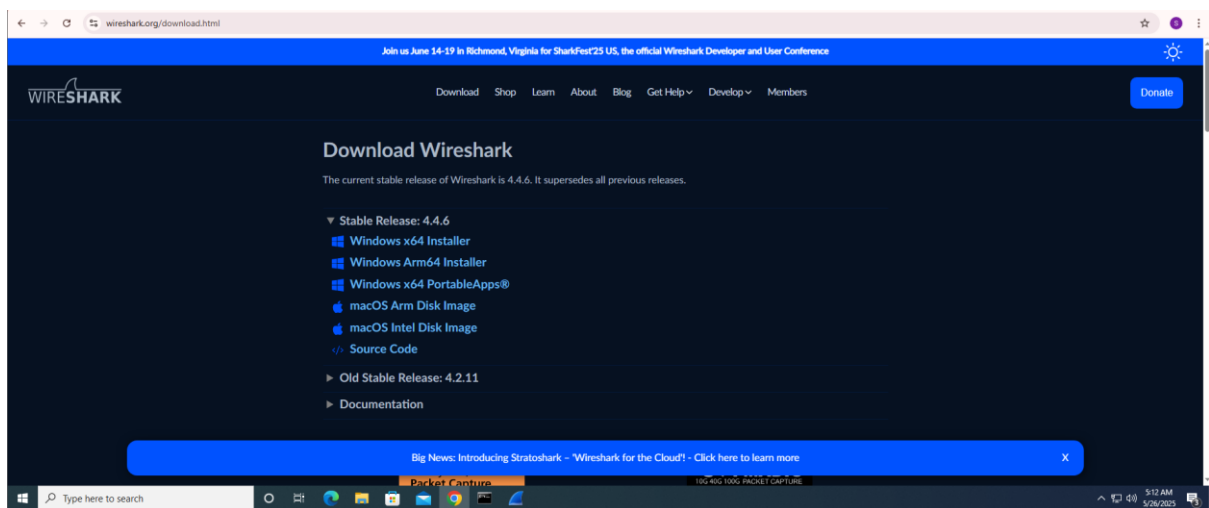


Downloading Nmap scan



Downloading wireshark

Different commands on cmd for ip configuration and nmap scan working

```
Command Prompt
C:\Users\UserCSEC202>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::7868:af1c:b62f:67bd%13
    IPv4 Address. . . . . : 192.168.91.144
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.91.2

C:\Users\UserCSEC202>nmap -sS 192.168.1.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-05-26 02:14 -0400
^C
C:\Users\UserCSEC202>nmapo -sS 192.168.91.0/24
'nmapo' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\UserCSEC202>nmap -sS 192.168.91.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-05-26 02:14 -0400
Nmap scan report for 192.168.91.1
Host is up (0.0037s latency).
Not shown: 993 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   filtered apex-mesh
3306/tcp  open  mysql
5357/tcp  open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.91.2
Host is up (0.0010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F0:FB:92 (VMware)

Nmap scan report for 192.168.91.254
Host is up (0.0024s latency).
All 1000 scanned ports on 192.168.91.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F8:17:86 (VMware)

Nmap scan report for 192.168.91.144
Host is up (0.00042s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
```

```
Select Command Prompt
53/tcp open  domain
MAC Address: 00:50:56:F0:FB:92 (VMware)

Nmap scan report for 192.168.91.254
Host is up (0.0024s latency).
All 1000 scanned ports on 192.168.91.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F8:17:86 (VMware)

Nmap scan report for 192.168.91.144
