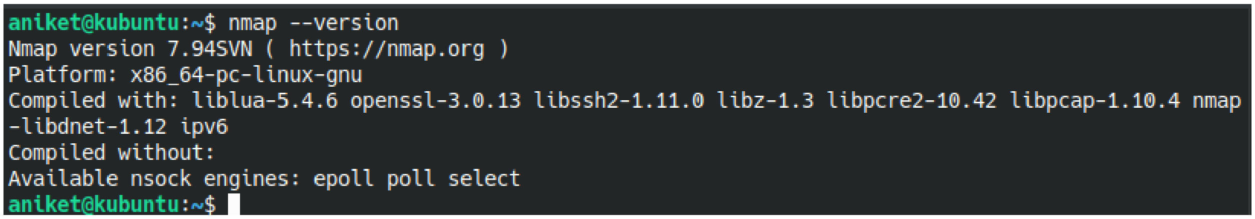
ELEVATE LABS - CYBER SECURITY INTERNSHIP

TASK 1: Scan Your Local Network for Open Ports

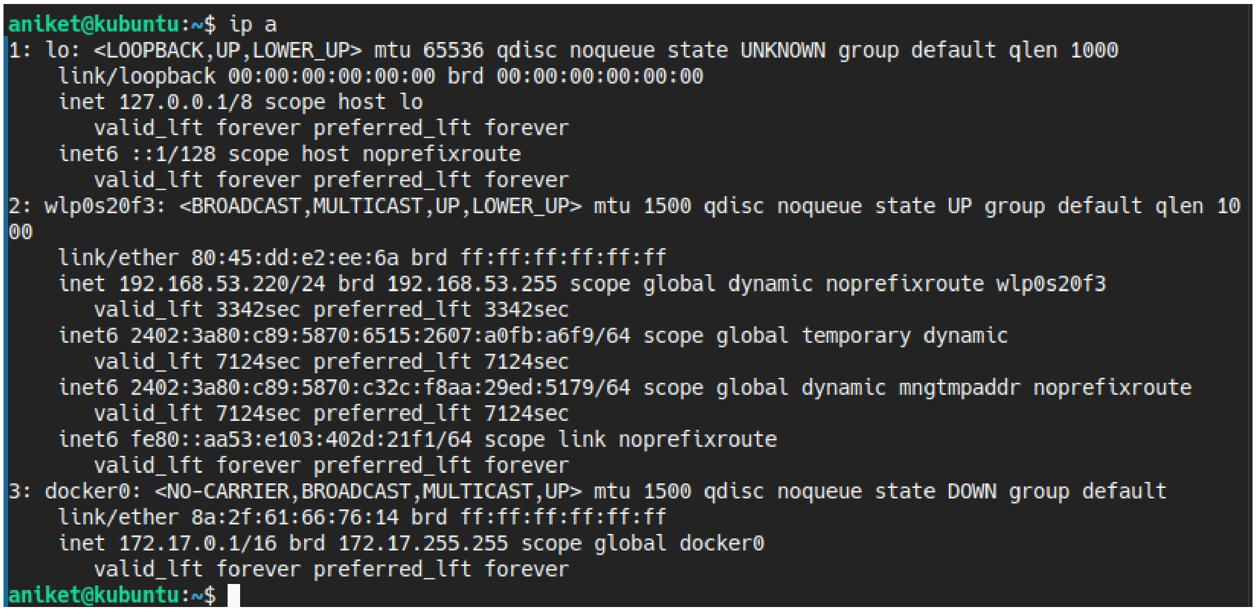
- **Objective:** Learn to discover open ports on devices in your local network to understand network exposure.
- **Tools:** Nmap (free), Wireshark (optional)

Step 1: Install nmap (nmap is installed)



```
aniket@kubuntu:~$ nmap --version
Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.0.13 libssh2-1.11.0 libz-1.3 libpcre2-10.42 libpcap-1.10.4 nmap
-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
aniket@kubuntu:~$ 
```

