Network tools: ifconfig

- ifconfig tool is used to configure network interfaces in Unix and Linux systems. It allows you to view and modify network configuration, such as IP addresses, subnet masks, active interfaces, and data transmission statistics

```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.249.136  netmask 255.255.240.0  broadcast 172.17.255.255
        inet6 fe80::8561:40f6:6741:200c  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:36:36  txqueuelen 1000  (Ethernet)
        RX packets 44  bytes 16075 (15.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 2942 (2.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Picture own elaboration

Network tools: ip

- ip tool is a command-line utility in Unix and Linux systems used to display and configure network information, including network interfaces, network routes, ARP tables, and firewall rules

```
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:36:36 brd ff:ff:ff:ff:ff:ff
    inet 172.17.249.136/20 brd 172.17.255.255 scope global dynamic noprefixroute eth0
       valid_lft 85878sec preferred_lft 85878sec
    inet6 fe80::8561:40f6:6741:200c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Picture own elaboration

Network tools: route

- route tool in Unix and Linux systems is used to display and manipulate the kernel routing table. It allows you to view the configured network routes on the system and add, delete, or modify routes

```
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.17.240.1    0.0.0.0         UG    100    0        0 eth0
10.0.0.0        0.0.0.0         255.0.0.0       U     0      0        0 eth1
172.17.240.0    0.0.0.0         255.255.240.0   U     100    0        0 eth0
```

Picture own elaboration

Network tools: ping

- ping tool is used to check network connectivity between two devices by sending ICMP Echo Request packets and waiting for ICMP Echo Reply responses

```
└─$ ping 10.0.0.100
PING 10.0.0.100 (10.0.0.100) 56(84) bytes of data.
64 bytes from 10.0.0.100: icmp_seq=1 ttl=64 time=0.033 ms
64 bytes from 10.0.0.100: icmp_seq=2 ttl=64 time=0.023 ms
64 bytes from 10.0.0.100: icmp_seq=3 ttl=64 time=0.027 ms
^C
── 10.0.0.100 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2032ms
rtt min/avg/max/mdev = 0.023/0.027/0.033/0.004 ms
```

Picture own elaboration

Network tools: fping

- fping tool is similar to ping, but it allows sending multiple ICMP Echo Request packets to multiple hosts simultaneously. This can be useful for testing connectivity to multiple hosts at once

```
└─$ fping -c 1 10.0.0.1 10.0.0.100
10.0.0.100 : [0], 64 bytes, 0.033 ms (0.033 avg, 0% loss)
10.0.0.1   : [0], timed out (NaN avg, 100% loss)

10.0.0.1   : xmt/rcv/%loss = 1/0/100%
10.0.0.100 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 0.033/0.033/0.033
```

Picture own elaboration

Network tools: netstat

- netstat tool displays detailed information about network connections, routing tables, interface statistics, and other network-related data on a system. It can show active connections, open ports, established connections, and much more

```
└─$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name

tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -

tcp6       0      0 :::22                   :::*                    LISTEN      -

tcp6       0      0 ::1:3350                :::*                    LISTEN      -
```

