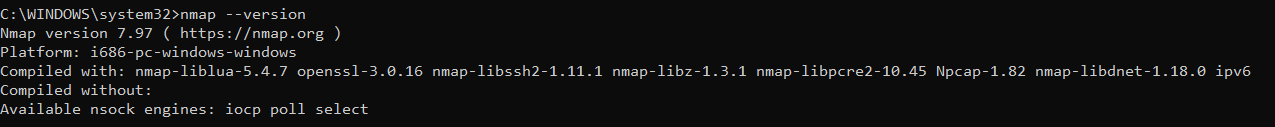
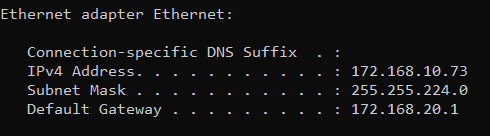
**TASK – 1**

### Step 1: Install Nmap

1. Go to the official Nmap website: <https://nmap.org/download.html>
2. Download the Latest stable release self-installer: [nmap-7.97-setup.exe](https://nmap.org/dist/nmap-7.97-setup.exe)
3. After installation, open a terminal or Command Prompt to verify:
   * nmap –version

### ****Step 2: Find Your Local IP and Subnet Range****

1. Open command prompt and run:
   * Ipconfig
2. Look for your **IPv4 Address** and **Subnet Mask**.



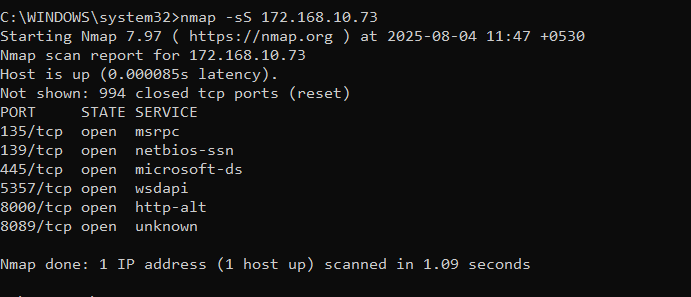
### ****Step 3: Perform a TCP SYN Scan****

1. Run Nmap in terminal:
   * nmap -sS 172.168.10.73
2. We’ll see output listing live hosts, open ports, and services.

### ****Step 4: Note Down IPs and Open Ports****

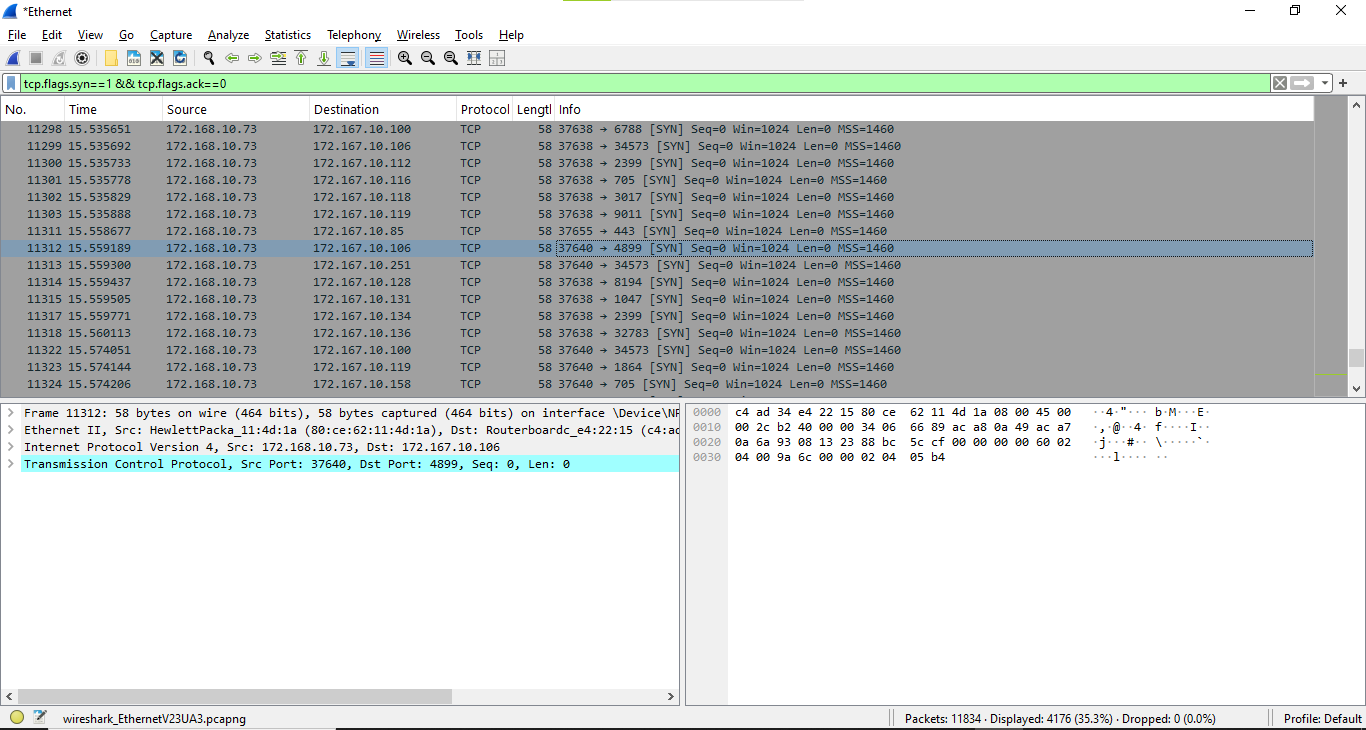
Review of the Nmap results.

