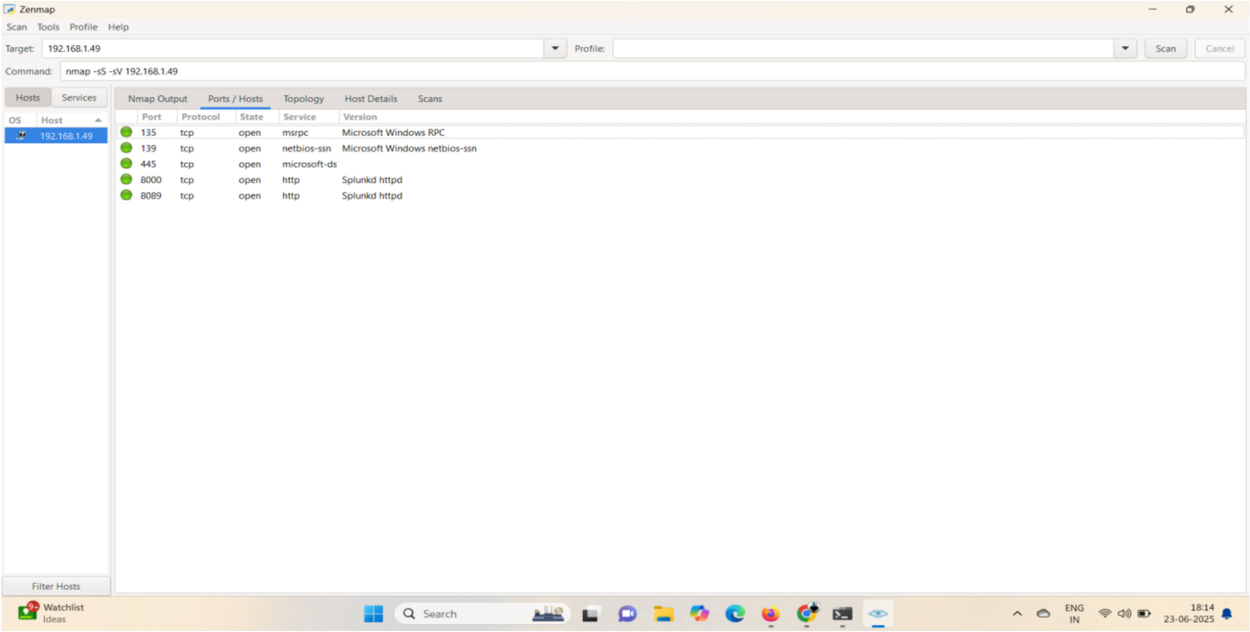
By Nmap scan results for the IP address `192.168.1.49` ,I identified potential security risks from the open ports:



Target: 192.168.1.49

Profile:

Command: nmap -sS -sV 192.168.1.49

OS	Host
	192.168.1.49

	Port	Protocol	State	Service	Version
●	135	tcp	open	msrpc	Microsoft Windows RPC
●	139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
●	445	tcp	open	microsoft-ds	
●	8000	tcp	open	http	Splunkd httpd
●	8089	tcp	open	http	Splunkd httpd

Scan Results Summary

-**IP Address**: 192.168.1.49

-**Open Ports and Services**:

- **135/tcp**: Microsoft Windows RPC

- **139/tcp**: NetBIOS-ssn (Microsoft Windows netbios-ssn)

- **445/tcp**: Microsoft-ds (Microsoft Windows)

- **8089/tcp**: Splunk http (Splunk httpd)

- **Service Info**: OS: Windows; CPE: cpe:/o:microsoft:windows

Potential Security Risks

1. Port 135 (Microsoft Windows RPC):

- **Risk**: Remote Procedure Call (RPC) is used by Windows for communication between systems. If unpatched, it can be exploited by vulnerabilities like the MS03-026 (Blaster worm) or MS17-010 (EternalBlue) to execute remote code.

- **Concern**: Exposure to outdated systems or lack of patches increases vulnerability.

2. Port 139 (NetBIOS-ssn):

- **Risk**: NetBIOS over TCP (NetBIOS-ssn) is an older protocol prone to man-in-the-middle attacks and unauthorized access if not secured. It can expose file shares or printer services.

- **Concern**: Unnecessary exposure in modern networks; potential for credential theft.

3. Port 445 (Microsoft-ds):

- **Risk**: Microsoft Directory Services (SMB) is commonly targeted. The MS17-010 vulnerability (EternalBlue) allows remote code execution, leading to ransomware (e.g., WannaCry) or data breaches.

- **Concern**: High risk if the system is unpatched or running an outdated Windows version.

4. Port 8089 (Splunk http):

- **Risk**: Splunk’s HTTP interface (port 8089) is used for management. If not properly secured with authentication or encryption, it could be exploited for unauthorized access to logs or system control.

- **Concern**: Default credentials or weak configurations may allow attackers to gain entry.

General Observations

- ****Windows Environment****: The OS detection indicates a Windows system, which may have additional vulnerabilities if not regularly updated.

- ****Multiple Open Ports****: The presence of multiple service ports suggests a server or workstation with extensive network exposure, increasing the attack surface.

Recommendations to Mitigate Risks

- ****Patch Systems****: Update the Windows OS and Splunk software to the latest versions to address known vulnerabilities.

- ****Disable Unused Services****: If ports 135, 139, or 445 are not required, disable them via firewall settings or service management.

- ****Secure Splunk****: Enforce strong authentication, use HTTPS, and restrict access to port 8089.

- ****Firewall Rules****: Configure a firewall to block unnecessary inbound traffic to these ports.

- ****Monitor Activity****: Use tools like Wireshark to detect unusual traffic patterns on these ports.