

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
3. After installation, open a terminal or Command Prompt to verify:

→ nmap --version

```
C:\Users\aksha>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-lib
z-1.3.1 nmap-libpcap-1.0.4 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.

```

C:\Users\aksha>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 5:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::bdc7:679c:ec1b:67c5%19
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::47d4:f11b:98b3:5c6e%14
    IPv4 Address. . . . . : 192.168.253.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e6ae:4603:6ad7:2c8a%10
    IPv4 Address. . . . . : 192.168.154.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

```

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

```
C:\Windows\System32>nmap -sS 192.168.1.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-04 19:11 +0530
Nmap scan report for 192.168.1.1
Host is up (0.0065s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
1900/tcp  open  upnp
MAC Address: 40:ED:00:C7:41:28 (TP-Link Limited)
```

```
Nmap scan report for 192.168.1.3
Host is up (0.0089s latency).
All 1000 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: C2:41:8E:4F:A6:CC (Unknown)
```

```
Nmap scan report for 192.168.1.4
Host is up (0.058s latency).
All 1000 scanned ports on 192.168.1.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 70:5F:A3:69:4B:F1 (Xiaomi Communications)
```

```
Nmap scan report for 192.168.1.28
Host is up (0.042s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 14:D4:24:D9:A4:C5 (AzureWave Technology)
```

```
Nmap scan report for 192.168.1.32
Host is up (0.15s latency).
All 1000 scanned ports on 192.168.1.32 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 72:27:54:66:F5:34 (Unknown)
```

```
Nmap scan report for 192.168.1.37
Host is up (0.00084s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
```

```
912/tcp   open  apex-mesh
3306/tcp  open  mysql
5432/tcp  open  postgresql
```

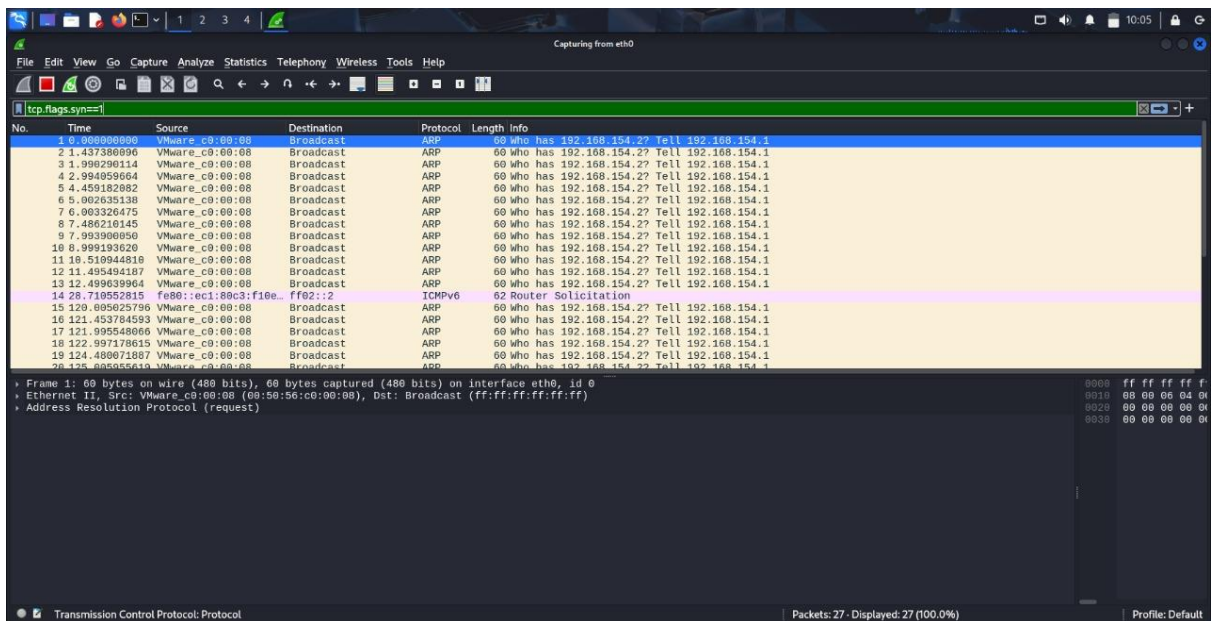
```
Nmap done: 256 IP addresses (6 hosts up) scanned in 310.67 seconds
```