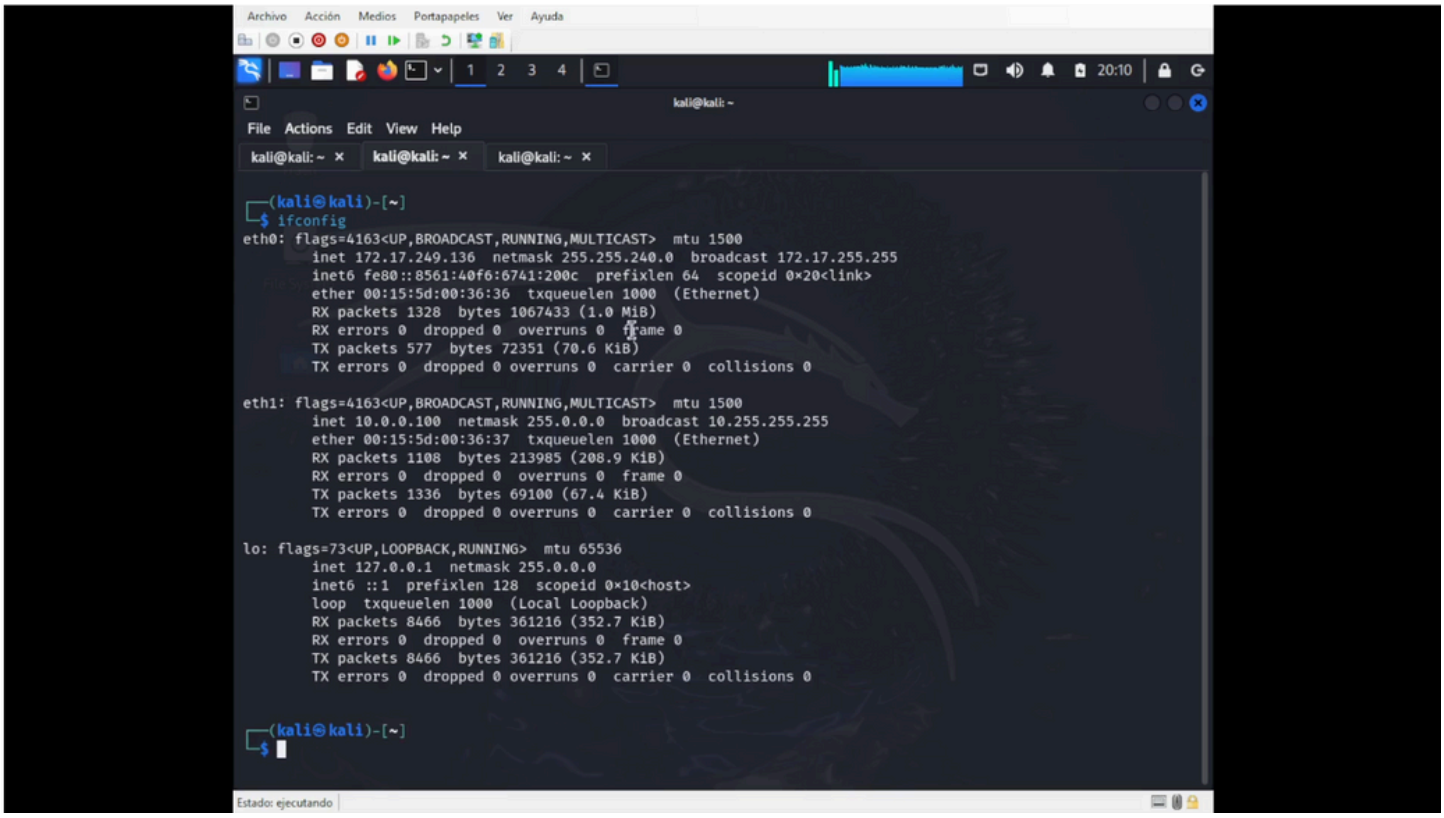
Picture own elaboration

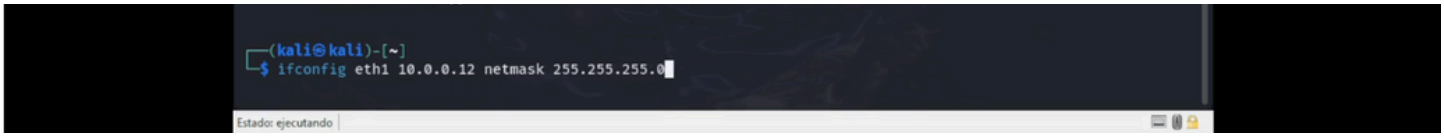
Network tools: hping3

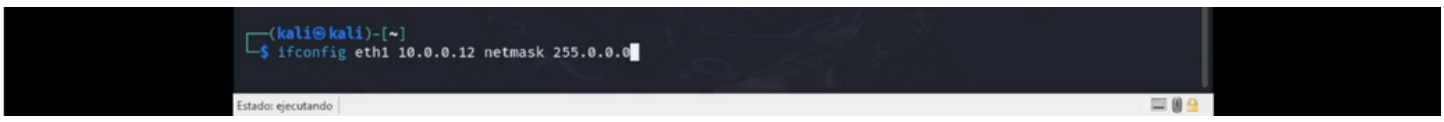
- hping3 tool is an advanced network utility that allows users to send TCP/IP packets and perform connectivity tests on a network. It can be used to send ICMP, TCP, and UDP packets with advanced configuration options such as specifying ports, packet sizes, and custom header fields

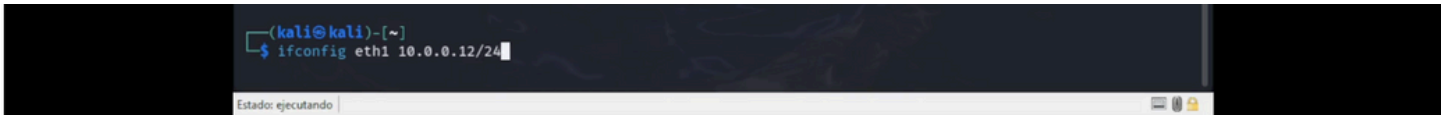
```
└─$ sudo hping3 -c 1 --faster -S --scan 20-500 10.0.0.20
Scanning 10.0.0.20 (10.0.0.20), port 20-500
481 ports to scan, use -V to see all the replies
+----+------------+---------+---+-----+-------+-----+
|port| serv name  |  flags  |ttl| id  | win   | len |
+----+------------+---------+---+-----+-------+-----+
   22 ssh        : .S..A...   64     0 29200    44
   80 http       : .S..A...   64     0 29200    44
All replies received. Done.
Not responding ports:
```

Picture own elaboration









```
┌──(kali㉿kali)-[~]
└─$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:36:36 brd ff:ff:ff:ff:ff:ff
    inet 172.17.249.136/20 brd 172.17.255.255 scope global dynamic noprefixroute eth0
       valid_lft 83477sec preferred_lft 83477sec
    inet6 fe80::8561:40f0:6741:200c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:36:37 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.100/8 brd 10.255.255.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet 10.0.0.12/24 scope global eth1
       valid_lft forever preferred_lft forever
    inet 10.0.0.22/24 scope global secondary eth1
       valid_lft forever preferred_lft forever
    inet 10.0.0.23/24 scope global secondary eth1
       valid_lft forever preferred_lft forever
    inet 10.0.0.24/24 scope global secondary eth1
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$
```

Estado: ejecutando

```
┌──(kali㉿kali)-[~]
└─$ sudo ip address add 10.0.0.30/24 dev eth1
```

Estado: ejecutando

```
┌──(kali㉿kali)-[~]
└─$ sudo ip address del 10.0.0.30/24 dev eth1
```

Estado: ejecutando

```
┌──(kali㉿kali)-[~]
└─$ ip route show
default via 172.17.240.1 dev eth0 proto dhcp src 172.17.249.136 metric 100
10.0.0.0/8 dev eth1 proto kernel scope link src 10.0.0.100
172.17.240.0/20 dev eth0 proto kernel scope link src 172.17.249.136 metric 100

┌──(kali㉿kali)-[~]
└─$
```

