**Step-by-Step: Using Nmap for Vulnerability Scanning on Windows**

**1. Install Nmap on Windows**

**Download from Official Site:**

https://nmap.org/download.html

Choose the **"Self-installer"** version for Windows.

### ****2. Open a Command Prompt****

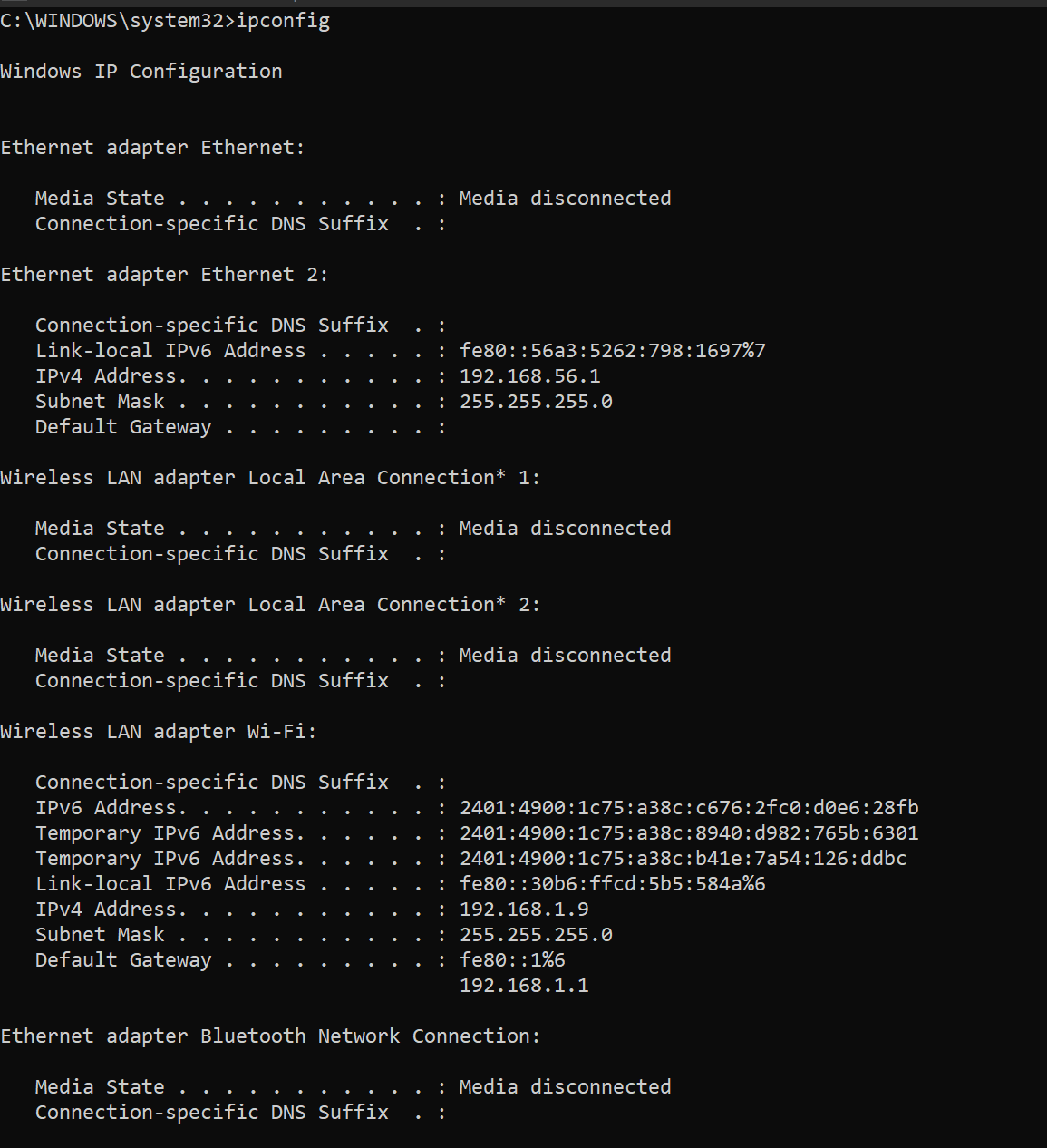
**Press** Start**, type cmd, right-click** Command Prompt**, choose** "Run as administrator"**.**

### ****3. Find Your IP Address****

Open Command Prompt and run: ipconfig

Look under your **Ethernet** or **Wi-Fi adapter** for something like:

IPv4 Address. . . . . . . . . . . : 192.168.1.5



### ****4. Run a Full Service & Vulnerability Scan****

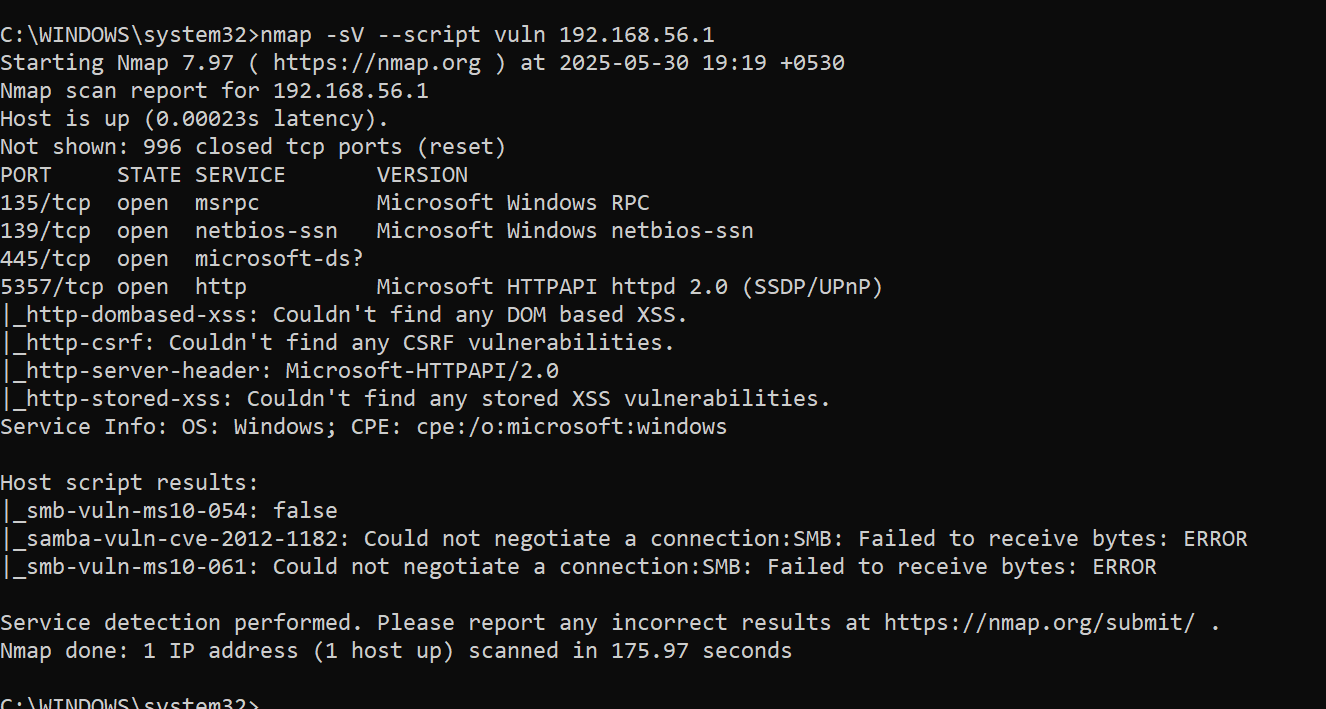
**Basic Vulnerability Scan:**

*nmap -sV --script vuln <your-ip>*

This tells Nmap to:

-sV: Detect services and versions

--script vuln: Run the default vulnerability detection scripts



**Host Information**

* **Host is up** – The system is online and reachable.
* **Latency** – Response time is extremely low: 0.00023s.

**Ports and Services**

Out of 1000 scanned TCP ports, **996 are closed**, and **4 are open**:

1. **135/tcp – msrpc**
   * Microsoft RPC (Remote Procedure Call)
   * Used by various Windows services for inter-process communication.
2. **139/tcp – netbios-ssn**
   * NetBIOS Session Service
   * Supports file/printer sharing over the network in older Windows environments.
3. **445/tcp – microsoft-ds**
   * SMB over TCP
   * Used for modern Windows file sharing and various network services.
4. **5357/tcp – http (Microsoft HTTPAPI httpd 2.0)**
   * A lightweight HTTP server for Windows services (e.g., SSDP/UPnP).

**HTTP Vulnerability Scripts**

These scripts scanned the HTTP service for common vulnerabilities:

* **DOM-based XSS** – None found.
* **CSRF** – None found.
* **Stored XSS** – None found.
* **HTTP Server Header** – Shows Microsoft-HTTPAPI/2.0.

**SMB Vulnerability Checks**

* **smb-vuln-ms10-054** – Not vulnerable.
* **smb-vuln-ms10-061** – Scan failed; possibly blocked or unsupported SMB version.
* **samba-vuln-cve-2012-1182** – Could not negotiate connection; likely not running Samba (more common on Linux).

**Service Info**

* **Operating System** – Detected as Windows.
* **CPE** – cpe:/o:microsoft:windows (Common Platform Enumeration).

**Recommendations:**

* Ensure the system is **fully patched**, especially services exposed to the network (SMB, HTTP).
* **Disable NetBIOS** (port 139) if not needed — it's outdated and often unnecessary.
* Use a **firewall** to limit access to these ports.
* **Monitor** for suspicious activity on port 445 (frequent target for malware/ransomware).