```
C:\Windows\System32>_
```

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`



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 (spam risk if misconfigured)
80	HTTP	Unencrypted web traffic.	⚠️ Medium	Hosting websites or web apps
81	hosts2-ns (alternate)	Alternate HTTP or name service.	⚠️ Medium	Often used by device admin panels
443	HTTPS	Secure web traffic over TLS/SSL.	✅ 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/testing servers
8081	blackice-icecap	Used by older intrusion detection or custom services.	⚠️ Medium	Legacy/custom apps
8082	blackice-alerts	Possibly alert ports for intrusion detection systems.	⚠️ Medium	Legacy/custom systems
8443	HTTPS-Alt	Alternate HTTPS port, used by dashboards or control panels.	⚠️ Medium	Admin consoles, dashboards


Port	Service Name	Description	Risk Level	Common Use Cases
10001	SCP-Config	Often used by IoT devices or network equipment config.	High 	May expose vulnerable config interfaces
10002	Documentum	EMC Document Management System.	Medium 	Enterprise document systems
20000	DNP (Distributed NP)	Used in industrial SCADA systems.	High 	Industrial control – must not be exposed
30000	NDMPs	Network Data Management Protocol (backup-related).	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 applications
7999	IRDMI2	Often custom or legacy services.	Medium 	Unknown – requires further investigation
8083	US-SRV	Unknown/custom application port.	Medium 	May require manual analysis


2. Observations & Recommendations

SSH (22) Open on Many Hosts



- Common for remote administration (Linux/Unix systems).
-  **Ensure strong authentication** (e.g., key-based access).
-  **Disable root login** and use fail2ban or similar tools to prevent brute-force attacks.

SMB (445), NetBIOS (139) Detected




- Used for Windows file sharing and printer services.
-  Should be **restricted to internal networks only**.

-  Disable if not needed, especially on servers exposed to the internet.
-



Web Services Found on 8443, 8888, 9090

- May indicate **non-standard admin panels** or **development interfaces**.
 -  Audit each service to identify exposed dashboards or outdated software.
 -  Use HTTPS and strong access controls.
-


RDP (3389) Found Externally

-  Common for Windows remote management.
 -  **High-risk service if exposed externally.**
 -  Use a VPN or gateway jump host instead; enforce MFA.
-

SNMP (161) Exposed

- Used for network device monitoring.
 -  If misconfigured, can leak critical system info.
 -  Change default community strings and restrict access via ACLs.
-

Closed/Filtered Ports

- Good sign: many hosts had filtered or closed ports.
 -  Suggests firewalls or intrusion prevention systems are functioning properly.
-

Suggested Next Steps

Step-by-Step Action Plan

1. **Enumerate services** running on non-standard ports (e.g., 8888, 9090, 8443) with tools like netstat, lsof, or endpoint analysis.
2. **Conduct vulnerability scans** using updated tools (e.g., Nessus, Nmap scripts, OpenVAS) on exposed services.

3. **Secure exposed services** with access controls, strong authentication, and least-privilege configurations.
 4. **Map and document** all services and roles of devices within the network.
 5. **Restrict unused services** through host-based firewalls or perimeter filtering.
 6. **Schedule regular scans** (monthly/quarterly) to catch changes or unauthorized systems.
-

How to Save These Results

You can save your Nmap scan results like this:

```
nmap -sS 10.10.20.0/24 -oN results_scan.txt
```




Or to generate an XML report:

```
nmap -sS 10.10.20.0/24 -oX results_scan.xml
```




Step 7: Identify Potential Security Risks

Potential Security Risks from Open Ports




Port 21 – FTP (File Transfer Protocol)

-  **Risk:** Transmits data and credentials in plaintext; can be intercepted easily.
 -  **Vulnerability:** Susceptible to brute-force attacks, anonymous login misuse, and directory traversal.
 -  **Recommendation:** Disable FTP if not required. Use SFTP or FTPS instead for secure file transfer.
-




Port 23 – Telnet

-  **Risk:** Legacy protocol with **no encryption**, often targeted in brute-force attacks.
-  **Vulnerability:** Allows remote command execution if misconfigured or weak credentials are used.
-  **Recommendation:** Replace with SSH (Port 22). Disable Telnet completely on all modern systems.




Port 3306 – MySQL Database

-  **Risk:** May expose backend databases directly to attackers.
-  **Vulnerability:** Weak or default credentials, SQL injection if connected to web apps.
-  **Recommendation:** Bind MySQL to localhost or internal IPs only. Use firewall rules to restrict access.




Port 5000 – Flask / Dev APIs

-  **Risk:** Common port for development tools and web-based dashboards.
-  **Vulnerability:** Lack of authentication, debug modes enabled, sensitive data exposure.
-  **Recommendation:** Restrict access, enable authentication, and disable debug mode in production.

Port 1433 – Microsoft SQL Server

-  **Risk:** Often scanned and attacked for brute-force or SQL injection vectors.
-  **Vulnerability:** Can allow unauthorized access to critical databases.
-  **Recommendation:** Do not expose externally; use encryption and strong credentials.

Port 49152–65535 – High Random Ports (Ephemeral)

-  **Risk:** Used by various services dynamically (e.g., RPC, VoIP); often overlooked in scans.
-  **Vulnerability:** May expose unknown or unmanaged services.
-  **Recommendation:** Log and monitor traffic, and limit exposure at firewalls. Investigate any persistent services using these ports.


Summary of Key Risks


Port	Risk Level	Description
21	High	Insecure file transfer and credential exposure
23	High	Unencrypted remote shell; vulnerable to brute-force
3306	High	Database exposure and potential SQL injection
5000	Medium	Exposed dev interface; often lacks authentication
1433	High	SQL server exposure; target for brute-force attacks
49152+	Medium	Unmonitored high ports; possible hidden services


General Security Recommendations

1. **Patch regularly** – Keep systems and applications up to date.
2. **Disable unused services** – Reduces attack surface.
3. **Enforce strong authentication** – Especially on admin interfaces.
4. **Use network segmentation** – Keep databases and dev tools away from the internet.
5. **Run routine vulnerability scans** – Tools like Nessus, OpenVAS, or nmap --script help uncover weak points.

Step 8: Save Your Scan Results

-  **To save results as a plain text report, use:**

```
nmap -sV 10.0.0.0/24 -oN network_scan_report.txt
```
-  **To export results in XML format for automation or tools like Nessus, use:**

```
nmap -sV 10.0.0.0/24 -oX network_scan_report.xml
```
-  **To save in grepable format for scripting or filtering:**

```
nmap -sV 10.0.0.0/24 -oG grepable_results.txt
```

✓ Result Saved Confirmation:

✓ Scan completed.

✓ Output saved to: network_scan_report.txt