

## TASK – 1

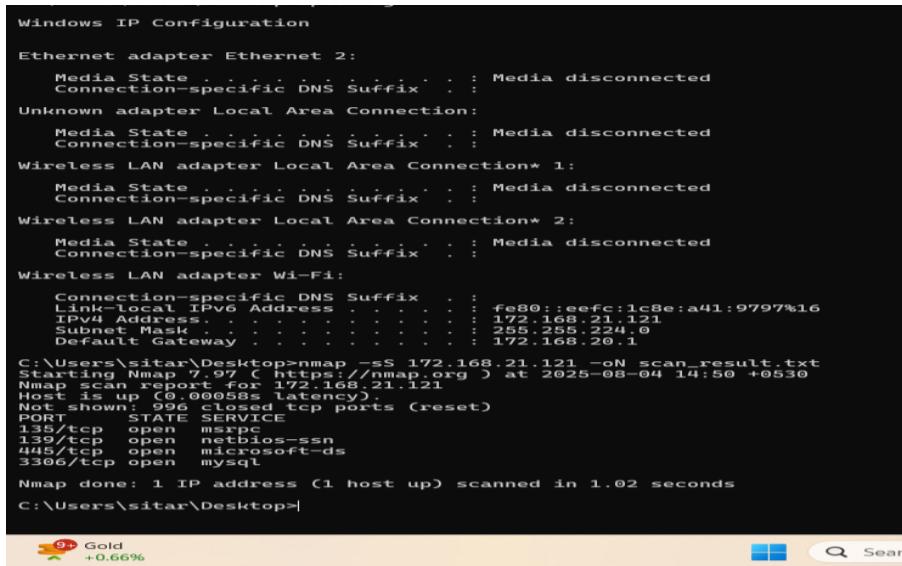
### **Step 1: Install Nmap**

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

```
C:\WINDOWS\system32>nmap --version
Nmap version 7.97 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.4.7 openssl-3.0.16 nmap-libssh2-1.11.1 nmap-libz-1.3.1 nmap-libpcre2-10.45 Npcap-1.82 nmap-libdnet-1.18.0 ipv6
Compiled without:
Available nsock engines: iocp poll select
```

### **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**.



The screenshot shows a Windows Command Prompt window. At the top, it displays "Windows IP Configuration". Below that, it lists several network adapters: "Ethernet adapter Ethernet 2", "Unknown adapter Local Area Connection", "Wireless LAN adapter Local Area Connection\*", and "Wireless LAN adapter Local Area Connection\* 2". Each adapter shows its status as "Media disconnected" and "Connection-specific DNS Suffix". Under "Unknown adapter Local Area Connection", it shows the "Link-local IPv6 Address" as fe80::eefc:1c8e:a41:9797%16 and the "Default Gateway" as 172.168.20.1. In the bottom half of the window, the command "C:\Users\sitar\Desktop>nmap -ss 172.168.21.121 -oN scan\_result.txt" is run, followed by the output of the Nmap scan report. The report shows one host up at 172.168.21.121 with various open ports and services, including port 139/tcp (netbios-ssn) and port 445/tcp (microsoft-ds).

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

1. Run Nmap in terminal:  
→ nmap -sS 172.168.22.111
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 (172.168.22.111)
- Hostname
- Open Ports

```
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::eefc:1c8e:a41:9797%16
IPv4 Address. . . . . : 172.168.21.121
Subnet Mask . . . . . : 255.255.224.0
Default Gateway . . . . . : 172.168.20.1

C:\Users\sitar\Desktop>nmap -sS 172.168.21.121 -oN scan_result.txt
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-04 14:50 +0530
Nmap scan report for 172.168.21.121
Host is up (0.00058s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3306/tcp   open  mysql

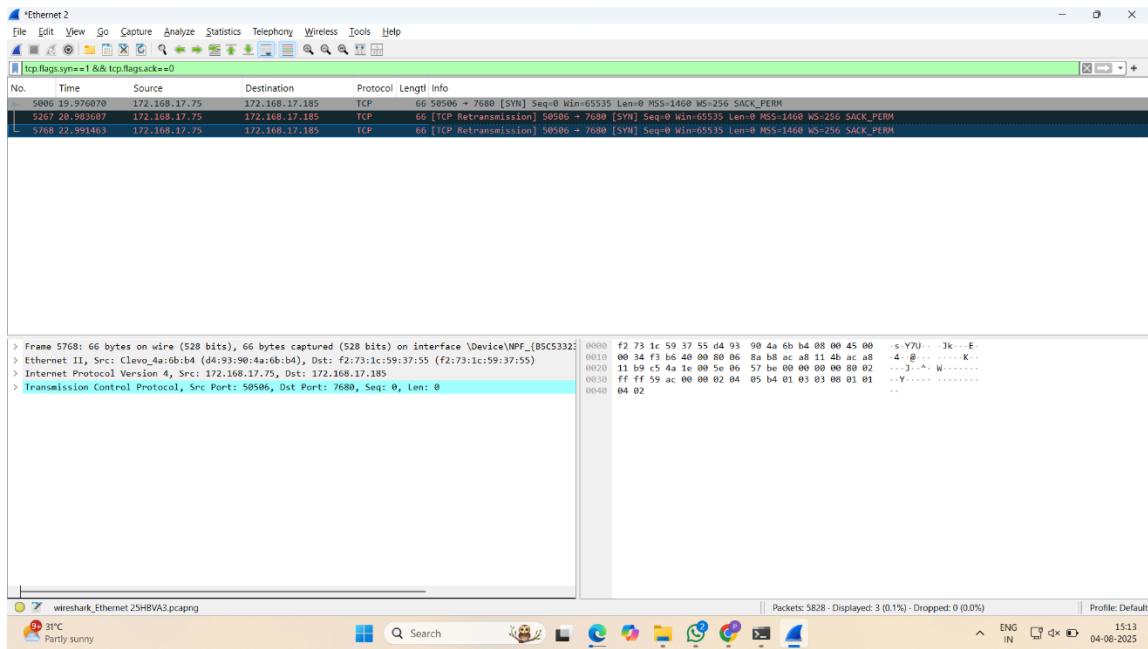
Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds

C:\Users\sitar\Desktop>
```

### **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	Description
135/tcp	msrpc	Microsoft Remote Procedure Call
139/tcp	netbios-ssn	NetBIOS Session Service
445/tcp	microsoft-ds	Microsoft Directory Services (SMB)
3306/tcp	mysql	MySQL Database

### 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 – 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	Service	Risk Description	Potential Impact
135/tcp	microsoft-ds	Microsoft RPC service port; vulnerable to remote code execution and privilege escalation exploits.	Remote code execution, privilege escalation
139/tcp	netbios-ssn	NetBIOS session service; commonly targeted for SMB-related attacks and information disclosure.	Information leakage, unauthorized access
445/tcp	microsoft-ds	SMB over TCP port; frequently targeted in ransomware and exploits like EternalBlue.	Ransomware attacks, data breaches
3306/tcp	mysql	MySQL database port; risk of unauthorized access if misconfigured or exposed.	Data theft, SQL injection attacks

---

## 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  
!!!