Name: Satya Chaitanya

Task1: Scan Your Local Network for Open Ports (stealth scan)

Date: 20-10-2025

Tools used: Nmap, Wireshark

Nmap: Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Wireshark:

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

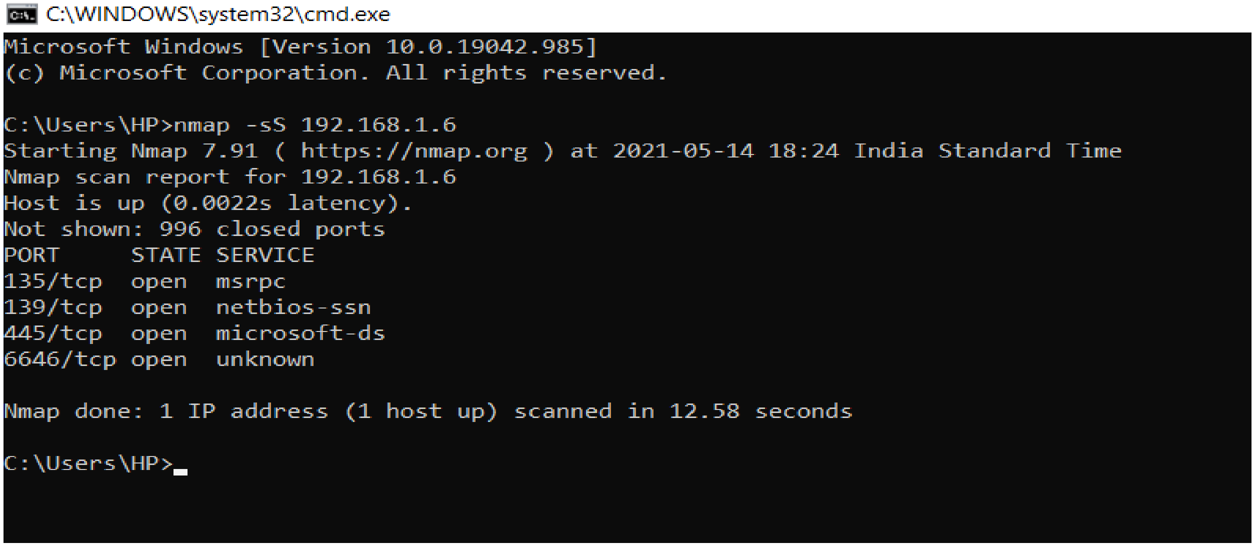
You could think of a network packet analyzer as a measuring device for examining what’s happening inside a network cable, just like an electrician uses a voltmeter for examining what’s happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Stealth scan: A stealth scan in Nmap, known as a TCP SYN scan (-sS), sends a SYN packet to a target port but doesn't complete the full TCP connection. If the port is open, the target responds with a SYN/ACK, which Nmap immediately tears down by sending an RST packet. This "half-open" technique is faster than a regular TCP connect scan and is less likely to be logged by applications, as only full connections are typically recorded.

Command for stealth scan in nmap is “nmap -sS <IP address/address range>”

Nmap

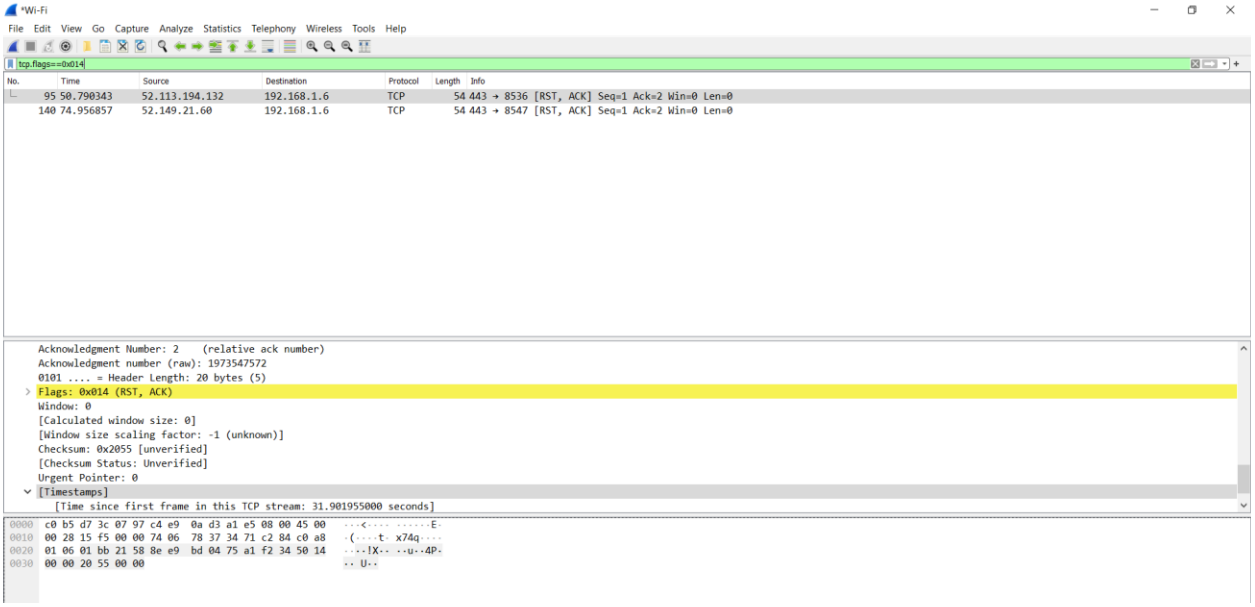


C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>nmap -sS 192.168.1.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-14 18:24 India Standard Time
Nmap scan report for 192.168.1.6
Host is up (0.0022s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6646/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 12.58 seconds

C:\Users\HP>_
```

Open ports obtained: msrpc, netbios-ssn, Microsoft-ds, 6646 port

Wireshark capture



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags==0x014

```
No.  Time        Source           Destination   Protocol  Length  Info
  95 50.790343   52.113.194.132   192.168.1.6   TCP           54  443 → 8536 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
 140 74.956857   52.149.21.60     192.168.1.6   TCP           54  443 → 8547 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
```

```
    Acknowledgment Number: 2    (relative ack number)
    Acknowledgment number (raw): 1973547572
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x014 (RST, ACK)
    Window: 0
    [Calculated window size: 0]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x2055 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ∨ [Timestamps]
      [Time since first frame in this TCP stream: 31.901955000 seconds]
```

```
0000  c0 b5 d7 3c 07 97 c4 e9  0a d3 a1 e5 08 00 45 00   ···<···· ······E·
0010  00 28 15 f5 00 00 74 06  78 37 34 71 c2 84 c0 a8   ·(····t· x74q····
0020  01 06 01 bb 21 58 8e e9  bd 04 75 a1 f2 34 50 14   ····!X·· ··u··4P·
0030  00 00 20 55 00 00                                  ·· U··
```