

# 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 NXDc
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

```
~ > sudo tcpdump -i eth0 src 192.168.0.1
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:54:19.668573 IP 192.168.0.1 > 192.168.0.67: ICMP echo reply, id 5, seq 1, length 64
11:54:20.671156 IP 192.168.0.1 > 192.168.0.67: ICMP echo reply, id 5, seq 2, length 64
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
```

### 8. Tráfico hacia una IP concreta (host destino)

---

tcpdump -i eth0 dst 192.168.43.143

```
~ > sudo tcpdump -i eth0 dst 192.168.0.1
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:55:28.541566 ARP, Request who-has 192.168.0.1 (Broadcast) tell 192.168.0.90, length 46
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
```

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

---

tcpdump host 192.168.1.143

```
~ > sudo tcpdump host 192.168.0.1
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:56:52.879623 ARP, Request who-has 192.168.0.1 tell 192.168.0.46, length 46
11:56:55.676141 IP 192.168.0.67 > 192.168.0.1: ICMP echo request, id 6, seq 1, length 64
11:56:55.676622 IP 192.168.0.1 > 192.168.0.67: ICMP echo reply, id 6, seq 1, length 64
11:56:56.702837 IP 192.168.0.67 > 192.168.0.1: ICMP echo request, id 6, seq 2, length 64
11:56:56.703314 IP 192.168.0.1 > 192.168.0.67: ICMP echo reply, id 6, seq 2, length 64
^C
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

## ◆ Filtrado por MAC y red

### 10. Tráfico con destino a una dirección MAC

---

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

```
~ > sudo tcpdump ether dst 00:a0:26:d2:68:9a
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:03:37.772222 IP 192.168.0.67.56378 > 254.red-80-58-61.staticip.rima-tde.net.domain: 64028+ A? www.google.com.
12:03:37.772246 IP 192.168.0.67.56378 > 254.red-80-58-61.staticip.rima-tde.net.domain: 23322+ AAAA? www.google.c
12:03:37.787992 IP 192.168.0.67.38679 > 254.red-80-58-61.staticip.rima-tde.net.domain: 33638+ PTR? 254.61.58.80.
. (43)
12:03:37.794979 IP 192.168.0.67.51870 > 254.red-80-58-61.staticip.rima-tde.net.domain: 5447+ A? www.google.com.
12:03:37.794994 IP 192.168.0.67.51870 > 254.red-80-58-61.staticip.rima-tde.net.domain: 60229+ AAAA? www.google.c
12:03:37.801813 IP 192.168.0.67.33024 > 254.red-80-58-61.staticip.rima-tde.net.domain: 23849+ PTR? 67.0.168.192.
. (43)
12:03:37.818631 IP 192.168.0.67.45953 > waw02s06-in-f68.1e100.net.https: UDP, length 1357
12:03:37.818726 IP 192.168.0.67.45953 > waw02s06-in-f68.1e100.net.https: UDP, length 237
```

## 11. Tráfico de una red completa

---

tcpdump net 192.168.43.0/24

```
~ > sudo tcpdump net 192.168.0.0/24
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:05:45.243547 ARP, Request who-has 192.168.0.94 tell 192.168.0.142, length 46
12:05:45.255318 IP 192.168.0.67.41210 > 254.red-80-58-61.staticip.rima-tde.net.domain: 5499
. (43)
12:05:45.276497 IP 254.red-80-58-61.staticip.rima-tde.net.domain > 192.168.0.67.41210: 5499
12:05:45.276555 IP 192.168.0.67.50089 > 254.red-80-58-61.staticip.rima-tde.net.domain: 5539
a. (44)
12:05:45.290496 IP 254.red-80-58-61.staticip.rima-tde.net.domain > 192.168.0.67.50089: 5539
12:05:45.359584 IP 192.168.0.67.49758 > 254.red-80-58-61.staticip.rima-tde.net.domain: 1117
. (43)
12:05:45.380255 IP 254.red-80-58-61.staticip.rima-tde.net.domain > 192.168.0.67.49758: 1117
```

### ◆ Visualización de datos

## 12. Mostrar el contenido en ASCII

---

tcpdump -i eth0 -A

```
~ > sudo tcpdump -i eth0 -A
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:06:42.374909 ARP, Request who-has 192.168.0.49 tell 192.168.0.49, length 46
.....1.....1.....
12:06:42.440220 IP 192.168.0.67.56447 > 254.red-80-58-61.staticip.rima-tde.net.domain: 2747
. (43)
E..G.Y.@.@.....CP:=...L.5.30hkP.....49.0.168.192.in-addr.arpa.....
12:06:42.461209 IP 254.red-80-58-61.staticip.rima-tde.net.domain > 192.168.0.67.56447: 2747
E...q}@.4...P:=...C.5.....k.kP.....49.0.168.192.in-addr.arpa.....N.A.prison
hostmaster.root-servers.EwT.....:..:..
12:06:42.543501 IP 192.168.0.67.47948 > 254.red-80-58-61.staticip.rima-tde.net.domain: 2301
. (43)
E..G..@.@.....CP:=...L.5.30hY.....254.61.58.80.in-addr.arpa.....
12:06:42.557296 IP 254.red-80-58-61.staticip.rima-tde.net.domain > 192.168.0.67.47948: 2301
icip.rima-tde.net. (95)
E..{..@.4..mP:=...C.5.L.g|CY.....254.61.58.80.in-addr.arpa.....(.254.red
12:06:42.557354 IP 192.168.0.67.58512 > 254.red-80-58-61.staticip.rima-tde.net.domain: 5136
. (43)
E..G..@.@.*.....CP:=...5.30h.....67.0.168.192.in-addr.arpa.....
12:06:42.578168 IP 254.red-80-58-61.staticip.rima-tde.net.domain > 192.168.0.67.58512: 5136
E....v@.5.q.P:=...C.5.....T.....67.0.168.192.in-addr.arpa.....J.A.prison
```

## 13. Mostrar el contenido en hexadecimal

---

tcpdump -i eth0 -XX



