Main
Broadband
Reviews
Articles
Forums
Info

Login
Please Login

Shortcuts
- 5300+ Routers
- 65535 Ports
- FAQs
- Glossary
- SG Broadband Tools
- SG IP Locator
- SG Network Tools
- SG Security Scan
- SG Speed Test
- TCP/IP Analyzer
- TCP/IP Optimizer

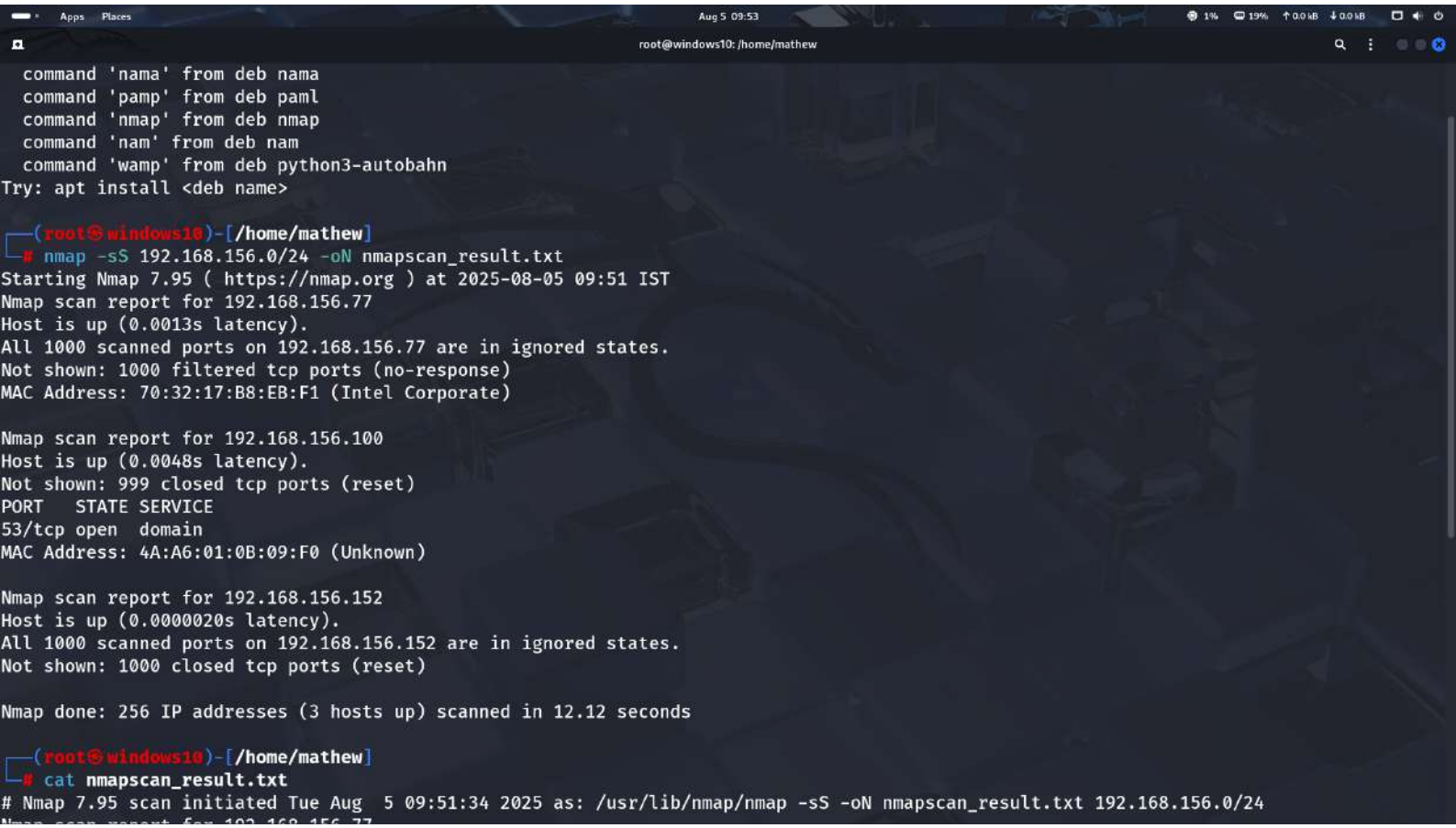
Port 135 Details

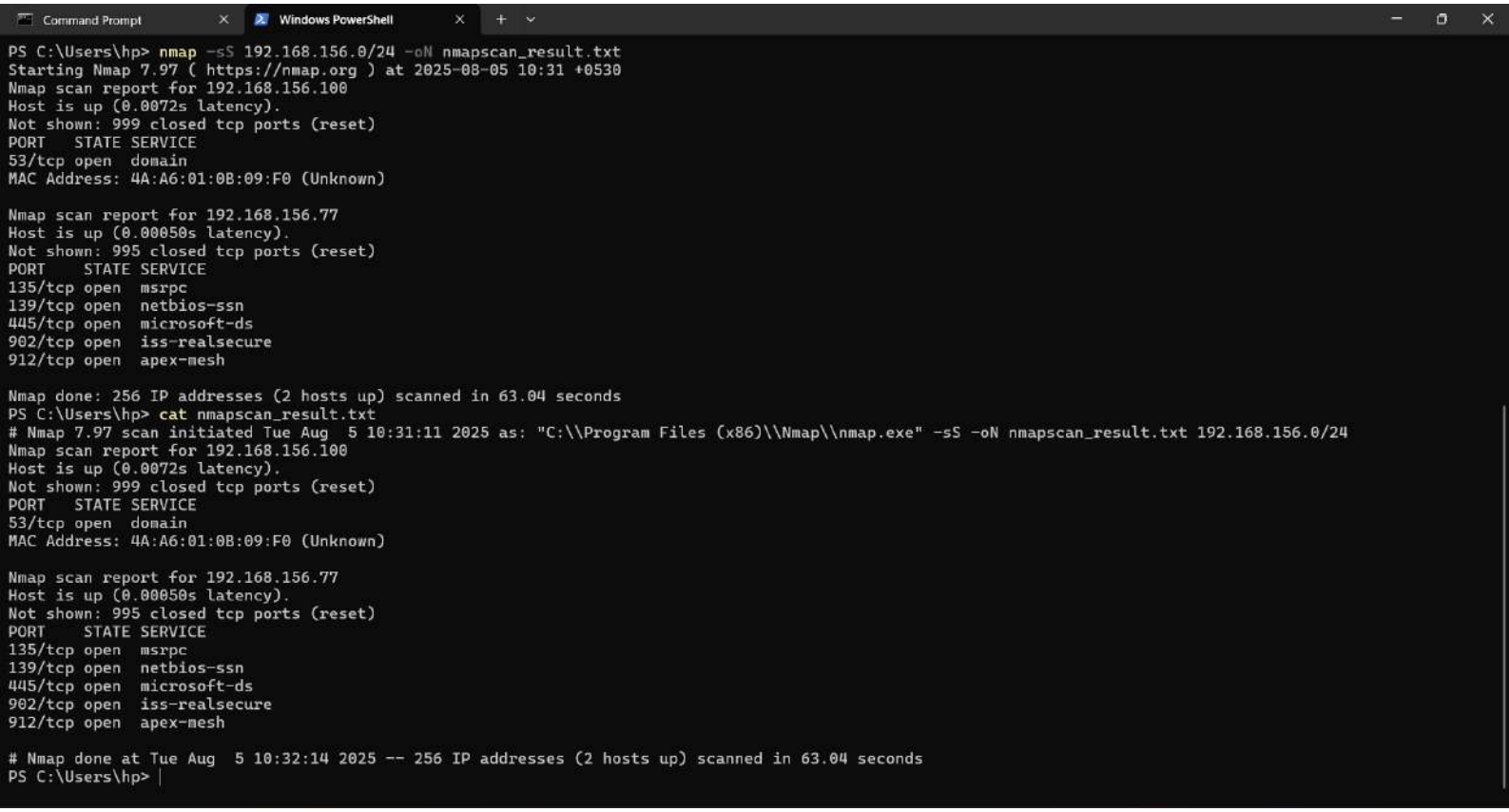
threat/application/port search: SEARCH

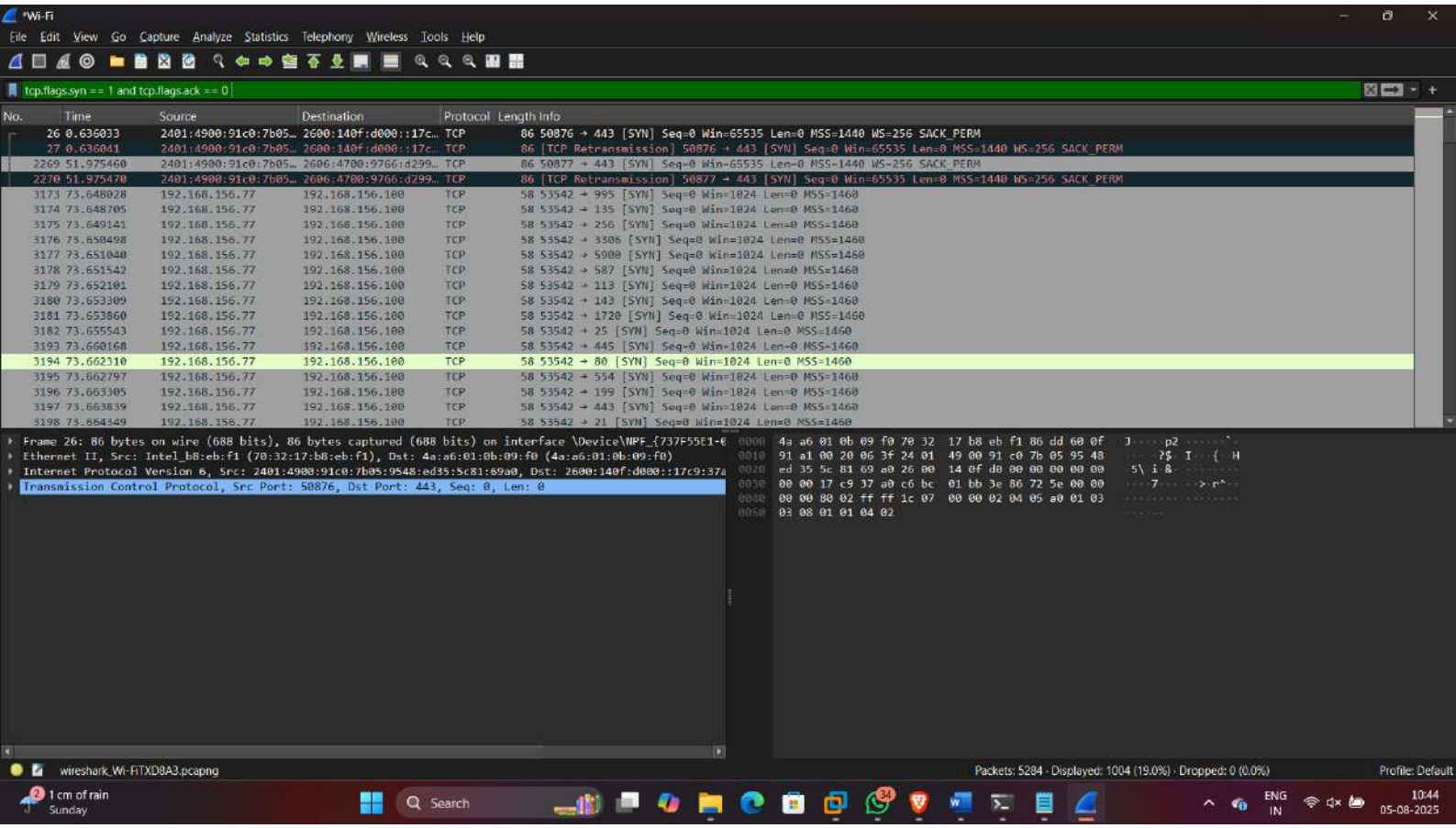
known port assignments and vulnerabilities

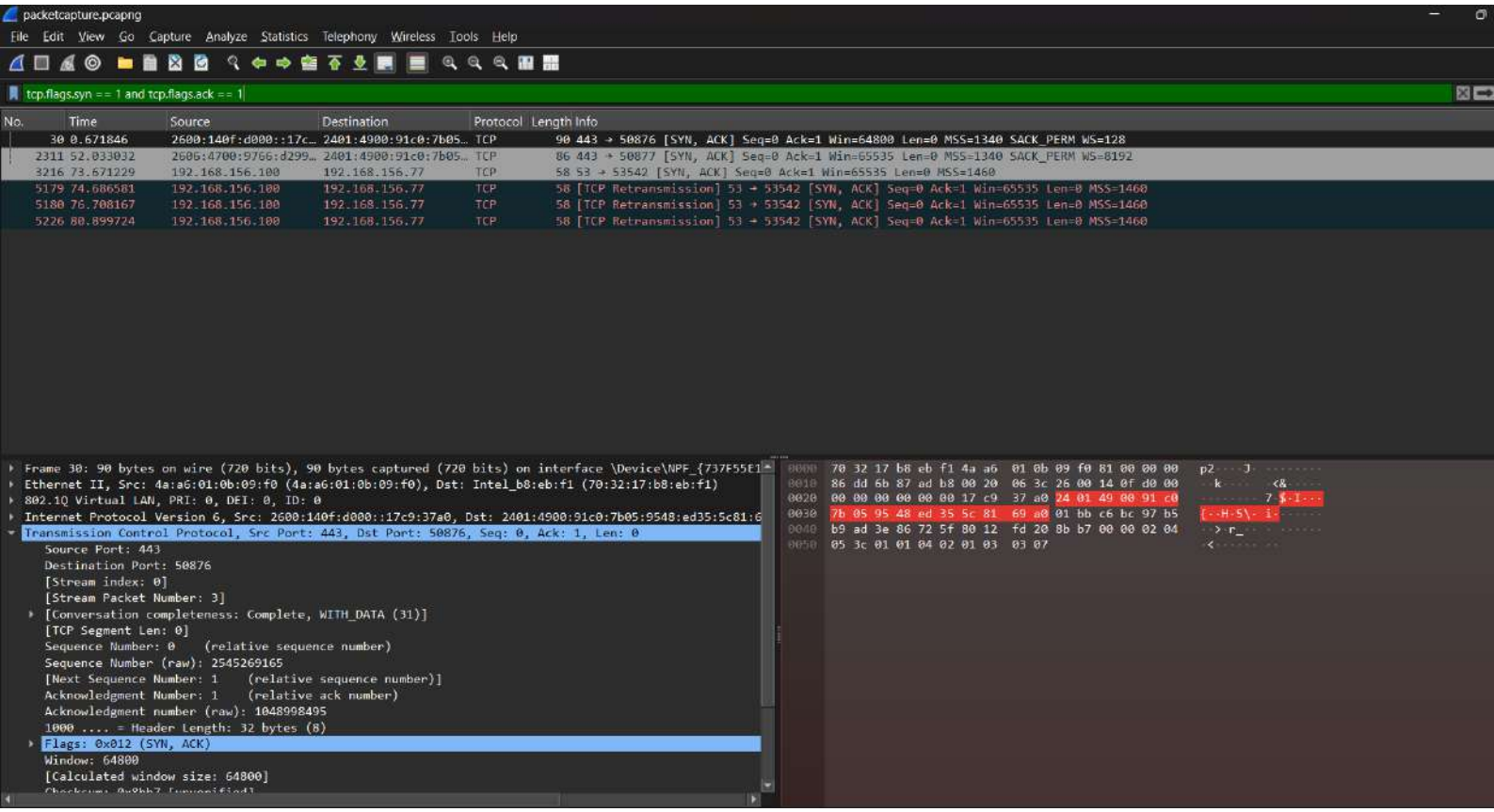
Port(s)	Protocol	Service	Details	Source
135	tcp,udp	loc-srv	Remote Procedure Call (RPC) port 135 is used in client/server applications (might be on a single machine) such as Exchange clients, the recently exploited messenger service, as well as other Windows