

Nmap 7.95 scan initiated Mon Aug 4 18:56:29 2025 as: /usr/lib/nmap/nmap --privileged -sS -oN scan_results.txt 192.168.1.21/24

Nmap scan report for 192.168.1.1 Host is up (0.0083s latency). Not shown: 995 closed tcp ports (reset) PORT STATE SERVICE 22/tcp filtered ssh 23/tcp filtered telnet 53/tcp open domain 80/tcp open http 443/tcp open https MAC Address: 6C:4F:89:E7:4A:91 (Unknown)

Nmap scan report for 192.168.1.2 Host is up (0.00054s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 5357/tcp open wsdapi MAC Address: F8:FE:5E:80:5F:70 (Intel Corporate)

Nmap scan report for oppo17 (192.168.1.7) Host is up (0.047s latency). All 1000 scanned ports on oppo17 (192.168.1.7) are in ignored states. Not shown: 1000 closed tcp ports (reset) MAC Address: 0A:15:F7:50:C2:4D (Unknown)

Nmap scan report for 192.168.1.8 Host is up (0.023s latency). All 1000 scanned ports on 192.168.1.8 are in ignored states. Not shown: 1000 closed tcp ports (reset) MAC Address: AA:27:8D:E4:72:85 (Unknown)

Nmap scan report for 192.168.1.16 Host is up (0.038s latency). Not shown: 999 filtered tcp ports (no-response) PORT STATE SERVICE 2869/tcp open icslap MAC Address: F8:54:F6:22:DB:4B (AzureWave Technology)

Nmap scan report for 192.168.1.21 Host is up (0.000013s latency). All 1000 scanned ports on 192.168.1.21 are in ignored states. Not shown: 1000 closed tcp ports (reset)

└─(hemanth🌀kali)-[~]

Minimize all open windows and show the desktop

File Actions Edit View Help

Nmap done at Mon Aug 4 18:56:44 2025 -- 256 IP addresses (6 hosts up) scanned in 15.19 seconds

(hemanth@kali)-[~]

\$ nmap -sS 192.168.1.21/24

Starting Nmap 7.95 (<https://nmap.org>) at 2025-08-04 19:04 IST

Nmap scan report for 192.168.1.21

Host is up (0.0000030s latency).

All 1000 scanned ports on 192.168.1.21 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (1 host up) scanned in 29.48 seconds

(hemanth@kali)-[~]

\$ nmap -sS 192.168.1.21/24 -oN scan_results.txt

Starting Nmap 7.95 (<https://nmap.org>) at 2025-08-04 19:06 IST

Nmap scan report for 192.168.1.1

Host is up (0.020s latency).

Not shown: 995 closed tcp ports (reset)

PORT	STATE	SERVICE
------	-------	---------

22/tcp	filtered	ssh
--------	----------	-----

23/tcp	filtered	telnet
--------	----------	--------

53/tcp	open	domain
--------	------	--------

80/tcp	open	http
--------	------	------

443/tcp	open	https
---------	------	-------

MAC Address: 6C:4F:89:E7:54:51 (Unknown)

Nmap scan report for MSI (192.168.1.5)

Host is up (0.00076s latency).

Not shown: 996 closed tcp ports (reset)

PORT	STATE	SERVICE
------	-------	---------

135/tcp	open	msrpc
---------	------	-------

139/tcp	open	netbios-ssn
---------	------	-------------

445/tcp	open	microsoft-ds
---------	------	--------------

5357/tcp	open	wsdapi
----------	------	--------

MAC Address: F8:FE:5E:80:5F:70 (Intel Corporate)

Nmap scan report for ROY (192.168.1.13)

Host is up (0.072s latency).

All 1000 scanned ports on ROY (192.168.1.13) are in ignored states.

Not shown: 1000 closed tcp ports (reset)

MAC Address: EA:2F:E3:51:8F:DD (Unknown)

Nmap scan report for 192.168.1.21

Host is up (0.0000020s latency).

