Ejercicios de tcpdump

🔷 Ejercicios básicos

1. Listar interfaces disponibles

tcpdump -D

```
~ ❯ tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
```

👉 Muestra todas las interfaces de red que tcpdump puede usar.

2. Capturar tráfico en la interfaz eth0

tcpdump -i eth0

```
~ ❯ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:46:40.433462 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 46
11:46:40.433919 ARP, Request who-has 10.0.2.15 tell 10.0.2.15, length 46
11:46:40.445894 ARP, Request who-has 192.168.0.228 (Broadcast) tell 192.168.0.90, length 46
11:46:40.467992 ARP, Request who-has 192.168.0.229 (Broadcast) tell 192.168.0.90, length 46
11:46:40.494289 ARP, Request who-has 192.168.0.230 (Broadcast) tell 192.168.0.90, length 46
11:46:40.515532 ARP, Request who-has 192.168.0.231 (Broadcast) tell 192.168.0.90, length 46
11:46:40.515817 IP 192.168.0.67.38237 > 254.red-80-58-61.staticip.rima-tde.net.domain: 20794+ PTR
9)
11:46:40.529575 IP 254.red-80-58-61.staticip.rima-tde.net.domain > 192.168.0.67.38237: 20794 NXDo
11:46:40.529637 IP 192.168.0.67.54903 > 254.red-80-58-61.staticip.rima-tde.net.domain: 40940+ PTR
40)
```

👉 Ver los primeros 20 paquetes que pasan por eth0.

3. Guardar captura en un fichero

tcpdump -i eth0 -w trafico.log

```
~ ❯ sudo tcpdump -i eth0 -w trafico.log
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C788 packets captured
790 packets received by filter
0 packets dropped by kernel
```

👉 Luego ábrelo con:

tcpdump -r trafico.log

```
~ ❯ tcpdump -r trafico.log
reading from file trafico.log, link-type EN10MB (Ethernet), snapshot length 262144
11:47:15.622547 IP6 fe80::aed:edff:feb5:aae6.dhcpv6-client > ff02::1:2.dhcpv6-server: dhcp6 solicit
11:47:15.668023 LLDP, length 228: PA1-LINKSYS
11:47:15.746134 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 46
11:47:15.746602 ARP, Request who-has 10.0.2.15 tell 10.0.2.15, length 46
11:47:16.174189 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 46
11:47:16.223062 IP 192.168.0.21.38809 > 239.255.255.250.1900: UDP, length 324
11:47:16.253567 IP 192.168.0.21.50573 > 239.255.255.250.1900: UDP, length 380
11:47:16.284503 IP 192.168.0.21.33152 > 239.255.255.250.1900: UDP, length 333
```

🔷 Filtrado por protocolos y puertos

4. Capturar solo tráfico TCP en eth0

tcpdump -i eth0 tcp

```
~ ❯ sudo tcpdump -i eth0 tcp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:49:42.231035 IP 192.168.0.67.42580 > ec2-35-157-26-135.eu-central-1.compute.amazonaws.com.https: Flags [
, win 64240, options [mss 1460,sackOK,TS val 1834136032 ecr 0,nop,wscale 7], length 0
11:49:42.275139 IP ec2-35-157-26-135.eu-central-1.compute.amazonaws.com.https > 192.168.0.67.42580: Flags [
, ack 244914225, win 65084, options [mss 1240,sackOK,TS val 2102530691 ecr 1834136032,nop,wscale 9], length
11:49:42.275162 IP 192.168.0.67.42580 > ec2-35-157-26-135.eu-central-1.compute.amazonaws.com.https: Flags [
2, options [nop,nop,TS val 1834136076 ecr 2102530691], length 0
11:49:42.275740 IP 192.168.0.67.42580 > ec2-35-157-26-135.eu-central-1.compute.amazonaws.com.https: Flags [
ck 1, win 502, options [nop,nop,TS val 1834136077 ecr 2102530691], length 968
11:49:42.319033 IP ec2-35-157-26-135.eu-central-1.compute.amazonaws.com.https > 192.168.0.67.42580: Flags [
131, options [nop,nop,TS val 2102530735 ecr 1834136077], length 0
```