NT/2K/XP software. If you have remote users who VPN into your network, you might need to open this port on the firewall to allow access to the Exchange server. There is a RPC (a RPC's Endpoint Mapper component) vulnerability in Windows NT where a malformed request to port 135 could cause denial of service (DoS). RPC contains a flaw that causes it to fail upon receipt of a request that contains a particular type of malformed data. To restore normal functionality victim has to reboot the system. Alternatively, you can upgrade/patch your OS (there is patch downloadable from Microsoft), or you can close port 135. Port 135 is used by Messenger Service (not MSN Messenger) and exploited in popup net send messenger spam [MSKB 330904]. To stop the popups you'd need to filter port 135 at the firewall level or stop the messenger service. The service uses all the following ports: 135/tcp, 135/udp, 137/udp 138/udp, 139/tcp, 445/tcp. MS Security Bulletin [MS03-026] outlines another critical Buffer Overrun RPC vulnerability that can be exploited via ports 135, 139, 445, 593 (or any other specifically configured RPC port). You should filter the above mentioned ports at the firewall level and not allow RPC over an unsecure network, such as the Internet. W32.Blaster.Worm [Symantec-2003-081113-0229-99] - a widely spread worm that exploits the DCOM RPC vulnerability described above (MS Security Bulletin [MS03-026]). The worm allows remote access to an infected computer via ports 4444/tcp and 69/UDP, and spreads through port 135/tcp. To avoid being infected consider closing those ports.	*SG*