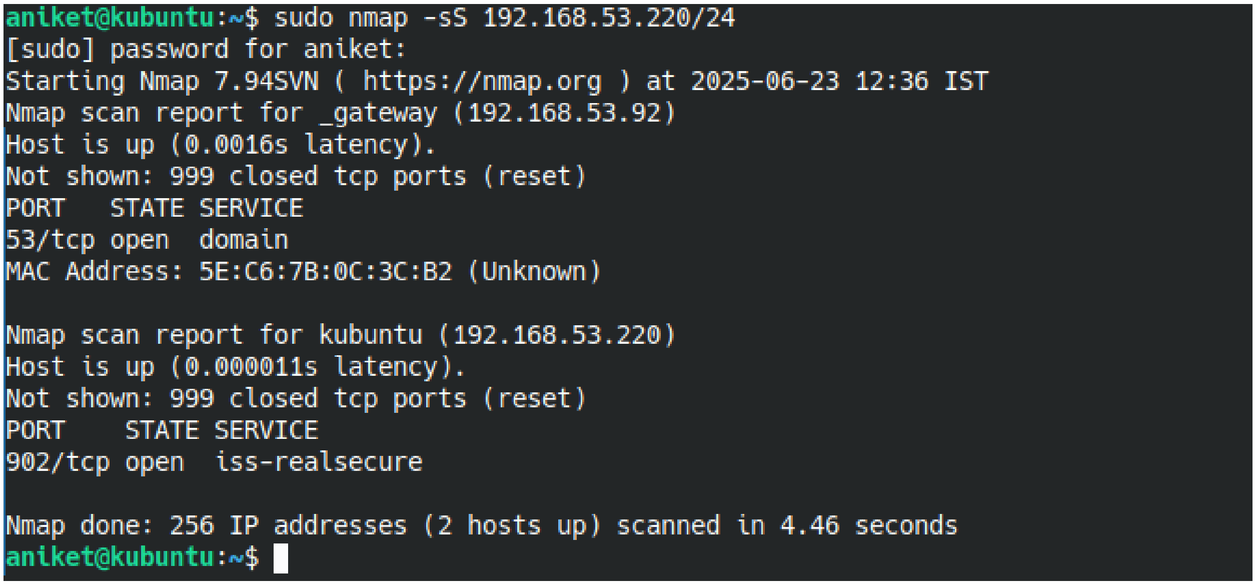
Step 2: Local IP address



```
aniket@kubuntu:~$ 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: wlp0s20f3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 10
00
    link/ether 80:45:dd:e2:ee:6a brd ff:ff:ff:ff:ff:ff
    inet 192.168.53.220/24 brd 192.168.53.255 scope global dynamic noprefixroute wlp0s20f3
       valid_lft 3342sec preferred_lft 3342sec
    inet6 2402:3a80:c89:5870:6515:2607:a0fb:a6f9/64 scope global temporary dynamic
       valid_lft 7124sec preferred_lft 7124sec
    inet6 2402:3a80:c89:5870:c32c:f8aa:29ed:5179/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 7124sec preferred_lft 7124sec
    inet6 fe80::aa53:e103:402d:21f1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 8a:2f:61:66:76:14 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
aniket@kubuntu:~$ 
```

IP address = *192.168.53.220*

Step 3: Run: nmap -sS 192.168.53.220/24 to perform TCP SYN scan.



```
aniket@kubuntu:~$ sudo nmap -sS 192.168.53.220/24
[sudo] password for aniket:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 12:36 IST
Nmap scan report for _gateway (192.168.53.92)
Host is up (0.0016s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 5E:C6:7B:0C:3C:B2 (Unknown)

Nmap scan report for kubuntu (192.168.53.220)
Host is up (0.000011s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
902/tcp open  iss-realsecure

Nmap done: 256 IP addresses (2 hosts up) scanned in 4.46 seconds
aniket@kubuntu:~$ 
```

