**1.Insta l Nmap from official website.**

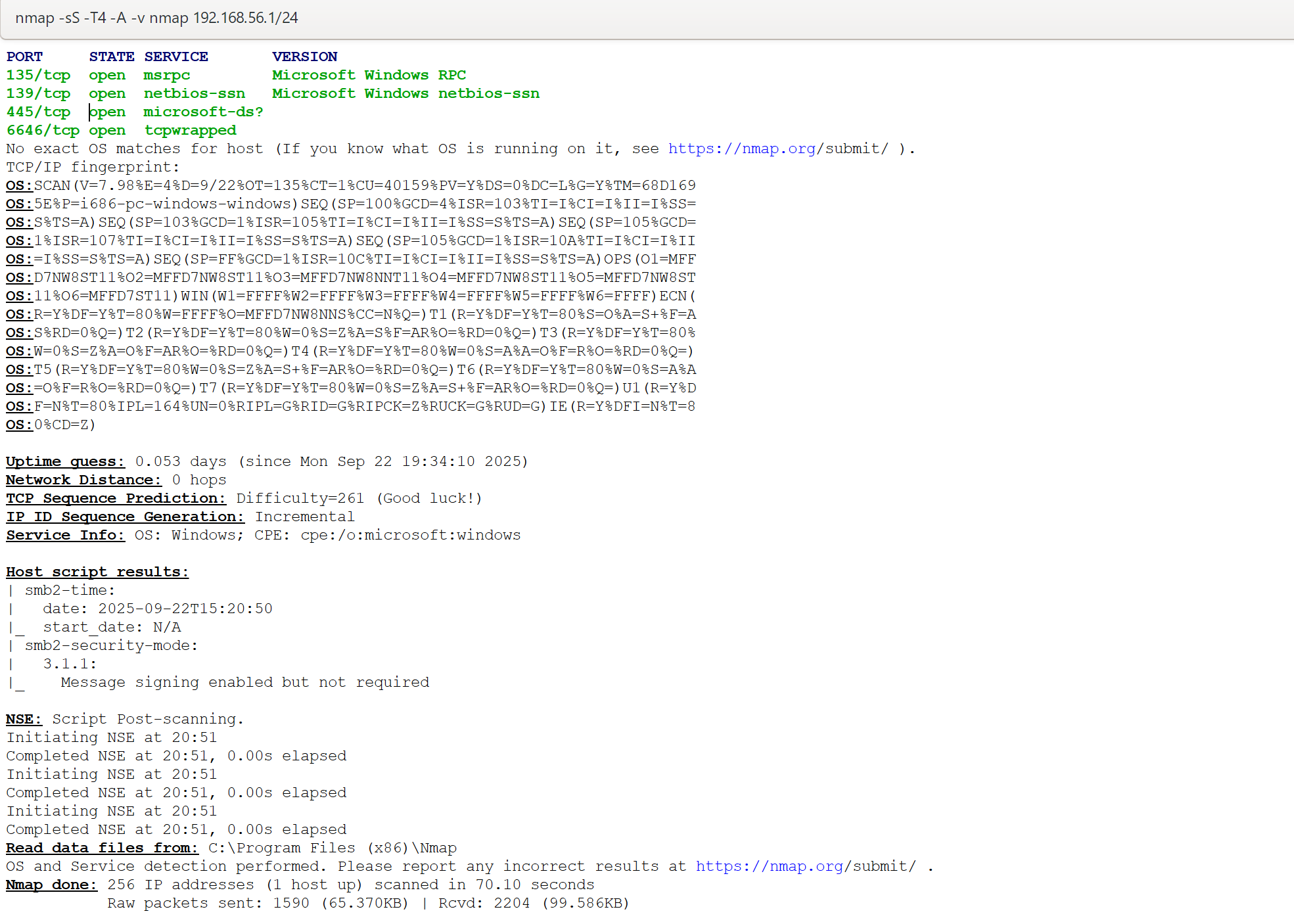


Already Installed(windows)

**2.Find your local IP range (e.g., 192.168.1.0/24);**

192.1\*\*.\*\*.\*

**3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.**





**4.Note down IP addresses and open ports found.**

* IP address:- 192.1\*\*.\*\*.\*/24
* Open Ports-

1. Port 135/tcp:
2. Port 139/tcp:
3. Port 445/tcp:
4. Port 6646/tcp:

**5.Research common services running on those ports**.

* Port 135/tcp - msrpc

Service: Microsoft Remote Procedure Call (RPC) Endpoint Mapper.

* Port 139/tcp - netbios-ssn

-Service: NetBIOS Session Service.

* Port 445/tcp –

-Service: Server Message Block (SMB), also known as Microsoft Directory Services.

* Port 6646/tcp – topwrapped

- Service: This is not a standard, well-known service port. The name topwrapped is a generic placeholder Nmap sometimes uses.

**6.Identify potential security risks from open ports.**

-SMB and NetBIOS Exposure (Ports 135, 139, 445)

-Potential Backdoor or Trojan: Port 6646is not associated with any common, legitimate service. Its presence could indicate a **Remote Access Trojan (RAT)** or other malware has been installed, giving an attacker a persistent backdoor into the system.