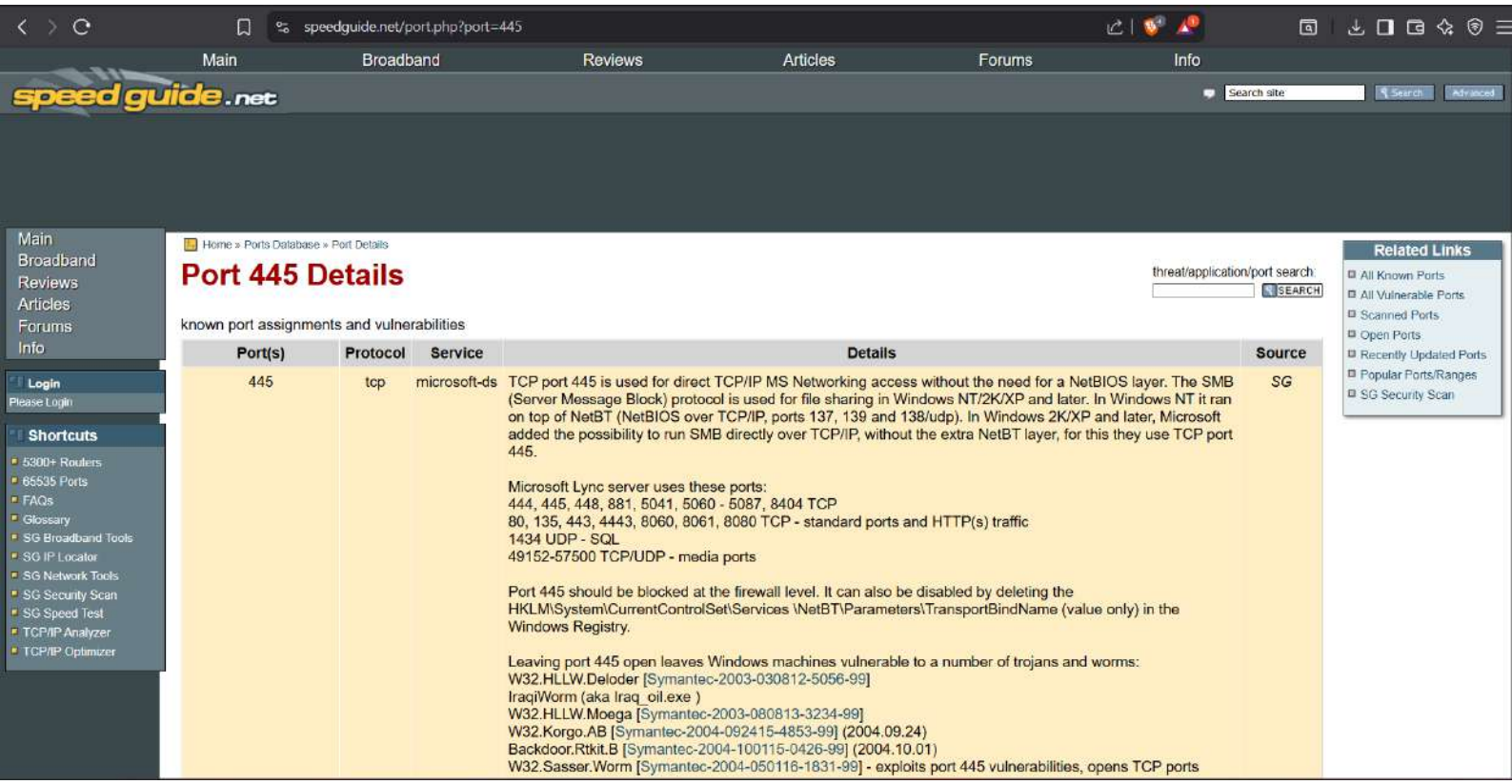
Related Links
- All Known Ports
- All Vulnerable Ports
- Scanned Ports
- Open Ports
- Recently Updated Ports
- Popular Ports/Ranges
- SG Security Scan


Apps Places
Aug 5 09:53
1% 19% 0.0 kB 0.0 kB
root@windows10: /home/mathew
command 'nama' from deb nama
command 'pamp' from deb paml
command 'nmap' from deb nmap
command 'nam' from deb nam
command 'wamp' from deb python3-autobahn
Try: apt install <deb name>
┌──(root㉿windows10)-[/home/mathew]
└─# nmap -sS 192.168.156.0/24 -oN nmapscan_result.txt
Starting Nmap 7.95 (https://nmap.org) at 2025-08-05 09:51 IST
Nmap scan report for 192.168.156.77
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.156.77 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 70:32:17:B8:EB:F1 (Intel Corporate)