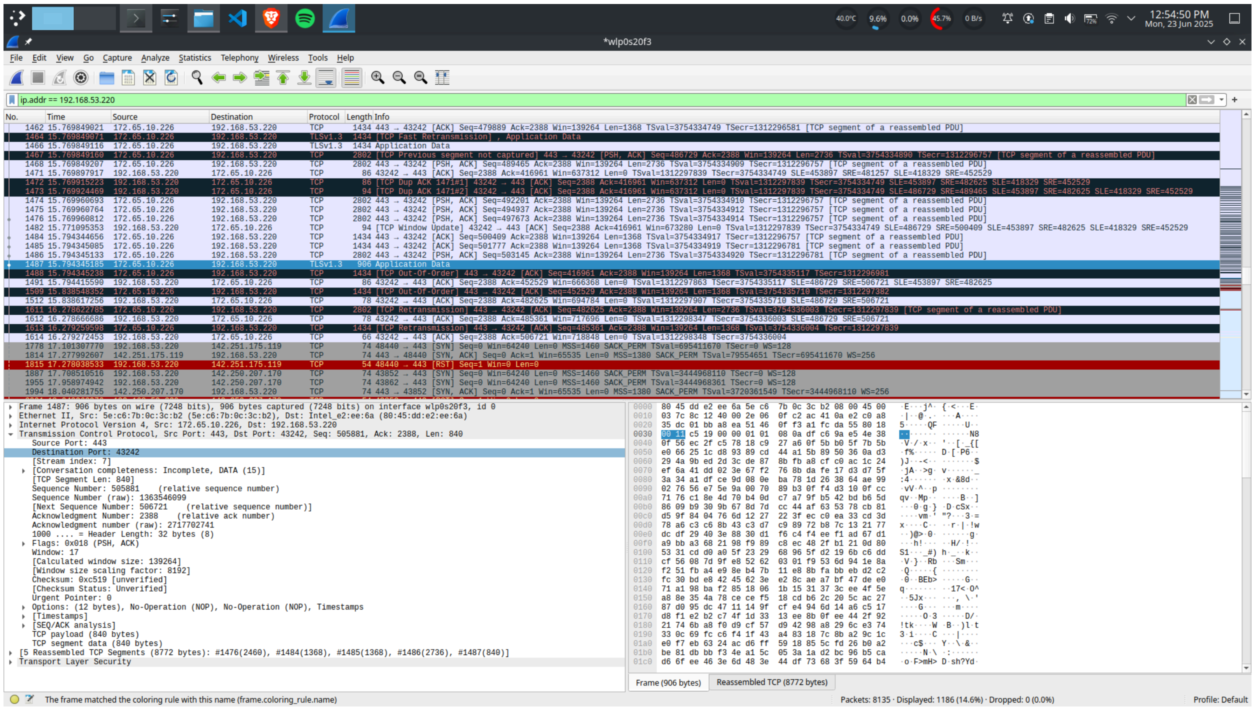
Open ports:

