|  |  |
| --- | --- |
| Roll No | 22SW040 |
| Name | Farooque Sajjad |
| Subject | IS |
| Assignment | 5 marks |

## ****What is Nmap?****

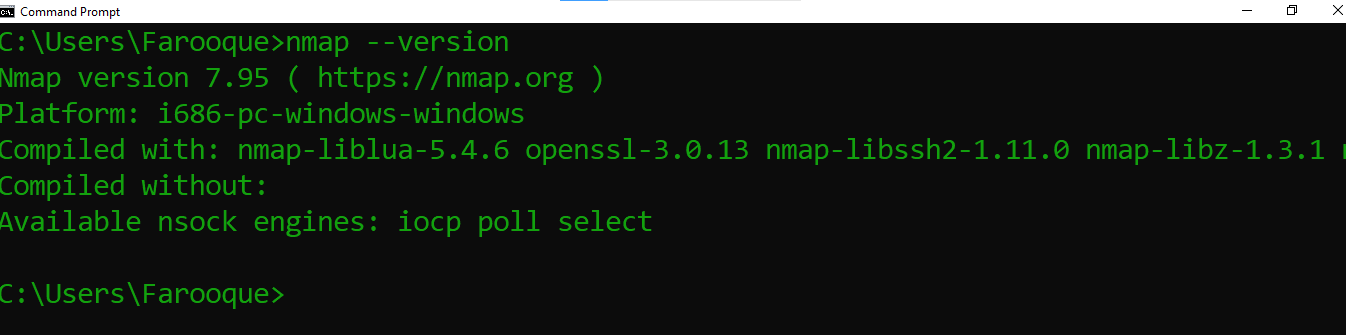
Nmap (Network Mapper) is a **powerful network scanning tool** used for:

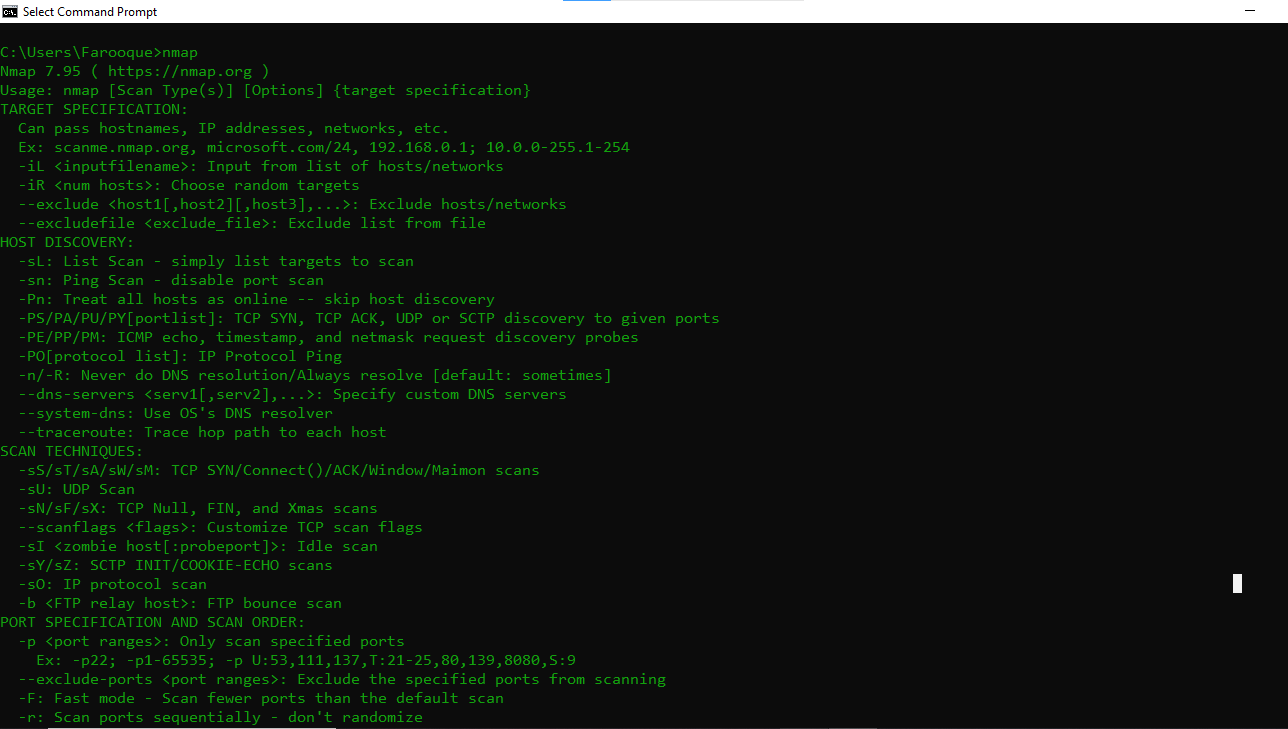
* **Finding live hosts** on a network
* **Identifying open ports and services**
* **Detecting operating systems and vulnerabilities**