All 1000 scanned ports on 192.168.1.21 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 39.88 seconds

Packet capture with Wireshark.

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main display area is divided into three panes:

- Filter:** A green bar at the top of the packet list pane contains the filter expression `tcp.flags.syn == 1 and tcp.flags.ack == 1`.
- Packet List:** A table showing a list of captured packets. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The list shows multiple TCP SYN packets from various sources to 192.168.1.21.
- Packet Details:** The bottom pane shows the detailed view of the selected packet (No. 687). It displays the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.

A "Screenshot taken" dialog box is visible in the top right corner, with a "View image" button.

No.	Time	Source	Destination	Protocol	Length	Info
687	82.378324204	192.168.1.2	192.168.1.21	TCP	60	135 → 36566 [SYN, ACK] Seq=123456789
742	82.454346241	192.168.1.1	192.168.1.21	TCP	60	80 → 36566 [SYN, ACK] Seq=123456789
761	82.475410721	192.168.1.9	192.168.1.21	TCP	60	135 → 36566 [SYN, ACK] Seq=123456789
787	82.487768903	192.168.1.2	192.168.1.21	TCP	60	445 → 36566 [SYN, ACK] Seq=123456789
823	82.500847168	192.168.1.1	192.168.1.21	TCP	60	443 → 36566 [SYN, ACK] Seq=123456789
919	82.534080726	192.168.1.9	192.168.1.21	TCP	60	445 → 36566 [SYN, ACK] Seq=123456789
930	82.539686214	192.168.1.2	192.168.1.21	TCP	60	139 → 36566 [SYN, ACK] Seq=123456789
933	82.552122256	192.168.1.1	192.168.1.21	TCP	60	53 → 36566 [SYN, ACK] Seq=123456789
5330	83.510216352	192.168.1.2	192.168.1.21	TCP	60	5357 → 36566 [SYN, ACK] Seq=123456789
6781	83.994210434	192.168.1.9	192.168.1.21	TCP	60	135 → 36571 [SYN, ACK] Seq=123456789
6942	84.051719829	192.168.1.9	192.168.1.21	TCP	60	139 → 36566 [SYN, ACK] Seq=123456789
7706	85.329696667	192.168.1.9	192.168.1.21	TCP	60	135 → 36573 [SYN, ACK] Seq=123456789
8563	86.608061253	192.168.1.9	192.168.1.21	TCP	60	135 → 36575 [SYN, ACK] Seq=123456789
12624	174.434743224	192.168.1.16	192.168.1.21	TCP	60	2869 → 36566 [SYN, ACK] Seq=123456789
12660	175.909470752	192.168.1.16	192.168.1.21	TCP	60	2869 → 36571 [SYN, ACK] Seq=123456789
12720	177.347692772	192.168.1.16	192.168.1.21	TCP	60	2869 → 36573 [SYN, ACK] Seq=123456789
12771	180.012966224	192.168.1.16	192.168.1.21	TCP	60	2869 → 36575 [SYN, ACK] Seq=123456789
12841	181.454157528	192.168.1.16	192.168.1.21	TCP	60	2869 → 36577 [SYN, ACK] Seq=123456789
12929	182.731237131	192.168.1.16	192.168.1.21	TCP	60	2869 → 36579 [SYN, ACK] Seq=123456789

Frame 687: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0
Ethernet II, Src: Intel_80:5f:70 (f8:fe:5e:80:5f:70), Dst: 08:00:27:e4:34:0a, Length: 60
Internet Protocol Version 4, Src: 192.168.1.2, Destination: 192.168.1.21
Transmission Control Protocol, Src Port: 135, Dst Port: 36566

0000 08 00 27 e4 34 0a f8 fe 5e 80 5f 70 08 00 45
0010 00 2c fb dd 40 00 80 06 7b 86 c0 a8 01 02 c0
0020 01 15 00 87 8e d6 0c 12 c9 5f cd 7f 2b 72 60
0030 ff ff b6 ed 00 00 02 04 05 b4 00 00