Port: *902/tcp*

State: *open*

Service: *iss-realsecure*

Step 4: Analyze using Wireshark



ip.addr == 192.168.53.220

```
No.   Time          Source          Destination     Protocol Length Info
 1462 15.769849021  172.65.10.226   192.168.53.220  TCP      1434 443 → 43242 [ACK] Seq=479889 Ack=2388 Win=139264 Len=1368 TSval=3754334749 TSecr=1312296581 [TCP segment of a reassembled PDU]
 1464 15.769849071  172.65.10.226   192.168.53.220  TLSv1.3  1434 [TCP Fast Retransmission] , Application Data
 1466 15.769849116  172.65.10.226   192.168.53.220  TLSv1.3  1434 Application Data
 1467 15.769849160  172.65.10.226   192.168.53.220  TCP      2802 [TCP Previous segment not captured] 443 → 43242 [PSH, ACK] Seq=486729 Ack=2388 Win=139264 Len=2736 TSval=3754334890 TSecr=1312296757 [TCP segment of a reassembled PDU]
 1468 15.769849207  172.65.10.226   192.168.53.220  TCP      2802 443 → 43242 [PSH, ACK] Seq=489465 Ack=2388 Win=139264 Len=2736 TSval=3754334909 TSecr=1312296757 [TCP segment of a reassembled PDU]
 1471 15.769897917  192.168.53.220  172.65.10.226   TCP        86 43242 → 443 [ACK] Seq=2388 Ack=416961 Win=637312 Len=0 TSval=1312297839 TSecr=3754334749 SLE=453897 SRE=481257 SLE=418329 SRE=452529
 1472 15.769915223  192.168.53.220  172.65.10.226   TCP        86 [TCP Dup ACK 1471#1] 43242 → 443 [ACK] Seq=2388 Ack=416961 Win=637312 Len=0 TSval=1312297839 TSecr=3754334749 SLE=453897 SRE=482625 SLE=418329 SRE=452529
 1473 15.769924469  192.168.53.220  172.65.10.226   TCP        94 [TCP Dup ACK 1471#2] 43242 → 443 [ACK] Seq=2388 Ack=416961 Win=637312 Len=0 TSval=1312297839 TSecr=3754334749 SLE=486729 SRE=489465 SLE=453897 SRE=482625 SLE=418329 SRE=452529
 1474 15.769960693  172.65.10.226   192.168.53.220  TCP      2802 443 → 43242 [PSH, ACK] Seq=492201 Ack=2388 Win=139264 Len=2736 TSval=3754334910 TSecr=1312296757 [TCP segment of a reassembled PDU]
 1475 15.769960764  172.65.10.226   192.168.53.220  TCP      2802 443 → 43242 [PSH, ACK] Seq=494937 Ack=2388 Win=139264 Len=2736 TSval=3754334912 TSecr=1312296757 [TCP segment of a reassembled PDU]
 1476 15.769960812  172.65.10.226   192.168.53.220  TCP      2802 443 → 43242 [PSH, ACK] Seq=497673 Ack=2388 Win=139264 Len=2736 TSval=3754334914 TSecr=1312296757 [TCP segment of a reassembled PDU]
 1482 15.771095353  192.168.53.220  172.65.10.226   TCP        94 [TCP Window Update] 43242 → 443 [ACK] Seq=2388 Ack=416961 Win=673280 Len=0 TSval=1312297839 TSecr=3754334749 SLE=486729 SRE=500409 SLE=453897 SRE=482625 SLE=418329 SRE=452529
 1484 15.794344656  172.65.10.226   192.168.53.220  TCP      1434 443 → 43242 [ACK] Seq=500409 Ack=2388 Win=139264 Len=1368 TSval=3754334917 TSecr=1312296757 [TCP segment of a reassembled PDU]
 1485 15.794345085  172.65.10.226   192.168.53.220  TCP      1434 443 → 43242 [ACK] Seq=501777 Ack=2388 Win=139264 Len=1368 TSval=3754334919 TSecr=1312296781 [TCP segment of a reassembled PDU]
 1486 15.794345133  172.65.10.226   192.168.53.220  TCP      2802 443 → 43242 [PSH, ACK] Seq=503145 Ack=2388 Win=139264 Len=2736 TSval=3754334920 TSecr=1312296781 [TCP segment of a reassembled PDU]
 1487 15.794345185  172.65.10.226   192.168.53.220  TLSv1.3   906 Application Data
 1488 15.794345238  172.65.10.226   192.168.53.220  TCP      1434 [TCP Out-Of-Order] 443 → 43242 [ACK] Seq=416961 Ack=2388 Win=139264 Len=1368 TSval=3754335117 TSecr=1312296981
 1491 15.794415590  192.168.53.220  172.65.10.226   TCP        86 43242 → 443 [ACK] Seq=2388 Ack=452529 Win=666368 Len=0 TSval=1312297863 TSecr=3754335117 SLE=486729 SRE=506721 SLE=453897 SRE=482625
 1509 15.838548352  172.65.10.226   192.168.53.220  TCP      1434 [TCP Out-Of-Order] 443 → 43242 [ACK] Seq=452529 Ack=2388 Win=139264 Len=1368 TSval=3754335710 TSecr=1312297382
 1512 15.838617256  192.168.53.220  172.65.10.226   TCP        78 43242 → 443 [ACK] Seq=2388 Ack=482625 Win=694784 Len=0 TSval=1312297907 TSecr=3754335710 SLE=486729 SRE=506721
 1611 16.278622785  172.65.10.226   192.168.53.220  TCP      2802 [TCP Retransmission] 443 → 43242 [ACK] Seq=482625 Ack=2388 Win=139264 Len=2736 TSval=3754336003 TSecr=1312297839 [TCP segment of a reassembled PDU]