Estado: ejecutando

```
┌──(kali㉿kali)-[~]
└─$ ip route add 11.0.0.0/24 via 10.0.0.1
```

```
┌──(kali㉿kali)-[~]
└─$ ip route del 11.0.0.0/24
```

```
┌──(kali㉿kali)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.17.240.1    0.0.0.0         UG    100    0        0 eth0
10.0.0.0        0.0.0.0         255.0.0.0       U     0      0        0 eth1
172.17.240.0    0.0.0.0         255.255.240.0   U     100    0        0 eth0

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ route add -net 11.0.0.0 netmask 255.255.255.0 gw 10.0.0.1
```

```
┌──(kali㉿kali)-[~]
└─$ route del -net 11.0.0.0 netmask 255.255.255.0 gw 10.0.0.1
```

```
┌──(kali㉿kali)-[~]
└─$ route add default gw 10.0.0.1
```

```
┌──(kali㉿kali)-[~]
└─$ route del default gw 172.17.240.1
```

```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.0.20
PING 10.0.0.20 (10.0.0.20) 56(84) bytes of data.
64 bytes from 10.0.0.20: icmp_seq=1 ttl=64 time=0.768 ms
64 bytes from 10.0.0.20: icmp_seq=2 ttl=64 time=0.407 ms
64 bytes from 10.0.0.20: icmp_seq=3 ttl=64 time=0.348 ms
^C
── 10.0.0.20 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 0.348/0.507/0.768/0.185 ms

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ ping -c 2 10.0.0.20
PING 10.0.0.20 (10.0.0.20) 56(84) bytes of data.
64 bytes from 10.0.0.20: icmp_seq=1 ttl=64 time=0.561 ms
64 bytes from 10.0.0.20: icmp_seq=2 ttl=64 time=0.986 ms

── 10.0.0.20 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1021ms
rtt min/avg/max/mdev = 0.561/0.773/0.986/0.212 ms

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ fping 10.0.0.1 10.0.0.20 10.0.0.100
10.0.0.20 is alive
10.0.0.100 is alive
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.1
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.1
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.1
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.1
10.0.0.1 is unreachable
```

```
┌──(kali㉿kali)-[~]
└─$ fping -g 10.0.0.1 10.0.0.20
10.0.0.12 is alive
10.0.0.20 is alive

Estado: ejecutando
```

```
kali@kali: ~ ×   kali@kali: ~ ×   kali@kali: ~ ×
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.17
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.17
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.17
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.17
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.16
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.16
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.16
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.16
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.18
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.18
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.18
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.18
10.0.0.1 is unreachable
10.0.0.2 is unreachable
10.0.0.3 is unreachable
10.0.0.4 is unreachable
10.0.0.5 is unreachable
10.0.0.6 is unreachable
10.0.0.7 is unreachable
10.0.0.8 is unreachable
10.0.0.9 is unreachable
10.0.0.10 is unreachable
10.0.0.11 is unreachable
10.0.0.13 is unreachable
10.0.0.14 is unreachable
10.0.0.15 is unreachable
10.0.0.16 is unreachable
10.0.0.17 is unreachable
10.0.0.18 is unreachable
10.0.0.19 is unreachable

┌──(kali㉿kali)-[~]
└─$

Estado: ejecutando
```

```
┌──(kali㉿kali)-[~]
└─$ fping -a 10.0.0.1 10.0.0.20 10.0.0.100
10.0.0.20
10.0.0.100
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.1
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.1
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.1
ICMP Host Unreachable from 10.0.0.100 for ICMP Echo sent to 10.0.0.1

┌──(kali㉿kali)-[~]
└─$

Estado: ejecutando
```

```
┌──(kali㉿kali)-[~]
└─$ fping -h

Estado: ejecutando
```

```
┌──(kali㉿kali)-[~]
└─$ netstat -n
Completing external command
netsed       netsniff-ng  netstat
```

```
┌──(kali㉿kali)-[~]
└─$ netstat -p
```

Estado: ejecutando

```
┌──(kali㉿kali)-[~]
└─$ netstat -np
```

Estado: ejecutando

```
┌──(kali㉿kali)-[~]
└─$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

```
┌──(kali㉿kali)-[~]
└─$ netstat -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 kali.mshome.net:bootpc  DESKTOP-6H1D57V.:bootps ESTABLISHED