5. Capturar tráfico en el puerto 80 (HTTP)

tcpdump -i eth0 tcp port 80

```
~ ❯ sudo tcpdump -i eth0 tcp port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel

~ ❯ sudo tcpdump -i eth0 tcp port 443
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:51:39.455721 IP 192.168.0.67.55584 > 172.64.152.233.https: Flags [P.], seq
options [nop,nop,TS val 3594464379 ecr 527903184], length 39
11:51:39.469361 IP 172.64.152.233.https > 192.168.0.67.55584: Flags [.], ack
```

6. Capturar tráfico DNS (UDP puerto 53)

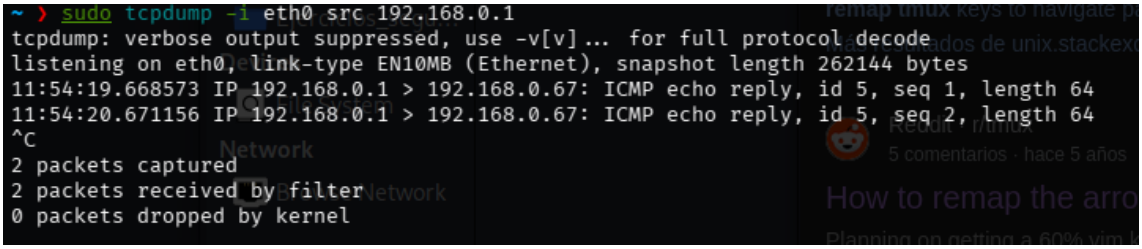
tcpdump -i eth0 udp port 53

```
~ ❯ sudo tcpdump -i eth0 udp port 53
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:52:23.780897 IP 192.168.0.67.35486 > 254.red-80-58-61.staticip.rima-tde.net.domain:
11:52:23.780922 IP 192.168.0.67.35486 > 254.red-80-58-61.staticip.rima-tde.net.domain:
11:52:23.801248 IP 254.red-80-58-61.staticip.rima-tde.net.domain > 192.168.0.67.35486:
11:52:23.801648 IP 254.red-80-58-61.staticip.rima-tde.net.domain > 192.168.0.67.35486:
2004 (60)
11:52:23.827114 IP 192.168.0.67.47269 > 254.red-80-58-61.staticip.rima-tde.net.domain:
. (43)
11:52:23.847952 IP 254.red-80-58-61.staticip.rima-tde.net.domain > 192.168.0.67.47269:
icip.rima-tde.net. (95)
11:52:23.848058 IP 192.168.0.67.40265 > 254.red-80-58-61.staticip.rima-tde.net.domain:
 (43)
```

🔷 Filtrado por IP

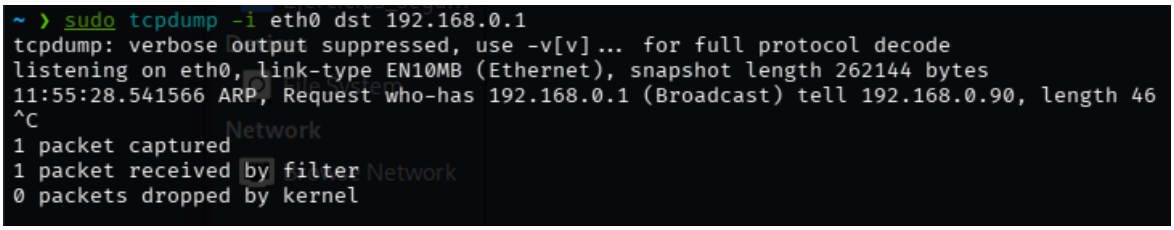
7. Tráfico desde una IP concreta (host origen)