Host is up (0.00042s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap done: 256 IP addresses (4 hosts up) scanned in 60.66 seconds

C:\Users\UserCSEC202>nmap -sS 192.168.1.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-05-26 02:16 -0400
^C
C:\Users\UserCSEC202>nmap -sS 192.168.91.0/24 -oN scan_results.txt
Starting Nmap 7.97 ( https://nmap.org ) at 2025-05-26 02:28 -0400
Nmap scan report for 192.168.91.1
Host is up (0.0024s latency).
Not shown: 993 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
3306/tcp   open  mysql
5357/tcp   open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.91.254
Host is up (0.0037s latency).
All 1000 scanned ports on 192.168.91.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F8:17:86 (VMware)

Nmap scan report for 192.168.91.144
Host is up (0.00s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap done: 256 IP addresses (3 hosts up) scanned in 57.95 seconds
```

```

C:\Users\UserCSEC202>nmap -sS 192.168.91.0/24 -oX scan_results.xml
Starting Nmap 7.97 ( https://nmap.org ) at 2025-05-26 02:30 -0400
Nmap scan report for 192.168.91.1
Host is up (0.0022s latency).
Not shown: 993 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-realsure
912/tcp    open  apex-mesh
3306/tcp   open  mysql
5357/tcp   open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)

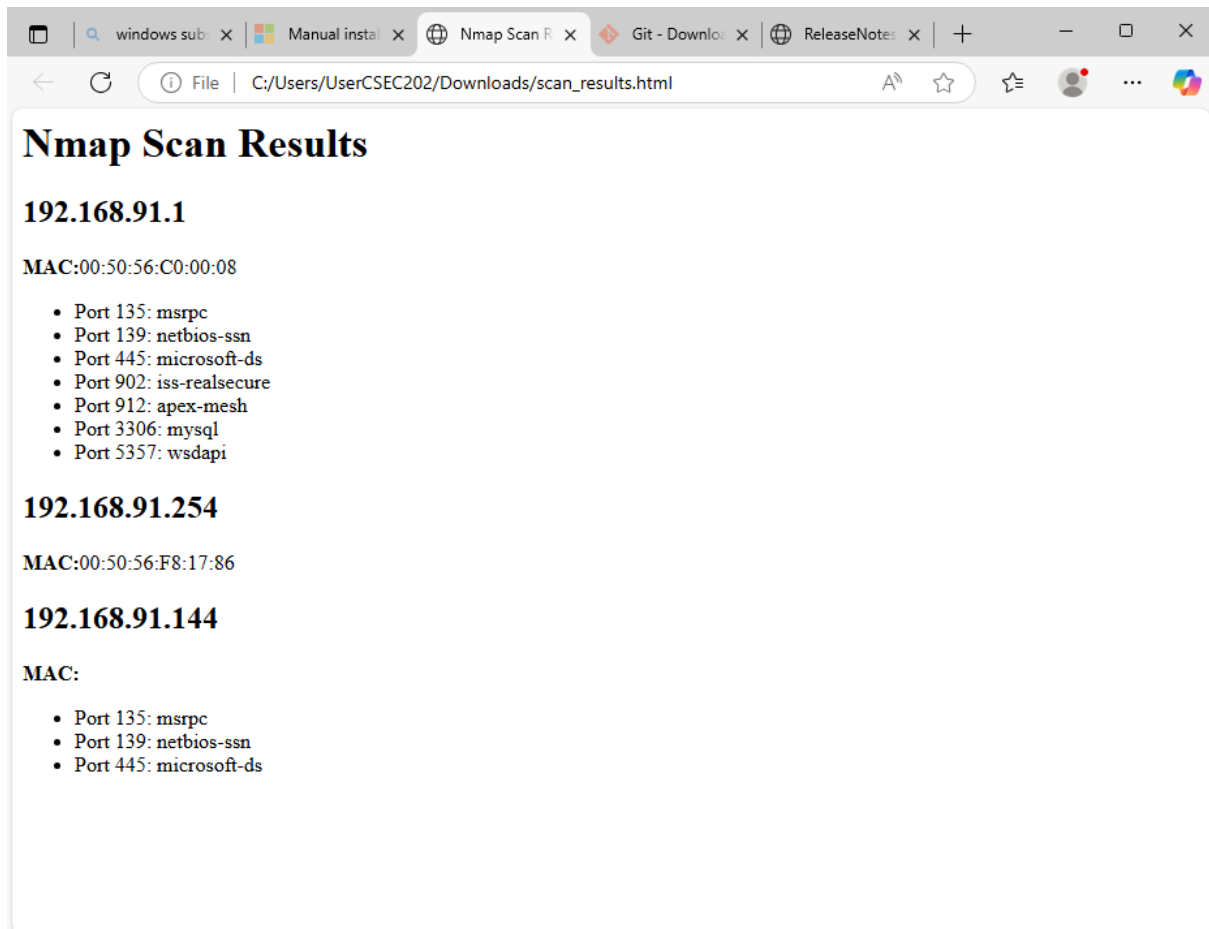
Nmap scan report for 192.168.91.254
Host is up (0.0038s latency).
All 1000 scanned ports on 192.168.91.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F8:17:86 (VMware)

Nmap scan report for 192.168.91.144
Host is up (0.00070s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap done: 256 IP addresses (3 hosts up) scanned in 60.42 seconds