### ****Step 1: Open Nmap in Windows/Linux****

After installing Nmap on Windows:

1. Open **Command Prompt** or **PowerShell**.
2. Type nmap to make sure it’s installed correctly.  
   You’ll see a list of available Nmap options.





### ****Step 2: Basic Nmap Commands****

Here are some **essential commands** to get started:

#### 1 ****Ping Scan (Find Live Hosts)****

nmap -sn 192.168.100.0/24

**What it does**: Scans a network to find all live devices.  
A screenshot of a computer program

Description automatically generated

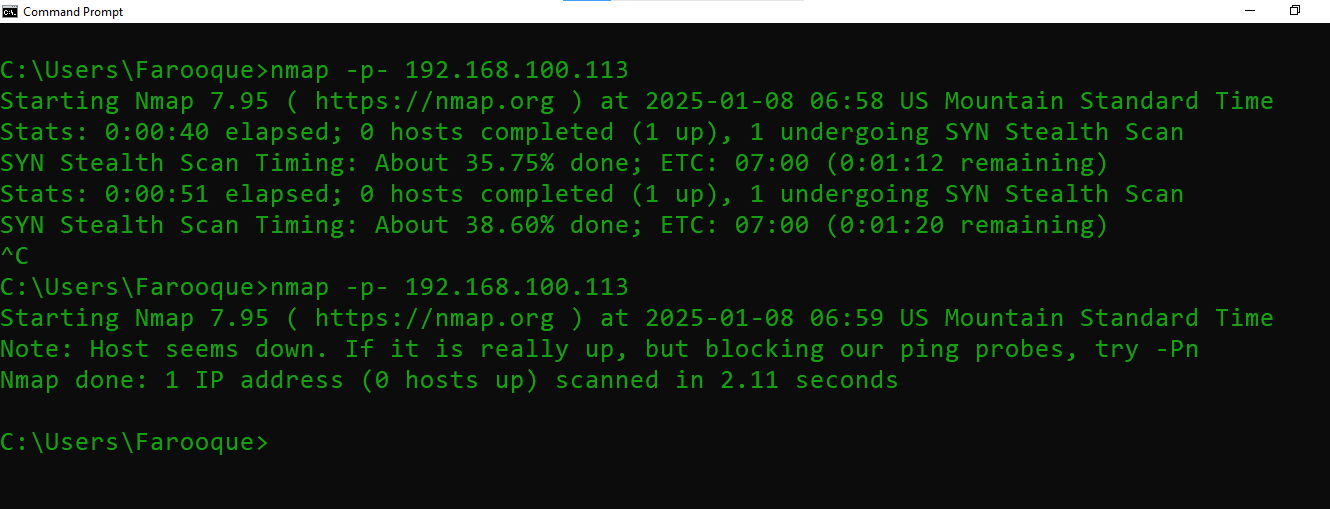
#### 2) ****Port Scan (Find Open Ports)****

nmap -p 80,443 192.168.1.1

**What it does**: Scans the **HTTP (80)** and **HTTPS (443)** ports on the target IP.

To scan **all ports** on a machine:

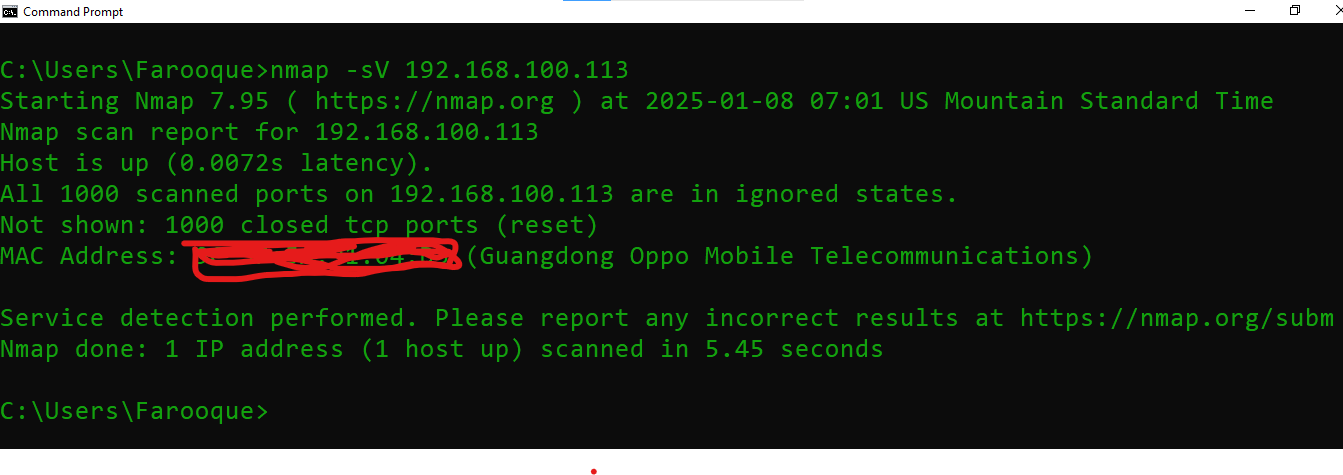
nmap -p- 192.168.100.113



#### 3) ****Service Detection****

nmap -sV 192.168.100.113

🔎 **What it does**: Detects what services are running on the target and their versions.



#### 4) ****Operating System Detection****

nmap -O 192.168.100.113

🔎 **What it does**: Tries to determine the operating system running on the target machine.

A screenshot of a computer screen

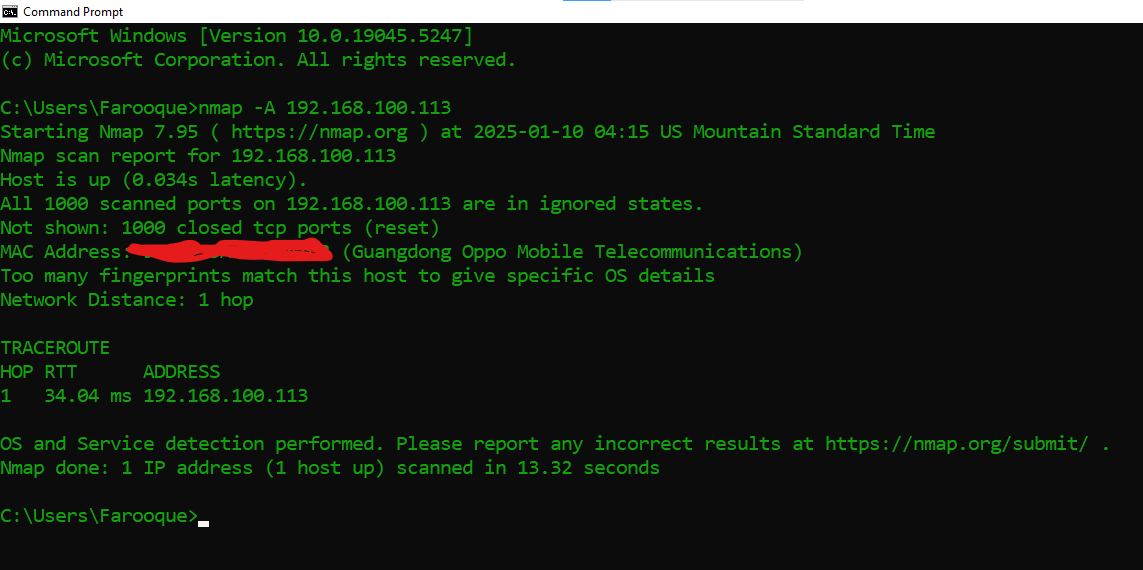
Description automatically generated

#### 5️⃣ ****Aggressive Scan (All-in-One)****

nmap -A 192.168.100.113

🔎 **What it does**: Performs a detailed scan including:

* OS detection
* Service detection
* Traceroute
* Script scanning



### 🔧 ****Step 3: Practice on a Test Server****

Nmap has its **own test server** that you can scan without getting into trouble:

nmap scanme.nmap.org

A screenshot of a computer program

Description automatically generated

### 📚 ****Step 4: Practice Common Use Cases****

Here are some practical Nmap commands for real-world scenarios:

| **Scenario** | **Command** |
| --- | --- |
| Scan a single IP | nmap 192.168.100.113 |
| Scan a range of IPs | nmap 192.168.100.1-100 |
| Scan a subnet | nmap 192.168.100.0/24 |
| Scan for open ports | nmap -p 1-65535 192.168.100.113 |
| Detect firewall rules | nmap -sA 192.168.100.113 |
| Detect vulnerabilities | nmap --script vuln 192.168.100.113 |

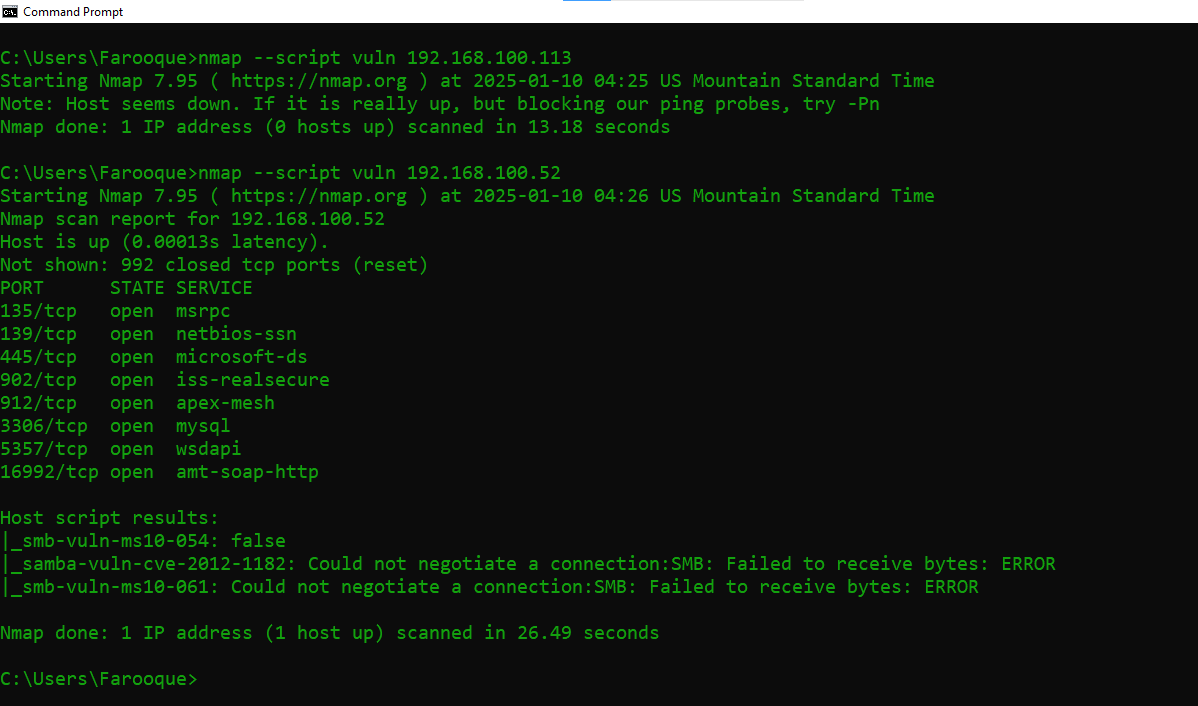
### 💡 ****Step 5: Using Nmap Scripts (NSE)****

Nmap has a powerful **scripting engine (NSE)** that can detect vulnerabilities:

#### Run a vulnerability scan:

nmap --script vuln 192.168.100.113

nmap --script vuln 192.168.100.52(this pc)



#### Run an HTTP enumeration script:

nmap --script http-enum 192.168.100.113

nmap –script http-enum 192.168.100.52