* IP Address (172.168.10.73)
* Hostname
* Open Ports



### ****Step 5 (Optional): Use Wireshark for Packet Capture****

1. Download & install: https://www.wireshark.org/download.html
2. Start Wireshark and begin capturing on your active network interface.
3. Run the Nmap scan again and observe the packets.
4. Use filters like:
   * tcp.flags.syn==1 && tcp.flags.ack==0



To see SYN packets sent during the scan.

### ****Step 6: Research Common Services on Ports****

Refer the websites for more info on ports:

* https://www.speedguide.net/port.php
* https://nmap.org/book/services.html

## 📝 Nmap Scan Analysis Report

### 🔍 ****1. Commonly Seen Ports and Their Services****

| **Port** | **Service Name** | **Description** | **Risk Level** | **Common Use Cases** |
| --- | --- | --- | --- | --- |
| **22** | SSH | Secure Shell for remote access to systems. | ⚠️ Medium | Remote login to Linux/Unix systems |
| **25** | SMTP | Simple Mail Transfer Protocol (email sending). | ⚠️ Medium | Mail servers (could be spam relay risk) |
| **80** | HTTP | Unencrypted web traffic. | ⚠️ Medium | Hosting websites or apps |
| **81** | hosts2-ns (alternate) | Alternate HTTP or name service. | ⚠️ Medium | Often used by management interfaces |
| **443** | HTTPS | Secure web traffic. | Low | Encrypted web services |
| **465** | SMTPS | Secure SMTP over SSL. | Low | Secure email sending |
| **587** | Submission | Email submission with authentication. | Low | Outbound mail from email clients |
| **993** | IMAPS | Secure IMAP for receiving email. | Low | Secure email access |
| **5432** | PostgreSQL | PostgreSQL database service. | ⚠️ Medium | Database servers |
| **8080** | HTTP-Proxy | Alternative HTTP service, often proxy or admin interfaces. | ⚠️ Medium | Proxies, dev servers |
| **8081** | blackice-icecap | Often used by older intrusion detection software or custom apps. | ⚠️ Medium | Legacy/unknown applications |
| **8082** | blackice-alerts | As above, might be alert ports for intrusion detection systems. | ⚠️ Medium | Legacy/unknown applications |
| **8443** | HTTPS-Alt | Alternate HTTPS port. | ⚠️ Medium | Web admin consoles, dashboards |
| **10001** | SCP-Config | Often used by IoT devices and network equipment for config. | ⚠️ High | May be vulnerable if exposed |
| **10002** | Documentum | EMC Document Management System. | ⚠️ Medium | Enterprise document systems |
| **20000** | DNP (Distributed Net Protocol) | Used in industrial SCADA systems. | 🔴 High | Industrial systems (must not be exposed) |
| **30000** | NDMPs | Network Data Management Protocol (used for backups). | ⚠️ Medium | Backup solutions |
| **50000** | IBM-DB2 | IBM DB2 Database Server. | ⚠️ Medium | Database systems |
| **2525** | MS-V-Worlds | Alternate SMTP or custom services. | ⚠️ Medium | Custom or legacy use |
| **7999** | IRDMI2 | Often custom or legacy services. | ⚠️ Medium | Unknown/needs further analysis |
| **8083** | US-SRV | Unknown/custom application port. | ⚠️ Medium | Requires investigation |

### 🔧 ****2. Observations & Recommendations****

#### 🔹 **HTTPS (443) Found on Many Hosts**

* Normal in enterprise environments (load balancers, internal web apps, APIs).
* ➤ Ensure proper SSL/TLS configuration and certificates.

#### 🔹 **Multiple PostgreSQL (5432) and DB2 (50000) Ports**

* ⚠️ These are database services and **should not be exposed to public networks**.
* ➤ Limit access using firewalls or internal VLANs.

#### 🔹 **Web Services on 80, 8080, 8443, 8000, 8081**

* ➤ Check if these are **login/admin interfaces** (especially on 8080/8443).
* ➤ Use HTTPS instead of HTTP to encrypt traffic.