 1612 16.278666686  192.168.53.220  172.65.10.226   TCP        78 43242 → 443 [ACK] Seq=2388 Ack=485361 Win=717696 Len=0 TSval=1312298347 TSecr=3754336003 SLE=486729 SRE=506721
 1613 16.279259598  172.65.10.226   192.168.53.220  TCP      1434 [TCP Retransmission] 443 → 43242 [ACK] Seq=485361 Ack=2388 Win=139264 Len=1368 TSval=3754336004 TSecr=1312297839
 1614 16.279272453  192.168.53.220  172.65.10.226   TCP        66 43242 → 443 [ACK] Seq=2388 Ack=506721 Win=718848 Len=0 TSval=1312298348 TSecr=3754336004
 1778 17.101307770  192.168.53.220  142.251.175.119 TCP        74 48440 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=695411670 TSecr=0 WS=128
 1814 17.277992607  142.251.175.119 192.168.53.220  TCP        74 443 → 48440 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=79554651 TSecr=695411670 WS=256
 1815 17.278038533  192.168.53.220  142.251.175.119 TCP        54 48440 → 443 [RST] Seq=1 Win=0 Len=0
 1887 17.708510516  192.168.53.220  142.250.207.170 TCP        74 43852 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3444968110 TSecr=0 WS=128
 1955 17.958974942  192.168.53.220  142.250.207.170 TCP        74 43862 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3444968361 TSecr=0 WS=128
 1994 18.040281755  142.250.207.170 192.168.53.220  TCP        74 443 → 43852 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM TSval=3720361549 TSecr=3444968110 WS=256
```

```
▸ Frame 1487: 906 bytes on wire (7248 bits), 906 bytes captured (7248 bits) on interface wlp0s20f3, id 0
▸ Ethernet II, Src: 5e:c6:7b:0c:3c:b2 (5e:c6:7b:0c:3c:b2), Dst: Intel_e2:ee:6a (80:45:dd:e2:ee:6a)
▸ Internet Protocol Version 4, Src: 172.65.10.226, Dst: 192.168.53.220
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 43242, Seq: 505881, Ack: 2388, Len: 840
    Source Port: 443
    Destination Port: 43242
    [Stream index: 7]
  ▸ [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 840]
    Sequence Number: 505881    (relative sequence number)
    Sequence Number (raw): 1363546099
    [Next Sequence Number: 506721    (relative sequence number)]
    Acknowledgment Number: 2388    (relative ack number)
    Acknowledgment number (raw): 2717702741
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 17
    [Calculated window size: 139264]
    [Window size scaling factor: 8192]
    Checksum: 0xc519 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (840 bytes)
    TCP segment data (840 bytes)
▸ [5 Reassembled TCP Segments (8772 bytes): #1476(2460), #1484(1368), #1485(1368), #1486(2736), #1487(840)]
▸ Transport Layer Security
```

```
0000  80 45 dd e2 ee 6a 5e c6  7b 0c 3c b2 08 00 45 00
0010  03 7c 8c 12 40 00 2e 06  0f c2 ac 41 0a e2 c0 a8
0020  35 dc 01 bb a8 ea 51 46  0f f3 a1 fc da 55 80 18
0030  00 11 c5 19 00 00 01 01  08 0a df c6 9a e5 4e 38
0040  0f 56 ec 2f c5 78 18 c9  27 a6 0f 5b b0 5f 7b 5b
0050  e0 66 25 1c d8 93 89 cd  44 a1 5b 89 50 36 0a d3
0060  29 4a 9b ed 2d 3c de 87  8b fb a8 cf c0 ac 1c 24
0070  ef 6a 41 dd 02 3e 67 f2  76 8b da fe 17 d3 d7 5f
0080  3a 34 a1 df ce 9d 08 0e  ba 78 1d 26 38 64 ae 99
0090  02 76 56 e7 5e 9a 00 70  89 b3 0f f4 d3 10 0f cc
00a0  71 76 c1 8e 4d 70 b4 0d  c7 a7 9f b5 42 bd b6 5d
00b0  86 09 b9 30 9b 67 8d 7d  cc 44 af 63 53 78 cb 81
00c0  d5 9f 84 04 76 6d 12 27  22 3f ec c0 ea 33 cd 3d
00d0  78 a6 c3 c6 8b 43 c3 d7  c9 89 72 b8 7c 13 21 77
00e0  dc df 29 40 3e 88 30 d1  f6 c4 f4 ee f1 ad 67 d1
00f0  a9 bb a3 68 21 98 f9 89  c8 ec 48 2f b1 21 0d 80
0100  53 31 cd d0 a0 5f 23 29  68 96 5f d2 19 6b c6 dd
0110  cf 56 08 7d 9f e8 52 62  03 01 f9 53 6d 94 1e 8a
0120  f2 51 fb a4 e9 8e b4 7b  11 e8 8b fa bb eb d2 c2
0130  fc 30 bd e8 42 45 62 3e  e2 8c ae a7 bf 47 de e0
0140  71 a1 98 ba f2 85 18 06  1b 15 31 37 3c ee 4f 5e
0150  a8 8e 35 4a 78 ce ce f5  18 cd b6 2c 20 5c ac 27
0160  87 d0 95 dc 47 11 14 9f  cf e4 94 6d 14 a6 c5 17
0170  d8 f1 e2 b2 c7 4f 1d 33  13 ee 8b 0f ee 44 2f 92
0180  21 74 6b a8 f0 d9 cf 57  d9 42 98 a8 29 6c e3 74
0190  33 0c 69 fc c6 f4 1f 43  a4 83 18 7c 8b a2 9c 1c
01a0  e0 f7 eb 63 24 ac d6 ff  59 18 85 5c fd 26 b0 a2
01b0  be 81 db bb f3 4e a1 5c  05 3a 1a d2 bc 96 b5 ca
01c0  d6 6f ee 46 3e 6d 48 3e  44 df 73 68 3f 59 64 b4
```