```
~ > sudo tcpdump -i eth0 -XX
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:08:26.576632 IP 192.168.0.50.mdns > mdns.mcast.net.mdns: 0 [2q] [2n] ANY (QM)? 5.0.b.c.c.3.e.f.f.7.2.0.0.a.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. ANY (QM)? osboxes-121.local. (155)
0x0000: 0100 5e00 00fb 0800 273c cb05 0800 4500 ..^.....<....E.
0x0010: 00b7 c182 4000 ff11 17dd c0a8 0032 e000 ....@.....2..
0x0020: 00fb 14e9 14e9 00a3 83ce 0000 0000 0002 .....
0x0030: 0000 0002 0000 0135 0130 0162 0163 0163 .....5.0.b.c.c
0x0040: 0133 0165 0166 0166 0166 0137 0132 0130 .3.e.f.f.7.2.0
0x0050: 0130 0161 0130 0130 0130 0130 0130 0130 .0.a.0.0.0.0.0
0x0060: 0130 0130 0130 0130 0130 0130 0130 0130 .0.0.0.0.0.0.0
0x0070: 0138 0165 0166 0369 7036 0461 7270 6100 .8.e.f.ip6.arpa
0x0080: 00ff 0001 0b6f 7362 6f78 6573 2d31 3231 .....osboxes-121
0x0090: 056c 6f63 616c 0000 ff00 01c0 5a00 1c00 .local.121
0x00a0: 0100 0000 7800 10fe 8000 0000 0000 000a ....X.....
0x00b0: 0027 fffe 3ccb 05c0 0c00 0c00 0100 0000 ..'<.....
0x00c0: 7800 02c0 5a ..x...Z
12:08:26.579533 IP 10.0.2.15.mdns > mdns.mcast.net.mdns: 0* [0q] 1/0/0 (Cache flush) PTR osboxes.local. (111)
0x0000: 0100 5e00 00fb 0800 273c cb05 0800 4500 ..^.....<....E.
0x0010: 008b a803 4000 ff11 e653 0a00 020f e000 ....@.....
0x0020: 00fb 14e9 14e9 0077 49ff 0000 8400 0000 .....wI.....
0x0030: 0001 0000 0000 0135 0130 0162 0163 0163 .....5.0.b.c.c
0x0040: 0133 0165 0166 0166 0166 0137 0132 0130 .3.e.f.f.7.2.0
0x0050: 0130 0161 0130 0130 0130 0130 0130 0130 .0.a.0.0.0.0.0
0x0060: 0130 0130 0130 0130 0130 0130 0130 0130 .0.0.0.0.0.0.0
0x0070: 0138 0165 0166 0369 7036 0461 7270 6100 .8.e.f.ip6.arpa
0x0080: 000c 8001 0000 0078 000f 076f 7362 6f78 .....X...osbox
0x0090: 6573 056c 6f63 616c 00 es.local.
^C^C^C^C^C^C12:08:26.624647 ARP, Request who-has 192.168.0.203 tell 192.168.0.83, length 46 as in vim
0x0000: ffff ffff ffff 3417 ebc4 6c81 0806 0001 .....4...l.....
```

## ◆ 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)

```

(kali@kali)-[~]
$ sudo tcpdump -i eth0 "src 192.168.0.67 and (port http or https)"
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:15:57.418922 IP 192.168.0.67.44522 > 172.64.152.233.https: Flags [P.], seq 4056308098:405630812
, options [nop,nop,TS val 3595922342 ecr 2482913416], length 30
12:15:57.718665 IP 192.168.0.67.57032 > 172.64.144.177.https: Flags [S], seq 2553833754, win 64240
,TS val 482762582 ecr 0,nop,wscale 7], length 0
12:15:57.732023 IP 192.168.0.67.57032 > 172.64.144.177.https: Flags [.], ack 3218910305, win 502,
2762595 ecr 552558837], length 0
12:15:57.733287 IP 192.168.0.67.57032 > 172.64.144.177.https: Flags [P.], seq 0:1152, ack 1, win 5
l 482762596 ecr 552558837], length 1152
12:15:57.751799 IP 192.168.0.67.57032 > 172.64.144.177.https: Flags [.], ack 288, win 501, options
ecr 552558856], length 0
12:15:57.752237 IP 192.168.0.67.57032 > 172.64.144.177.https: Flags [P.], seq 1152:1216, ack 288,
TS val 482762615 ecr 552558856], length 64
12:15:57.752545 IP 192.168.0.67.57032 > 172.64.144.177.https: Flags [P.], seq 1216:1308, ack 288,
TS val 482762615 ecr 552558856], length 92
12:15:57.752565 IP 192.168.0.67.57032 > 172.64.144.177.https: Flags [P.], seq 1308:3119, ack 288,

```

👉 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.