Nmap scan report for 192.168.156.100
Host is up (0.0048s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 4A:A6:01:0B:09:F0 (Unknown)
Nmap scan report for 192.168.156.152
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.156.152 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Nmap done: 256 IP addresses (3 hosts up) scanned in 12.12 seconds
┌──(root㉿windows10)-[/home/mathew]
└─# cat nmapscan_result.txt
Nmap 7.95 scan initiated Tue Aug 5 09:51:34 2025 as: /usr/lib/nmap/nmap -sS -oN nmapscan_result.txt 192.168.156.0/24


Command Prompt
Windows PowerShell
PS C:\Users\hp> nmap -sS 192.168.156.0/24 -oN nmapscan_result.txt
Starting Nmap 7.97 (https://nmap.org) at 2025-08-05 10:31 +0530
Nmap scan report for 192.168.156.100
Host is up (0.0072s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 4A:A6:01:0B:09:F0 (Unknown)
Nmap scan report for 192.168.156.77
Host is up (0.00050s latency).
Not shown: 995 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
902/tcp open iss-realsecure
912/tcp open apex-mesh
Nmap done: 256 IP addresses (2 hosts up) scanned in 63.04 seconds
PS C:\Users\hp> cat nmapscan_result.txt
Nmap 7.97 scan initiated Tue Aug 5 10:31:11 2025 as: "C:\\Program Files (x86)\\Nmap\\nmap.exe" -sS -oN nmapscan_result.txt 192.168.156.0/24
Nmap scan report for 192.168.156.100
Host is up (0.0072s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 4A:A6:01:0B:09:F0 (Unknown)
Nmap scan report for 192.168.156.77
Host is up (0.00050s latency).
