# Task 1

**Step 1 - Install Nmap**

**Step 2 - Find Ip address by ipconfig**

**Step 3 – Run Scan of Nmap by “Nmap -sS <ip Address>**

**Step 4 – Not down open ports:**

```
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds

7070/tcp open  realserver
```

**Step 5 – Notice Common services running on these port and potential risks**

| Port | Protocol | Service | Description | Security Risk |
|---|---|---|---|---|
| 135 | TCP | MSRPC | Microsoft Remote Procedure Call. Used for DCOM services and Windows services communications. | Exploitable by malware like Blaster worm; should not be exposed to internet. |
| 139 | TCP | NetBIOS-SSN | NetBIOS Session Service. Used for Windows File and Printer Sharing (legacy). | Can leak system info and be exploited for SMB relay attacks. |
| 445 | TCP | Microsoft-DS | SMB over TCP. Used by Windows for file sharing, printer sharing, and Active Directory. | Vulnerable to ransomware (e.g., WannaCry, EternalBlue). |
| 7070 | TCP | RealServer | RealNetworks streaming media server (used by RealPlayer). | Often unused today; old versions may contain unpatched vulnerabilities. |