tcpdump -i eth0 src 192.168.43.143



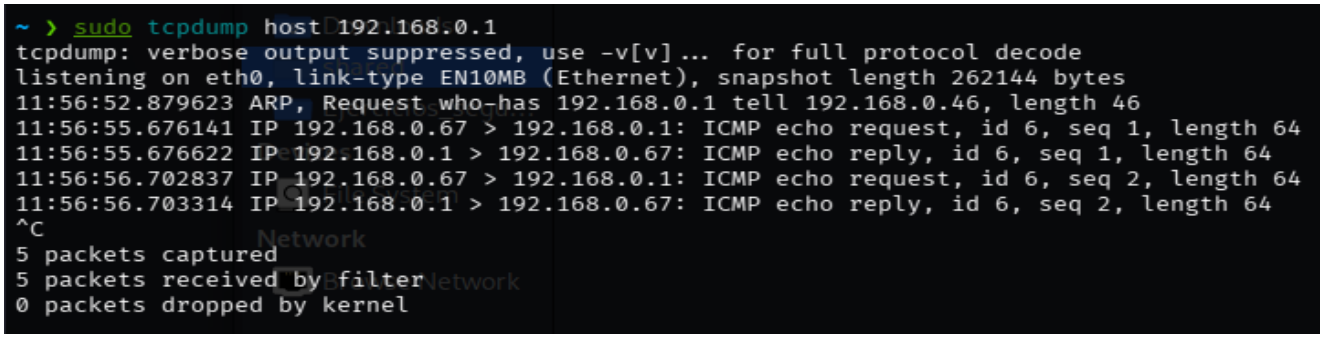
8. Tráfico hacia una IP concreta (host destino)

tcpdump -i eth0 dst 192.168.43.143



9. Tráfico de y hacia una IP concreta (host completo)

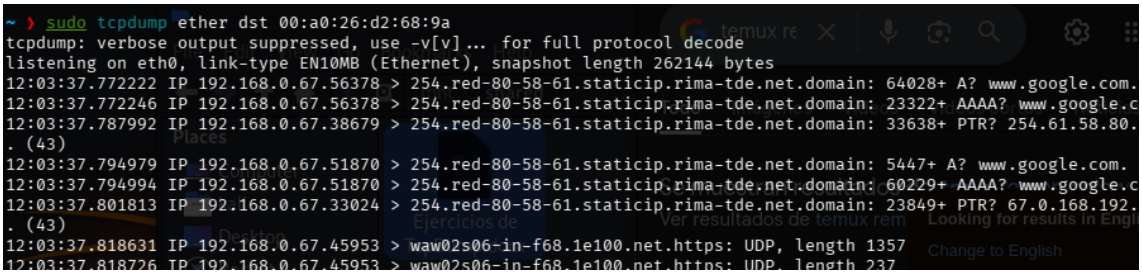
tcpdump host 192.168.1.143



🔷 Filtrado por MAC y red

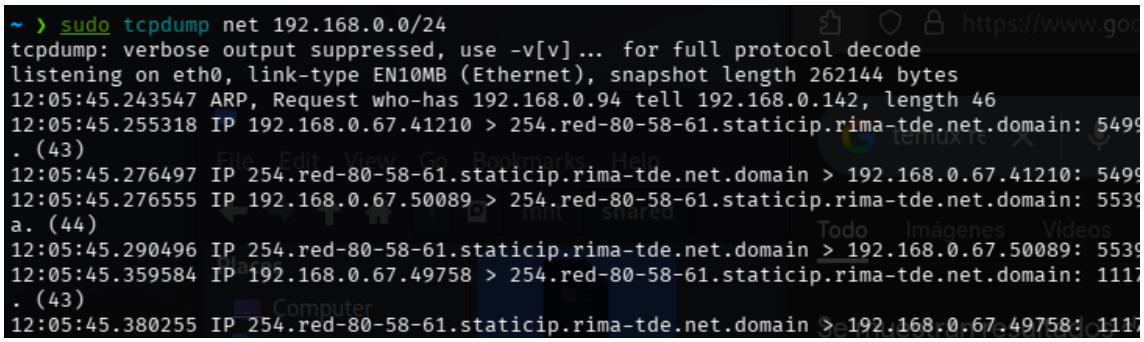
10. Tráfico con destino a una dirección MAC