Not shown: 995 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
902/tcp open iss-realsecure
912/tcp open apex-mesh
Nmap done at Tue Aug 5 10:32:14 2025 -- 256 IP addresses (2 hosts up) scanned in 63.04 seconds
PS C:\Users\hp>


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1 and tcp.flags.ack == 0
No. Time Source Destination Protocol Length Info
26 0.636033 2401:4900:91c0:7b05… 2600:140f:d000::17c… TCP 86 50876 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
27 0.636041 2401:4900:91c0:7b05… 2600:140f:d000::17c… TCP 86 [TCP Retransmission] 50876 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
2269 51.975460 2401:4900:91c0:7b05… 2606:4700:9766:d299… TCP 86 50877 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
2270 51.975470 2401:4900:91c0:7b05… 2606:4700:9766:d299… TCP 86 [TCP Retransmission] 50877 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
3173 73.648028 192.168.156.77 192.168.156.100 TCP 58 53542 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3174 73.648705 192.168.156.77 192.168.156.100 TCP 58 53542 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3175 73.649141 192.168.156.77 192.168.156.100 TCP 58 53542 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3176 73.650498 192.168.156.77 192.168.156.100 TCP 58 53542 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3177 73.651040 192.168.156.77 192.168.156.100 TCP 58 53542 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3178 73.651542 192.168.156.77 192.168.156.100 TCP 58 53542 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3179 73.652101 192.168.156.77 192.168.156.100 TCP 58 53542 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3180 73.653309 192.168.156.77 192.168.156.100 TCP 58 53542 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3181 73.653860 192.168.156.77 192.168.156.100 TCP 58 53542 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3182 73.655543 192.168.156.77 192.168.156.100 TCP 58 53542 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3193 73.660168 192.168.156.77 192.168.156.100 TCP 58 53542 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3194 73.662310 192.168.156.77 192.168.156.100 TCP 58 53542 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3195 73.662797 192.168.156.77 192.168.156.100 TCP 58 53542 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3196 73.663305 192.168.156.77 192.168.156.100 TCP 58 53542 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3197 73.663839 192.168.156.77 192.168.156.100 TCP 58 53542 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3198 73.664349 192.168.156.77 192.168.156.100 TCP 58 53542 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
Frame 26: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{737F55E1-6
Ethernet II, Src: Intel_b8:eb:f1 (70:32:17:b8:eb:f1), Dst: 4a:a6:01:0b:09:f0 (4a:a6:01:0b:09:f0)
Internet Protocol Version 6, Src: 2401:4900:91c0:7b05:9548:ed35:5c81:69a0, Dst: 2600:140f:d000::17c9:37a
Transmission Control Protocol, Src Port: 50876, Dst Port: 443, Seq: 0, Len: 0
0000 4a a6 01 0b 09 f0 70 32 17 b8 eb f1 86 dd 60 0f
0010 91 a1 00 20 06 3f 24 01 49 00 91 c0 7b 05 95 48
0020 ed 35 5c 81 69 a0 26 00 14 0f d0 00 00 00 00 00
0030 00 00 17 c9 37 a0 c6 bc 01 bb 3e 86 72 5e 00 00
0040 00 00 80 02 ff ff 1c 07 00 00 02 04 05 a0 01 03
0050 03 08 01 01 04 02
wireshark_Wi-FiTXD8A3.pcapng
Packets: 5284 · Displayed: 1004 (19.0%) · Dropped: 0 (0.0%)
Profile: Default
1 cm of rain
Sunday
Search
ENG
IN
10:44
05-08-2025


packetcapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1 and tcp.flags.ack == 1
No. Time Source Destination Protocol Length Info
30 0.671846 2600:140f:d000::17c… 2401:4900:91c0:7b05… TCP 90 443 → 50876 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1340 SACK_PERM WS=128
