

```
kali-linux-2025.2-vmware-a... x
File Actions Edit View Help
kali@kali: ~

(kali@kali)-[~]
$ ip addr 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 fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e7:ac:ee brd ff:ff:ff:ff:ff:ff
    inet 192.168.171.128/24 brd 192.168.171.255 scope global dynamic noprefixroute eth0
        valid_lft 1769sec preferred_lft 1769sec
    inet6 fe80::6aa2:5c5:6881:d577/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.171.128 netmask 255.255.255.0 broadcast 192.168.171.255
    inet6 fe80::6aa2:5c5:6881:d577 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:e7:ac:ee txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 830 (830.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27 bytes 3374 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$
```

```
kali-linux-2025.2-vmware-a... x
File Actions Edit View Help
kali@kali: ~

(kali@kali)-[~]
$ nmap -sS 192.168.171.128/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 07:23 EDT
Nmap scan report for 192.168.171.2
Host is up (0.000071s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 00:50:56:F3:9E:CA (VMware)

Nmap scan report for 192.168.171.254
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.171.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F8:F7:66 (VMware)

Nmap scan report for 192.168.171.128
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.171.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 7.31 seconds

(kali@kali)-[~]
$
```

Wireshark interface showing a packet capture of a TCP SYN scan. The top pane displays a list of packets, with packet 814 selected. The middle pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Network Time Protocol (NTP Version 4, client). The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
814	125.266884398	192.168.171.128	192.168.171.2	TCP	58	56873 → 5858 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
815	125.266902733	192.168.171.128	192.168.171.2	TCP	58	56873 → 85 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
816	125.266924193	192.168.171.128	192.168.171.2	TCP	58	56873 → 9228 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
817	125.266938976	192.168.171.2	192.168.171.128	TCP	60	27355 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
818	125.266931074	192.168.171.2	192.168.171.128	TCP	60	8831 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
819	125.266931151	192.168.171.2	192.168.171.128	TCP	60	5588 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
820	125.266937469	192.168.171.128	192.168.171.2	TCP	58	56873 → 39000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
821	125.266955258	192.168.171.128	192.168.171.2	TCP	58	56873 → 28201 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
822	125.266966094	192.168.171.128	192.168.171.2	TCP	58	56873 → 1832 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
823	125.266984134	192.168.171.128	192.168.171.2	TCP	58	56873 → 2949 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
824	125.266990041	192.168.171.2	192.168.171.128	TCP	60	85 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
825	125.266990129	192.168.171.2	192.168.171.128	TCP	60	9229 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
826	125.266990431	192.168.171.2	192.168.171.128	TCP	60	39000 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
827	125.267002138	192.168.171.128	192.168.171.2	TCP	58	56873 → 18048 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
828	125.267022440	192.168.171.128	192.168.171.2	TCP	58	56873 → 5825 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
829	125.267033943	192.168.171.128	192.168.171.2	TCP	58	56873 → 32777 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
830	125.267053710	192.168.171.128	192.168.171.2	TCP	58	56873 → 55056 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
831	125.267064950	192.168.171.128	192.168.171.2	TCP	58	56873 → 1688 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
832	125.267111453	192.168.171.2	192.168.171.128	TCP	60	23203 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
833	125.267104590	192.168.171.2	192.168.171.128	TCP	60	1832 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
834	125.267184058	192.168.171.2	192.168.171.128	TCP	60	2849 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
835	125.267184716	192.168.171.2	192.168.171.128	TCP	60	18048 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
836	125.267184784	192.168.171.2	192.168.171.128	TCP	60	5825 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
837	125.267184843	192.168.171.2	192.168.171.128	TCP	60	32777 → 56873 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0

Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0, id 0
Ethernet II, Src: VMware e7:ac:ee (00:0c:29:e7:ac:ee), Dst: VMware f3:9e:ca (00:50:56:f3:9e:ca)
Internet Protocol Version 4, Src: 192.168.171.128, Dst: 160.191.28.140
User Datagram Protocol, Src Port: 38310, Dst Port: 123
Network Time Protocol (NTP Version 4, client)

TCP_SYN_SCAN.pcapng Packets: 4549 Profile: Default

Wireshark interface showing a packet capture of a TCP SYN scan. The top pane displays a list of packets, with packet 2743 selected. The middle pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Network Time Protocol (NTP Version 4, client). The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2743	127.056905287	192.168.171.128	192.168.171.254	TCP	58	56875 → 8222 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2744	127.057084139	192.168.171.128	192.168.171.254	TCP	58	56875 → 56882 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2745	127.057015817	192.168.171.128	192.168.171.254	TCP	58	56875 → 1501 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2746	127.057033559	192.168.171.128	192.168.171.254	TCP	58	56875 → 45109 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2747	127.057045121	192.168.171.128	192.168.171.254	TCP	58	56875 → 20000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2748	127.057062269	192.168.171.128	192.168.171.254	TCP	58	56875 → 1082 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2749	127.057073705	192.168.171.128	192.168.171.254	TCP	58	56875 → 8100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2750	127.057090902	192.168.171.128	192.168.171.254	TCP	58	56875 → 7625 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2751	127.057102094	192.168.171.128	192.168.171.254	TCP	58	56875 → 44176 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2752	127.057119115	192.168.171.128	192.168.171.254	TCP	58	56875 → 912 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2753	127.057130200	192.168.171.128	192.168.171.254	TCP	58	56875 → 9929 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2754	127.057147427	192.168.171.128	192.168.171.254	TCP	58	56875 → 1836 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2755	127.057159232	192.168.171.128	192.168.171.254	TCP	58	56875 → 722 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2756	127.057177976	192.168.171.128	192.168.171.254	TCP	58	56873 → 8980 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2757	127.057188520	192.168.171.128	192.168.171.254	TCP	58	56873 → 16881 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2758	127.059570881	192.168.171.128	192.168.171.254	TCP	58	56875 → 1091 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2759	127.059590638	192.168.171.128	192.168.171.254	TCP	58	56875 → 3476 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2760	127.059622433	192.168.171.128	192.168.171.254	TCP	58	56875 → 2021 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2761	127.059635543	192.168.171.128	192.168.171.254	TCP	58	56875 → 5550 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2762	127.059654764	192.168.171.128	192.168.171.254	TCP	58	56875 → 1007 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2763	127.059660754	192.168.171.128	192.168.171.254	TCP	58	56875 → 1119 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2764	127.059684827	192.168.171.128	192.168.171.254	TCP	58	56875 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2765	127.059690515	192.168.171.128	192.168.171.254	TCP	58	56875 → 1801 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2766	127.059721931	192.168.171.128	192.168.171.254	TCP	58	56873 → 5254 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0, id 0
Ethernet II, Src: VMware e7:ac:ee (00:0c:29:e7:ac:ee), Dst: VMware f3:9e:ca (00:50:56:f3:9e:ca)
Internet Protocol Version 4, Src: 192.168.171.128, Dst: 160.191.28.140
User Datagram Protocol, Src Port: 38310, Dst Port: 123
Network Time Protocol (NTP Version 4, client)

TCP_SYN_SCAN.pcapng Packets: 4549 Profile: Default