio 9 — Añadir una entrada ARP estática (mitigación)

**Objetivo: fijar una IP↔️MAC para protegerla en el equipo local.**

**# sintaxis moderna recomendada**

**sudo ip neigh add 192.168.1.143 lladdr 9f:4b:0c:9f:14:cb nud permanent dev eth0**

**# comprobar**

**ip neigh show**

**Observa: que la entrada aparece como PERMANENT o REACHABLE según sistema.**

---

## Ejercicio 10 — Parar y limpiar la práctica

**Objetivo: dejar el entorno como estaba.**

**# parar arpwatch**

**sudo systemctl stop arpwatch**

**# eliminar entrada ARP creada (ejemplo)**

**sudo ip neigh del 192.168.1.143 dev eth0**

**# comprobar que ya no existe**

**ip neigh show**