2311 52.033032 2606:4700:9766:d299… 2401:4900:91c0:7b05… TCP 86 443 → 50877 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1340 SACK_PERM WS=8192
3216 73.671229 192.168.156.100 192.168.156.77 TCP 58 53 → 53542 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
5179 74.686581 192.168.156.100 192.168.156.77 TCP 58 [TCP Retransmission] 53 → 53542 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
5180 76.708167 192.168.156.100 192.168.156.77 TCP 58 [TCP Retransmission] 53 → 53542 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
5226 80.899724 192.168.156.100 192.168.156.77 TCP 58 [TCP Retransmission] 53 → 53542 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
Frame 30: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{737F55E1
Ethernet II, Src: 4a:a6:01:0b:09:f0 (4a:a6:01:0b:09:f0), Dst: Intel_b8:eb:f1 (70:32:17:b8:eb:f1)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 0
Internet Protocol Version 6, Src: 2600:140f:d000::17c9:37a0, Dst: 2401:4900:91c0:7b05:9548:ed35:5c81:6
Transmission Control Protocol, Src Port: 443, Dst Port: 50876, Seq: 0, Ack: 1, Len: 0
Source Port: 443
Destination Port: 50876
[Stream index: 0]
[Stream Packet Number: 3]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2545269165
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1048998495
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
Window: 64800
[Calculated window size: 64800]
0000 70 32 17 b8 eb f1 4a a6 01 0b 09 f0 81 00 00 00
0010 86 dd 6b b7 ad b8 00 20 06 3c 26 00 14 0f d0 00
0020 00 00 00 00 00 00 17 c9 37 a0 24 01 49 00 91 c0
0030 7b 05 95 48 ed 35 5c 81 69 a0 01 bb c6 bc 97 b5
0040 b9 ad 3e 86 72 5f 80 12 fd 20 8b b7 00 00 02 04
0050 05 3c 01 01 04 02 01 03 03 07


speedguide.net/port.php?port=445
Main
Broadband
Reviews
Articles
Forums
Info
speedguide.net
Search site
Search
Advanced
Main
Broadband
Reviews
Articles
Forums
Info
Login
Please Login
Shortcuts
5300+ Routers
65535 Ports
FAQs
Glossary
SG Broadband Tools
SG IP Locator
SG Network Tools
SG Security Scan
SG Speed Test
TCP/IP Analyzer
TCP/IP Optimizer
Home » Ports Database » Port Details
Port 445 Details
threat/application/port search:
SEARCH
known port assignments and vulnerabilities
Port(s) | Protocol | Service | Details | Source
445 | tcp | microsoft-ds | TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer. The SMB (Server Message Block) protocol is used for file sharing in Windows NT/2K/XP and later. In Windows NT it ran on top of NetBT (NetBIOS over TCP/IP, ports 137, 139 and 138/udp). In Windows 2K/XP and later, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra NetBT layer, for this they use TCP port 445.
Microsoft Lync server uses these ports:
444, 445, 448, 881, 5041, 5060 - 5087, 8404 TCP
80, 135, 443, 4443, 8060, 8061, 8080 TCP - standard ports and HTTP(s) traffic
1434 UDP - SQL
49152-57500 TCP/UDP - media ports
Port 445 should be blocked at the firewall level. It can also be disabled by deleting the HKLM\System\CurrentControlSet\Services \NetBT\Parameters\TransportBindName (value only) in the Windows Registry.
Leaving port 445 open leaves Windows machines vulnerable to a number of trojans and worms:
W32.HLLW.Deloder [Symantec-2003-030812-5056-99]
IraqiWorm (aka Iraq_oil.exe)
W32.HLLW.Moega [Symantec-2003-080813-3234-99]
W32.Korgo.AB [Symantec-2004-092415-4853-99] (2004.09.24)
Backdoor.Rtkit.B [Symantec-2004-100115-0426-99] (2004.10.01)
W32.Sasser.Worm [Symantec-2004-050116-1831-99] - exploits port 445 vulnerabilities, opens TCP ports | SG
Related Links
All Known Ports
All Vulnerable Ports
Scanned Ports
Open Ports
Recently Updated Ports
Popular Ports/Ranges
SG Security Scan