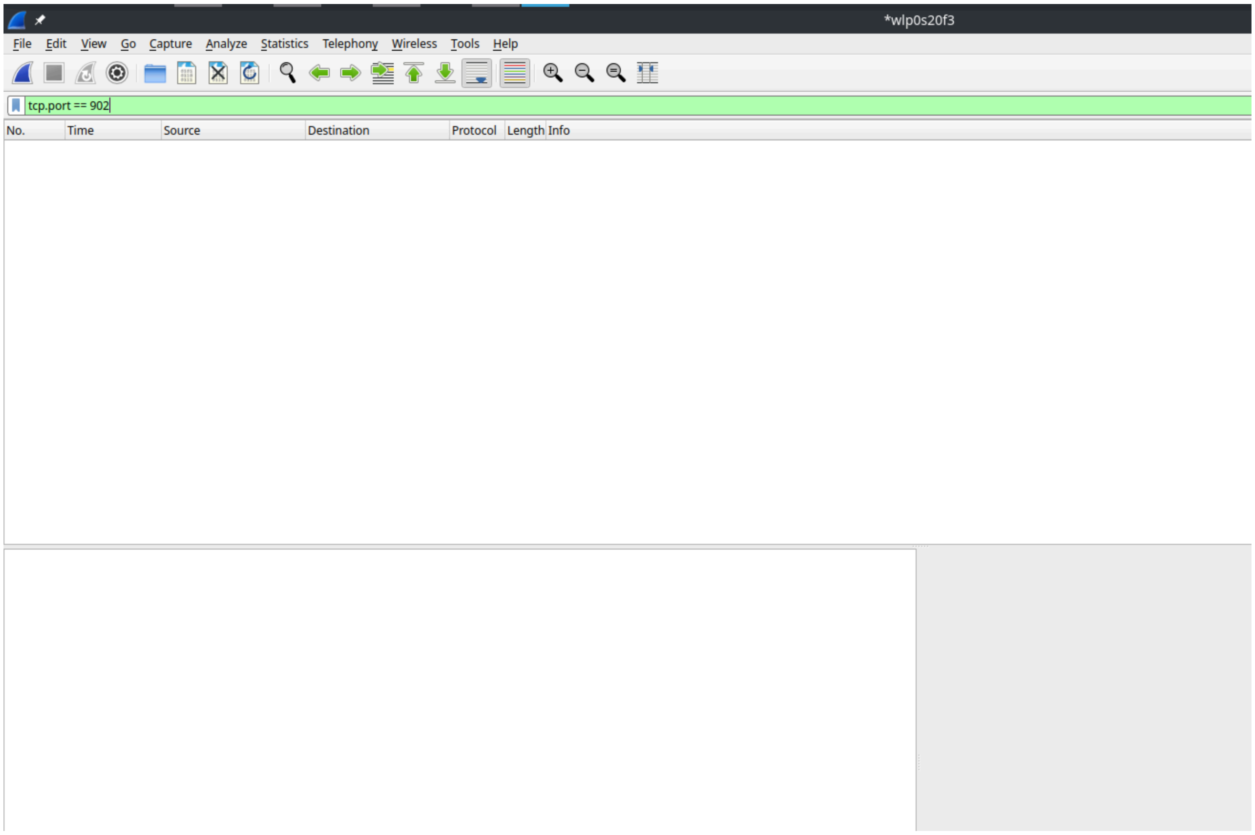
The frame matched the coloring rule with this name (frame.coloring_rule.name)