┌──(kali㉿kali)-[~]
└─$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 localhost:3350          [::]:*                  LISTEN
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     7564     /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     2879     /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     2881     /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM     LISTENING     2882     /run/systemd/io.systemd.ManagedOOM
unix  2      [ ACC ]     STREAM     LISTENING     9526     /tmp/ssh-BaUqCwl5Jxev/agent.1125
unix  2      [ ACC ]     STREAM     LISTENING     8636     /tmp/.ICE-unix/1125
unix  2      [ ACC ]     STREAM     LISTENING     2896     /run/systemd/fsck.progress
unix  2      [ ACC ]     STREAM     LISTENING     2902     /run/systemd/journal/stdout
unix  2      [ ACC ]     SEQPACKET  LISTENING     2904     /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     4165     /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING     9285     /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     9294     /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     9295     /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     9297     /run/user/1000/gcr/ssh
unix  2      [ ACC ]     STREAM     LISTENING     9299     /run/user/1000/keyring/control
```

```
┌──(kali㉿kali)-[~]
└─$ netstat -ltu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 localhost:3350          [::]:*                  LISTEN

┌──(kali㉿kali)-[~]
└─$
```

Estado: ejecutando

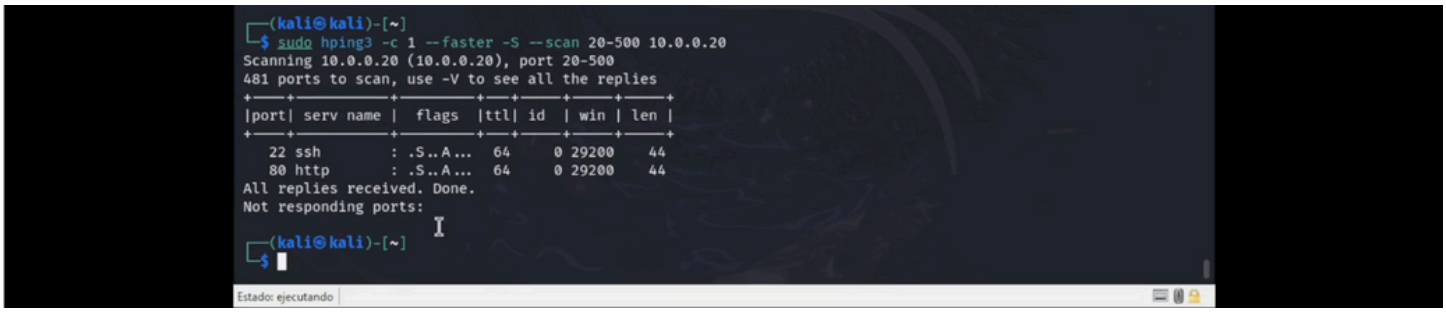
```
┌──(kali㉿kali)-[~]
└─$ netstat -ltun
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:3350                :::*                    LISTEN

┌──(kali㉿kali)-[~]
└─$
```

Estado: ejecutando

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -c 1 --fast -S --scan 20-500 10.0.0.20
[sudo] password for kali:
Scanning 10.0.0.20 (10.0.0.20), port 20-500
481 ports to scan, use -V to see all the replies
+----+-----------+--------+---+----+-----+-----+
|port| serv name |  flags |ttl| id | win | len |
+----+-----------+--------+---+----+-----+-----+
   22 ssh        : .S..A...  64     0 29200    44
   80 http       : .S..A...  64     0 29200    44
```

Estado: ejecutando


(kali㉿kali)-[~]
$ sudo hping3 -c 1 --faster -S --scan 20-500 10.0.0.20
Scanning 10.0.0.20 (10.0.0.20), port 20-500
481 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name | flags |ttl| id | win | len |
+----+-----------+---------+---+-----+-----+-----+
   22 ssh   : .S..A... 64   0 29200   44
   80 http   : .S..A... 64   0 29200   44
All replies received. Done.
Not responding ports:
(kali㉿kali)-[~]
$
Estado: ejecutando