```

Nmap scan results opened in web browser



The screenshot shows a web browser window with the following tabs: "windows sub...", "Manual instal...", "Nmap Scan R...", "Git - Downlo...", and "ReleaseNotes...". The address bar shows the file path "C:/Users/UserCSEC202/Downloads/scan_results.html".

Nmap Scan Results

192.168.91.1

MAC:00:50:56:C0:00:08

- Port 135: msrpc
- Port 139: netbios-ssn
- Port 445: microsoft-ds
- Port 902: iss-realsure
- Port 912: apex-mesh
- Port 3306: mysql
- Port 5357: wsdapi

192.168.91.254

MAC:00:50:56:F8:17:86

192.168.91.144

MAC:

- Port 135: msrpc
- Port 139: netbios-ssn
- Port 445: microsoft-ds

*Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1 && tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
336	32.565757	192.168.70.196	192.168.91.1	TCP	58	39054 → 443 [SYN] Seq
337	32.566374	192.168.70.196	192.168.91.2	TCP	58	39054 → 443 [SYN] Seq
338	32.566540	192.168.70.196	192.168.91.3	TCP	58	39054 → 443 [SYN] Seq
339	32.576318	192.168.70.196	192.168.91.6	TCP	58	39054 → 443 [SYN] Seq
340	33.576914	192.168.70.196	192.168.91.1	TCP	58	39056 → 443 [SYN] Seq
341	33.577966	192.168.70.196	192.168.91.2	TCP	58	39056 → 443 [SYN] Seq
342	33.578555	192.168.70.196	192.168.91.3	TCP	58	39056 → 443 [SYN] Seq
349	33.592184	192.168.70.196	192.168.91.6	TCP	58	39056 → 443 [SYN] Seq
355	34.595210	192.168.70.196	192.168.91.13	TCP	58	39054 → 443 [SYN] Seq
356	34.595604	192.168.70.196	192.168.91.14	TCP	58	39054 → 443 [SYN] Seq
357	34.595867	192.168.70.196	192.168.91.15	TCP	58	39054 → 443 [SYN] Seq

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0)

Total Length: 44

Identification: 0xd53d (54589)

> 000. = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 50

Protocol: TCP (6)

Header Checksum: 0x9078 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.70.196

Destination Address: 192.168.91.1

0000 8c c5 e1 17 da 6d 00 0c 29 48 c5 80 08 00 45

0010 00 2c d5 3d 00 00 32 06 90 78 c0 a8 46 c4 c0

0020 5b 01 98 8e 01 bb 68 b3 09 4d 00 00 00 00 60

0030 04 00 64 c6 00 00 02 04 05 b4

Destination Address (ip.dst), 4 bytes

Packets: 2216 · Displayed: 509 (23.0%) · Dropped: 0 (0.0%) | 2 new notifications

Wireshark results