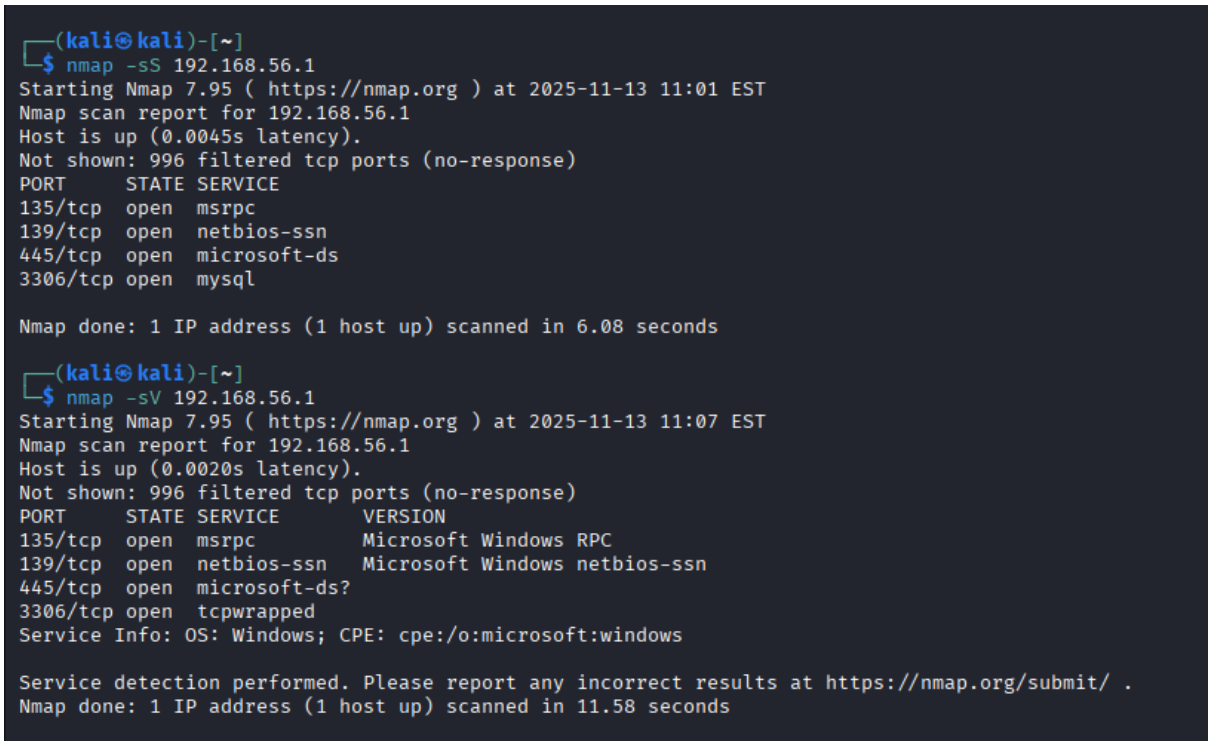
1. Result of Nmap Scan of my ip address.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.56.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-13 11:01 EST
Nmap scan report for 192.168.56.1
Host is up (0.0045s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 6.08 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-13 11:07 EST
Nmap scan report for 192.168.56.1
Host is up (0.0020s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  tcpwrapped
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.58 seconds
```

2. Potential security risks from open ports.

1. Understand What Each Port Means (Risk Level)

135 – Microsoft RPC (High Risk)

Used by Windows Remote Procedure Call.

Attackers use it for DCE/RPC exploits, lateral movement.

Common in WannaCry, Conficker, EternalBlue family.

➞ Risk: High

➞ Why: Often targeted for remote code execution (RCE).

---

3. 137, 138, 139 – NetBIOS (Very High Risk)

Used for Windows file sharing before SMB2.

Exposes:
Computer name
Users
Shared folders
Domain/workgroup information
➞ Risk: Very High
➞ Why: Can leak system info, allow enumeration (nbtscan, smbclient, enum4linux).

---

4. 445 – SMB / Microsoft-DS (Extremely High Risk)

This is the most dangerous open port on Windows.
Used for SMB file sharing.
Vulnerable historically (and still in many systems):
EternalBlue
WannaCry
SMBv1 vulnerabilities

Allows:
Password brute-force
Share enumeration
Exploits (Metasploit modules)

➞ Risk: Severe
➞ Why: Remote Code Execution (RCE) possible.

---

5. 3306 – MySQL Database (High Risk)

   If MySQL is exposed:
   Attackers can brute-force SQL credentials.
   If password is weak → database takeover.
   SQL injection testing possible.
   Sensitive data exposure risk.

   ➞ Risk: High
   ➞ Why: Database compromise likely.
