🔍 Nmap Network Scan Report

📅 Date: June 23, 2025

🕒 Time: 16:58 (GMT +5:30)

🔧 Tool Used: Zenmap (Nmap 7.97 GUI)

🔍 Scan Type: TCP SYN Scan (-sS)

🖥️ Target Subnet: 192.168.206.0/24

📈 Total Hosts Scanned: 256

✅ Live Hosts Detected: 2

🖧 Live Hosts & Open Ports

1. Host: 192.168.206.1

- **MAC Address:** *Not shown*
- **Latency:** 0.000041s
- **Open TCP Ports:**

Port	State	Service
80	Open	HTTP

Port	State	Service
135	Open	MSRPC
139	Open	NetBIOS-SSN
445	Open	Microsoft-DS
903	Open	ISS Console Manager
5357	Open	WSDAPI
8090	Open	OpsMessaging

---

2. Host: 192.168.206.254

- **MAC Address:** 00:50:56:E5:80:BB (VMware)
- **Open TCP Ports:** None reported
- **All 1000 scanned ports:** Filtered (no response)

🛡️ Security Observations

- **Ports 135, 139, 445:** Typically related to Windows file sharing and RPC. These may expose vulnerabilities (e.g., EternalBlue) if not properly secured.
- **Port 80:** Indicates a web server – check for outdated software or admin panels.
- **Port 903:** Related to VMware or ISS – potentially admin services.
- **Port 8090:** Often used for web management interfaces or custom apps.
- **Port 5357:** WSDAPI – Windows service for device discovery over the network.

📁 Recommendations

1. **Close Unused Ports:** Disable services that are not needed.
2. **Patch Systems:** Ensure all services are updated to the latest version.
3. **Firewall Rules:** Implement strict rules to restrict access to ports like 139, 445, and 135.

4. **Monitor Traffic:** Use Wireshark or similar tools to detect anomalies or unauthorized access.
5. **Run Version Scan:** Use nmap -sV 192.168.206.1 to determine service versions.

💾 Saving Report

You can export this scan from Zenmap using:

- **Text Format**: File → Save Scan → .txt
- **XML/HTML**: Use -oX or -oA in command line or Zenmap profile