Packets: 8135 · Displayed: 1186 (14.6%) · Dropped: 0 (0.0%)

Profile: Default

Used filters like *tcp.port == 80*, *tcp.port == 443*, *ip.addr == 192.168.53.220*

Step 5: Identify security risks:



*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port == 902
```

No. Time Source Destination Protocol Length Info

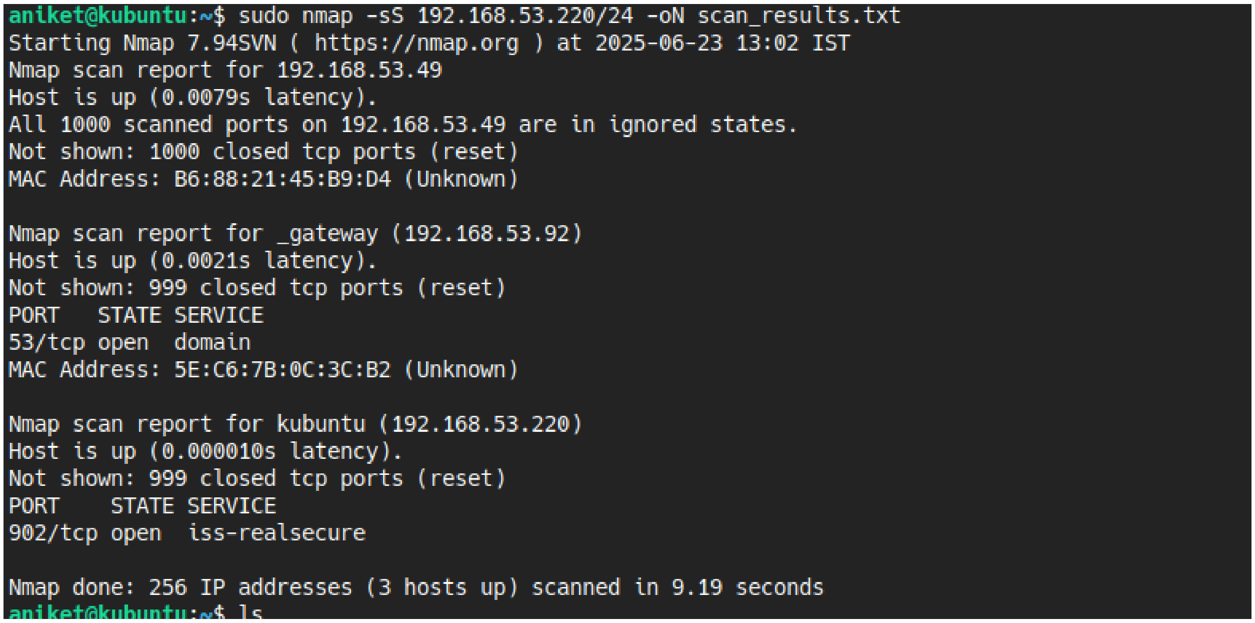
The port - 902 which is open in NMAP scan is not being used as per the Wireshark network scan.

Port 902 lets you manage a VMware virtualized environment.

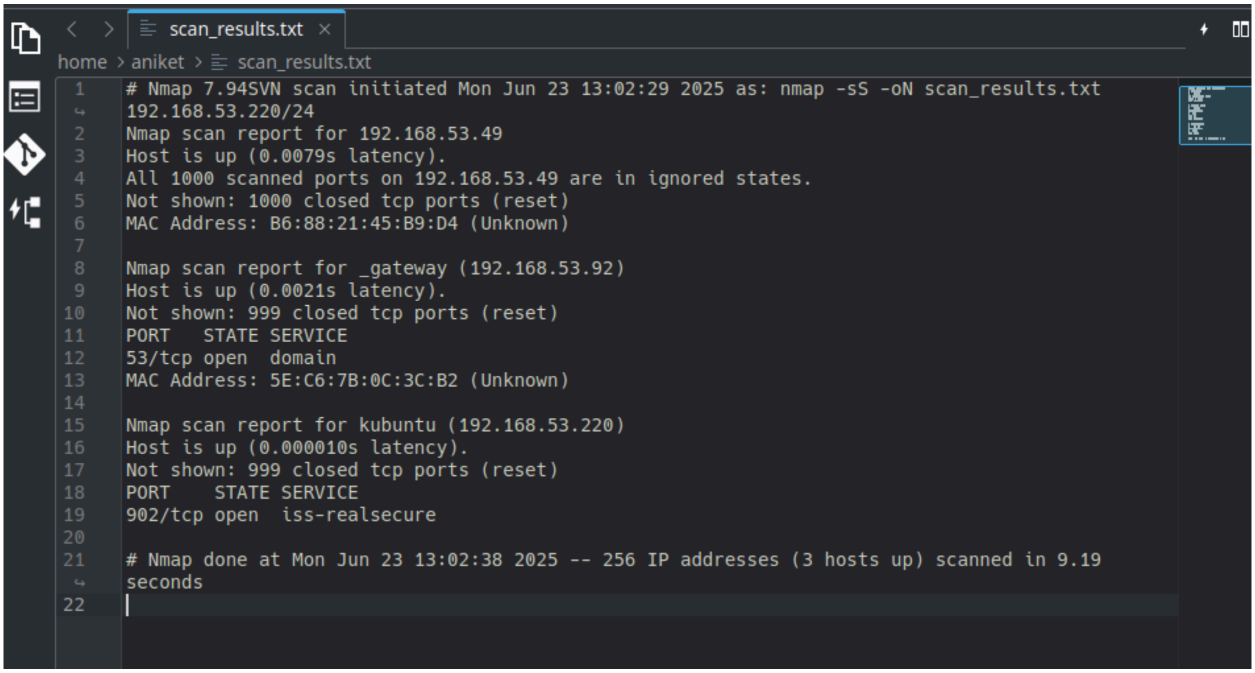
Step 6: Save scan results

For text:

```
sudo nmap -sS 192.168.53.220/24 -oN scan_results.txt
```



```
aniket@kubuntu:~$ sudo nmap -sS 192.168.53.220/24 -oN scan_results.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 13:02 IST
Nmap scan report for 192.168.53.49
Host is up (0.0079s latency).
All 1000 scanned ports on 192.168.53.49 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: B6:88:21:45:B9:D4 (Unknown)

Nmap scan report for _gateway (192.168.53.92)
Host is up (0.0021s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 5E:C6:7B:0C:3C:B2 (Unknown)