tcpdump ether dst 8A:B1:11:A0:BC:53



11. **Tráfico de una red completa**

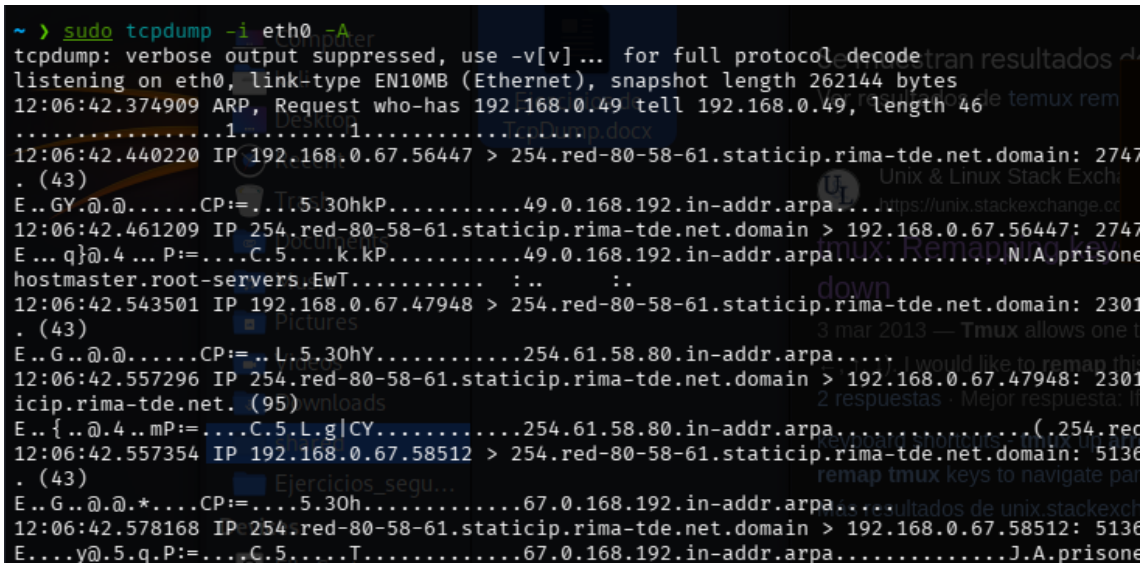
tcpdump net 192.168.43.0/24



🔷 **Visualización de datos**

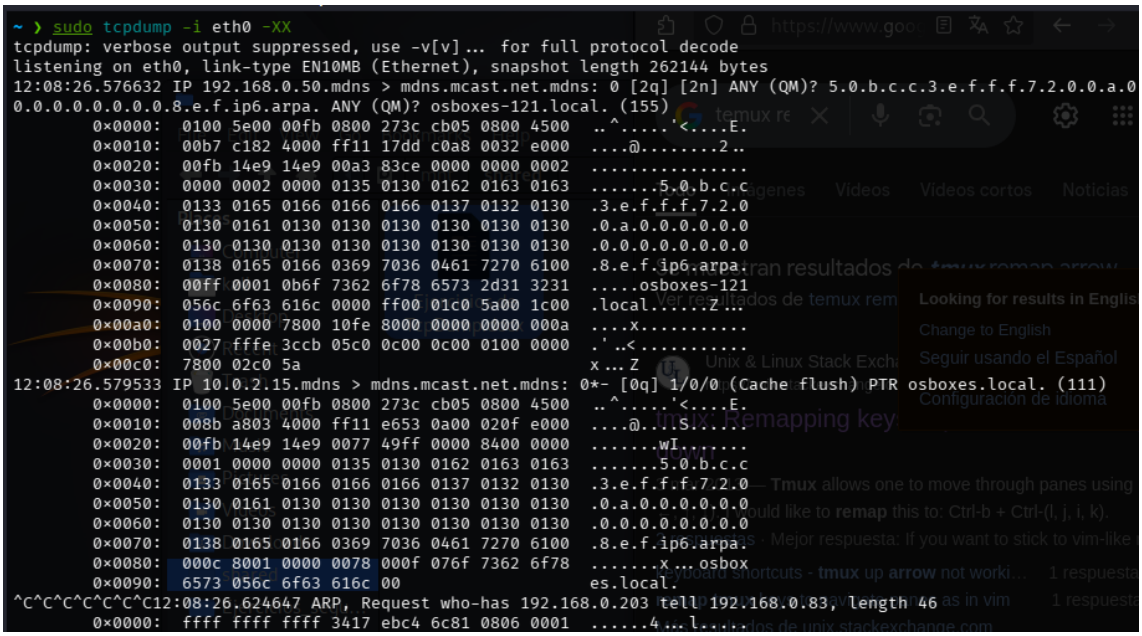
12. **Mostrar el contenido en ASCII**

tcpdump -i eth0 -A



13. **Mostrar el contenido en hexadecimal**

tcpdump -i eth0 -XX



🔷 Ejercicios combinados (operadores lógicos)

14. **Tráfico desde una IP y en puerto 80**

tcpdump -i eth0 src 192.168.43.143 and tcp port 80

```
~ ❯ sudo tcpdump -i eth0 src 192.168.0.67 and tcp port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:10:49.842701 IP 192.168.0.67.48640 > 0.0.0.80.http: Flags [S], seq 434171382,
4003977080 ecr 0,nop,wscale 7], length 0
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
```

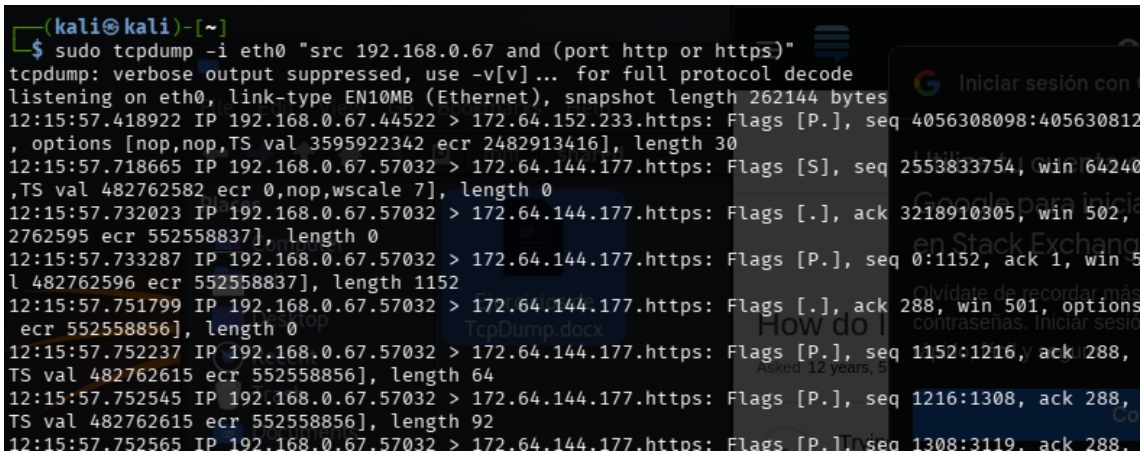
15. **Tráfico desde una IP excluyendo UDP**

tcpdump -i eth0 src 192.168.1.143 and not udp

```
~ ❯ sudo tcpdump -i eth0 src 192.168.0.1 and not udp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:11:42.593592 IP 192.168.0.1 > 192.168.0.67: ICMP host 192.168.0.1 unreachable, length 36
12:11:42.594542 IP 192.168.0.1 > 192.168.0.67: ICMP net 0.0.0.80 unreachable, length 36
12:11:45.553345 IP 192.168.0.1 > 192.168.0.67: ICMP host 192.168.0.1 unreachable, length 36
12:11:45.555279 IP 192.168.0.1 > 192.168.0.67: ICMP net 0.0.1.187 unreachable, length 36
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

16. **Tráfico desde una IP en HTTP o HTTPS**

tcpdump -i eth0 src 192.168.1.143 and (port http or https)



👉 Con esta lista de **16 ejercicios** tienes un recorrido completo:

- Empezando por capturar y guardar tráfico.
- Luego filtrando por protocolo, puerto, IP, MAC y red.
- Finalmente usando operadores lógicos y visualización en distintos formatos.