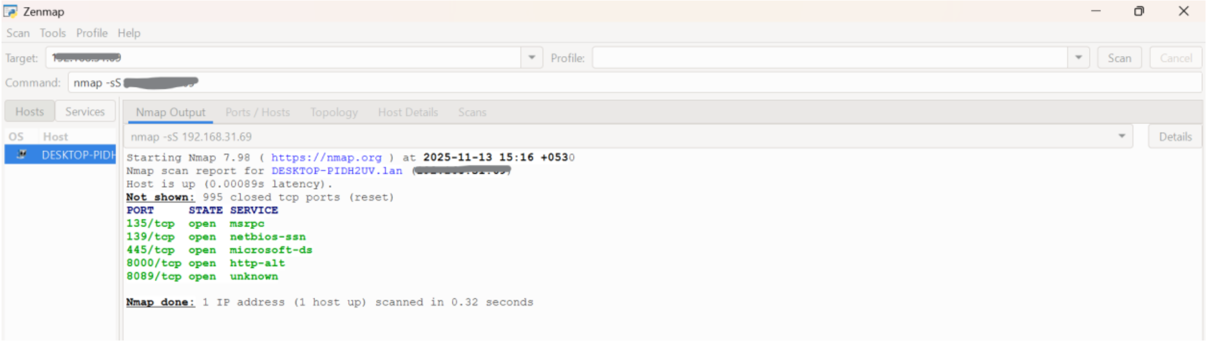
Cyber Security Internship

Task1: Scan your Local Network for Open Ports

- First, I had installed the Nmap and Wireshark of Windows version.
- From Command Prompt (cmd) – <ipconfig>, I got the details of my Windows IP configuration.
- My IPv4 address – 192.168.x.x
- Subnet mask – 255.255.255.0
- With the help of IP address, I ran the scan with command → nmap -sS 192.168.x.x & performed TCP SYN scan
-

Port	Common Service	Potential Risks / Threats
135/tcp	MSRPC (Microsoft RPC)	• Remote Code Execution (RCE) vulnerabilities• DCOM abuse for lateral movement• System/service enumeration by attackers• Used in old RPC-based worms (e.g., MS08-067)
139/tcp	NetBIOS-SSN	• Username/share enumeration• NBT-NS poisoning attacks• SMB brute-force attempts• Information leakage (device name, workgroup)
445/tcp	SMB (Microsoft-DS)	• High-risk RCE vulnerabilities (EternalBlue)• WannaCry/NotPetya ransomware attacks• Lateral movement (Pass-the-Hash, Pass-the-Ticket)• Unauthorized access to shared folders• SMB relay attacks
8000/tcp	HTTP-Alt	• Weak/no authentication on dashboards• OWASP Top 10 web exploits (XSS, SQLi, LFI)• Directory traversal• IoT device exposure• Sensitive data leakage
8089/tcp	Splunk Management Port / Custom API	• Unauthorized API access• Privilege escalation via Splunkd• Misconfigured authentication/TLS• Remote script execution via API• Custom services may contain unknown or unpatched vulnerabilities

Below are the screenshots of Nmap Scan:



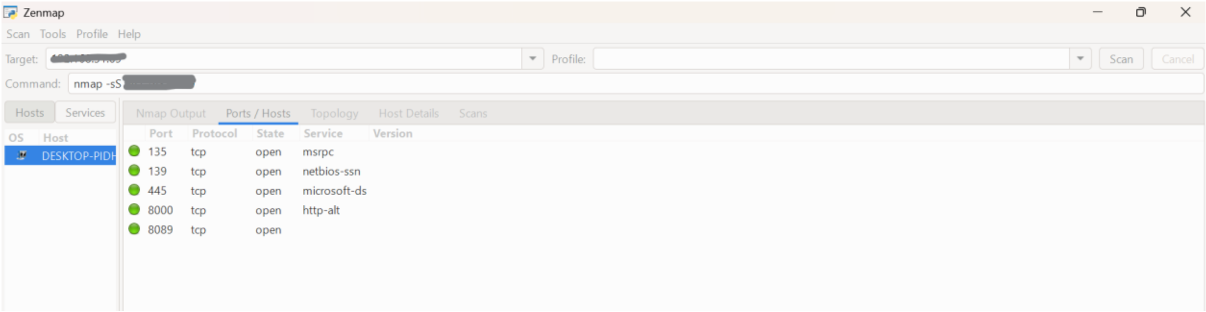
Target: [redacted]