Nmap scan report for kubuntu (192.168.53.220)
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
902/tcp open  iss-realsecure

Nmap done: 256 IP addresses (3 hosts up) scanned in 9.19 seconds
aniket@kubuntu:~$ ls
```

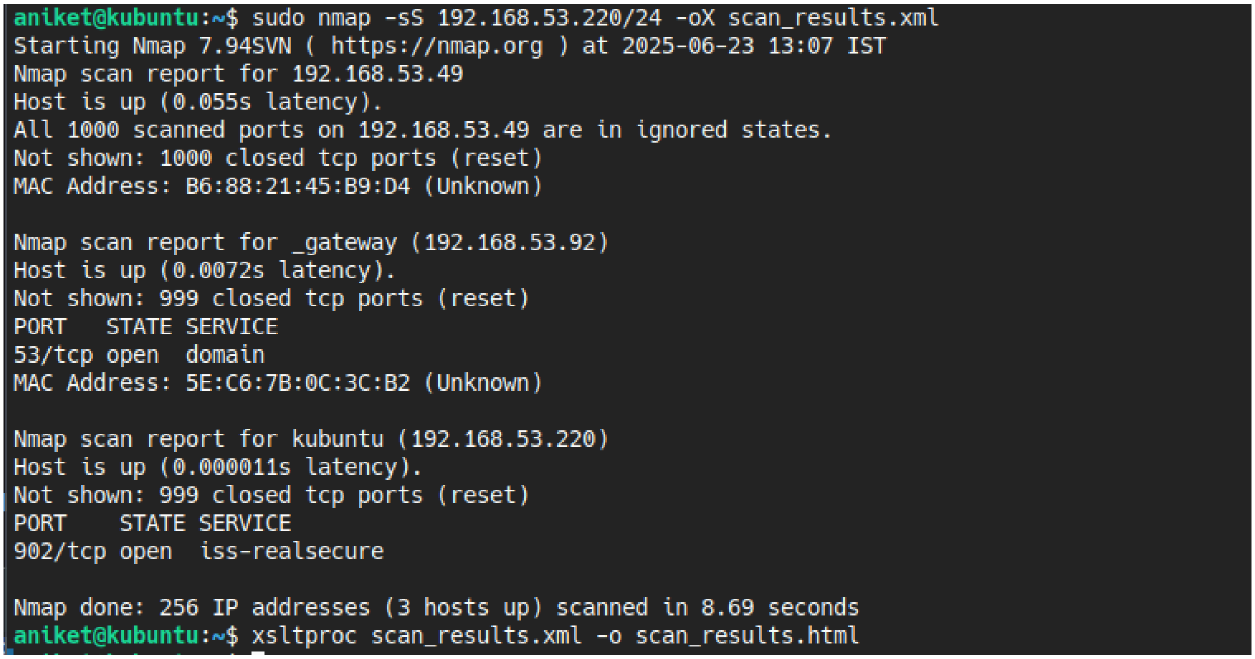


```
# Nmap 7.94SVN scan initiated Mon Jun 23 13:02:29 2025 as: nmap -sS -oN scan_results.txt 192.168.53.220/24
Nmap scan report for 192.168.53.49
Host is up (0.0079s latency).
All 1000 scanned ports on 192.168.53.49 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: B6:88:21:45:B9:D4 (Unknown)

Nmap scan report for _gateway (192.168.53.92)
Host is up (0.0021s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 5E:C6:7B:0C:3C:B2 (Unknown)

Nmap scan report for kubuntu (192.168.53.220)
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
902/tcp open  iss-realsecure

# Nmap done at Mon Jun 23 13:02:38 2025 -- 256 IP addresses (3 hosts up) scanned in 9.19 seconds
```

For HTML:

```
sudo nmap -sS 192.168.53.220/24 -oX scan_results.xml
```

```
xsltproc scan_results.xml -o scan_results.html
```



```
aniket@kubuntu:~$ sudo nmap -sS 192.168.53.220/24 -oX scan_results.xml
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 13:07 IST
Nmap scan report for 192.168.53.49
Host is up (0.055s latency).
All 1000 scanned ports on 192.168.53.49 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: B6:88:21:45:B9:D4 (Unknown)

Nmap scan report for _gateway (192.168.53.92)
Host is up (0.0072s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 5E:C6:7B:0C:3C:B2 (Unknown)

Nmap scan report for kubuntu (192.168.53.220)
Host is up (0.000011s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
902/tcp open  iss-realsecure

Nmap done: 256 IP addresses (3 hosts up) scanned in 8.69 seconds
aniket@kubuntu:~$ xsltproc scan_results.xml -o scan_results.html
```