#### 🔹 **DNP (20000) and SCP-Config (10001)**

* 🔴 High-risk in ICS/SCADA environments.
* ➤ These should be **strictly segmented** from IT/office networks.

#### 🔹 **Mail Ports (25, 465, 587)**

* ➤ Could be mail servers – ensure they are not **open relays** (spam risk).

#### 🔹 **Filtered Ports**

* Many hosts showed **filtered or closed** ports → indicates firewall or IDS/IPS systems are in place, which is good.

### 🛠️ ****Suggested Next Steps****

| **Step** | **Action** |
| --- | --- |
| 1 | Identify services behind unusual ports (7999, 10001, 8083) via netstat, lsof, or endpoint inspection. |
| 2 | Run vulnerability scans on critical systems with open services using tools like **Nessus**, **OpenVAS**, or **Nmap scripts**. |
| 3 | Harden hosts with exposed ports — especially web and database servers. |
| 4 | Document internal IP → service mappings in your network documentation. |
| 5 | Block unnecessary ports from external exposure (via firewall rules or security groups). |
| 6 | Perform regular scans to detect unauthorized services. |

### 📁 ****How to Save These Results****

You can export and save the results of your scan using:

nmap -sS 172.167.10.0/24 -oN scan\_results.txt

Or save as XML for report generation:

nmap -sS 172.167.10.0/24 -oX scan\_results.xml

### ****Step 7: Identify Potential Security Risks****

## 🔐 Potential Security Risks from Open Ports

### 🔸 ****Port 135 – MSRPC (Microsoft Remote Procedure Call)****

* 📌 **Risk:** Often targeted in Windows exploits like **WannaCry**, **Blaster**, etc.
* ⚠️ **Vulnerability:** Can expose RPC-based services to remote code execution.
* **Recommendation:** Block this port from external networks; only allow within internal trusted zones.

### 🔸 ****Port 139 – NetBIOS Session Service****

* 📌 **Risk:** Used for Windows file/printer sharing; susceptible to **information leakage**, **man-in-the-middle**, and **SMB relay attacks**.
* ⚠️ **Vulnerability:** Can expose computer name, domain, and shared files.
* **Recommendation:** Disable NetBIOS over TCP/IP unless required; block externally.

### 🔸 ****Port 445 – SMB (Microsoft-DS)****

* 📌 **Risk:** Commonly exploited in **ransomware attacks** (e.g., EternalBlue, WannaCry).
* ⚠️ **Vulnerability:** Remote code execution, file sharing abuse.
* **Recommendation:** Patch systems, disable if not needed, block on perimeter firewalls.

### 🔸 ****Port 5357 – WSDAPI (Web Services for Devices)****

* 📌 **Risk:** Windows service often enabled on local networks, but rarely needed.
* ⚠️ **Vulnerability:** Can be abused for reconnaissance or unwanted device exposure.
* **Recommendation:** Disable on unmanaged or exposed devices.

### 🔸 ****Port 8000 – HTTP-Alt****

* 📌 **Risk:** Could host a **web dashboard** or **development server** with weak authentication.
* ⚠️ **Vulnerability:** Information leakage, default credentials, outdated web apps.
* **Recommendation:** Use HTTPS, add authentication, restrict access.

### 🔸 ****Port 8089 – Unknown / Custom Application****

* 📌 **Risk:** Not a standard port — may run **Splunk**, **custom apps**, or **management UIs**.
* ⚠️ **Vulnerability:** Often overlooked during security reviews; may lack logging or patching.
* **Recommendation:** Identify the service, scan it with Nmap scripts (-sV -sC), and secure it.

## 🚨 Summary of Key Risks

| **Port** | **Risk Level** | **Description** |
| --- | --- | --- |
| 135 | High | RPC-based remote code execution (target of past worms) |
| 139 | High | NetBIOS file sharing and enumeration |
| 445 | Critical | SMB exploits like EternalBlue |
| 5357 | Medium | WSD exposure and information leakage |
| 8000 | Medium | Unsecured web servers or dashboards |
| 8089 | Unknown | Custom or unpatched service — needs investigation |

## 🛡️ General Security Recommendations

1. **Patch regularly** – Keep Windows and all services up to date.
2. **Block unnecessary ports** – Especially on firewalls and edge devices.
3. **Use strong authentication** – For any exposed web interfaces.
4. **Monitor open ports** – With tools like nmap, netstat, and endpoint protection.
5. **Run vulnerability scans** – Use Nessus, OpenVAS, or nmap --script vuln.

### ****Step 8: Save Scan Results****

* Save results as a **text file**:

nmap -sS 192.168.1.0/24 -oN scan\_result.txt

* Or as **HTML/XML**:

nmap -sS 192.168.1.0/24 -oX scan\_result.xml

!!!   
Scan Results are saved in the Text File: scan\_result.txt

!!!