Command: nmap -sS [redacted]

nmap -sS 192.168.31.69

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-13 15:16 +0530
Nmap scan report for DESKTOP-PIDH2UV.lan [redacted]
Host is up (0.00089s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8000/tcp open  http-alt
8089/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```



Target: [redacted]

Command: nmap -sS [redacted]

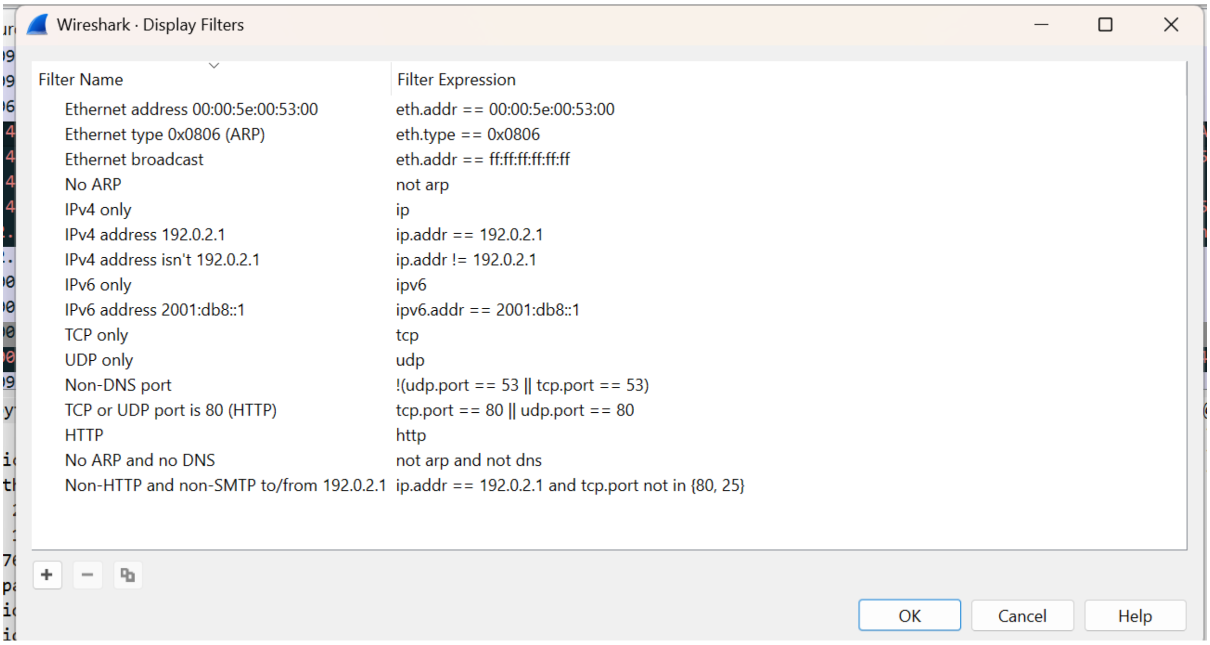
OS	Host
	DESKTOP-PIDH

	Port	Protocol	State	Service	Version
●	135	tcp	open	msrpc	
●	139	tcp	open	netbios-ssn	
●	445	tcp	open	microsoft-ds	
●	8000	tcp	open	http-alt	
●	8089	tcp	open		

- Below is the saved scan results in HTML file:

C:\Users\DELL 5400\Desktop\Cybersecurity Navya\Elevate Labs\portscan.html

- I had also analyzed packet capture with Wireshark.



Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1	ip.addr != 192.0.2.1
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS port	!(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 || udp.port == 80
HTTP	http
No ARP and no DNS	not arp and not dns
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and tcp.port not in {80, 25}

I had learned how to use Nmap & Wireshark, with my first scanning and analyzing of open ports. And got to know a lot of info to check the IP address - status, monitor and analyzing of network service.