

EJERCICIOS ARPWATCH

EJERCICIOS SENCILLOS OBLIGATORIOS

Ejercicio 1 — Instalar arpwat

Objetivo: tener la herramienta lista.

`sudo apt update`

`sudo apt install -y arpwat`

✓ **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).

```
crn @ valid_lft forever preferred_lft forever          pan.d/          sudo.conf
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
crn link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff      passwd          sudoers.d/
crn inet 192.168.0.78/23 brd 192.168.1.255 scope global dynamic noprefixroute eth0 do_logsrvd.conf
crn @ valid_lft 38712sec preferred_lft 38712sec        pass/          supercat/
crn inet6 fe80::f435:9b74:5e7:2d67/64 scope link noprefixroute
crn @ valid_lft forever preferred_lft forever          plymouth/      avsctl.d/
```

♦ Ejercicio 3 — Arrancar arpwat

Objetivo: poner en marcha el programa.

`sudo arpwat -i eth0 -d`

(reemplaza eth0 por la interfaz que hayas visto en el Ejercicio 2).

✓ **Qué verás:** la consola queda “escuchando” la red.

```
lepmo@d/          libnl-3/          pulse/
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo arpwat -i eth0 -d
```

♦ 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`

```
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > ping -c 3 localhost
PING localhost (::1) 56 data bytes:
64 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.020 ms
64 bytes from localhost (::1): icmp_seq=2 ttl=64 time=0.052 ms
64 bytes from localhost (::1): icmp_seq=3 ttl=64 time=0.051 ms
```

✓ **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`

```
~/Doc/Ejercicios_seguridad_informatica_2025 main ?1 > sudo journalctl -f | grep arpwatch
Sep 26 09:30:24 kali sudo[56835]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
Sep 26 09:30:45 kali arpwatch[56850]: chdir(/var/lib/arpwatch): Permission denied
Sep 26 09:30:45 kali arpwatch[56850]: (using current working directory)
Sep 26 09:30:45 kali arpwatch[56850]: pcap open eth0: eth0: You don't have permission to perform this capture on the device (socket: Operation not permitted)
```

```
~/Documents/box > sudo journalctl -f | grep arpswatch
Sep 26 09:49:32 kali sudo[58403]: 58403kali : TTY=pts/2 ; PWD=/home/kali/Documents/box ; USER=root ; COMMAND=/usr/bin/chown kali:kali /var/arpswatch/arp.dat
Sep 26 09:50:24 kali sudo[58533]: 58533kali : TTY=pts/2 ; PWD=/home/kali/Documents/box ; USER=root ; COMMAND=/usr/sbin/arpswatch -i eth0 -d
Sep 26 09:50:25 kali arpswatch[58536]: listening on eth0
```

EJERCICIOS AVANZADOS OPCIONALES

Objetivo: tener la herramienta disponible.

```
sudo apt install -y arpswatch
```

which arpwat

arpwatch -v

```
~/Documents/box > which arpwat
/usr/sbin/arpwatch-v = 0.017/0.034
```

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.

```
~/Documents/box > 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:d1:f8:5d brd ff:ff:ff:ff:ff:ff
```

Ejercicio 3 — Arrancar arpwat

Objetivo: ver la salida directa para entender su funcionamiento.

sudo arpwat -i eth0 -d

(Reemplaza eth0 por tu interfaz.)

Observa: mensajes en pantalla sobre nuevas estaciones o cambios ARP.

Ejercicio 4 — Ejecutar arpwat como servicio y comprobar proceso

Objetivo: poner como servicio y confirmarlo.

systemd

sudo systemctl enable --now arpwat

ps aux | grep arpwat

alternativa si no hay servicio:

sudo pkill -f arpwat; sudo arpwat -i eth0 -d &

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

```
~/Documents/box > ps aux | grep arpwat
root      58533  0.0  0.1  2252  8280 pts/2    S+   09:50   0:00 sudo arpwat -i eth0 -d
root      58535  0.0  0.0  2252  2708 pts/1    Ss   09:50   0:00 sudo arpwat -i eth0 -d
root      58536  0.0  0.1  11432  6620 pts/1    S+   09:50   0:00 arpwat -i eth0 -d
kali      58547  0.0  0.0   6660  2340 pts/0    S+   09:50   0:00 grep --color=auto arpwat
kali      58784  0.0  0.0   6528  2268 pts/6    S+   09:56   0:00 grep --color=auto arpwat
```

Ejercicio 5 — Monitorizar logs en tiempo real

Objetivo: ver las alertas que genera arpwat.

si tu sistema usa syslog

sudo tail -f /var/log/syslog | grep -i arpwat

si usa systemd/journal (Kali, etc.)

sudo journalctl -f | grep -i arpwat

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 arpwatc

sudo systemctl stop arpwatc

eliminar entrada ARP creada (ejemplo)

sudo ip neigh del 192.168.1.143 dev eth0

comprobar que ya no existe

ip neigh show