Assignment 01 Title**: Identify Open Ports and Services on a Localhost Using Nmap** Name: Suvhankar Dutta Date: 11th July 2025

✅ Tools Used: Nmap: Network Mapper (pre-installed in Kali Linux)

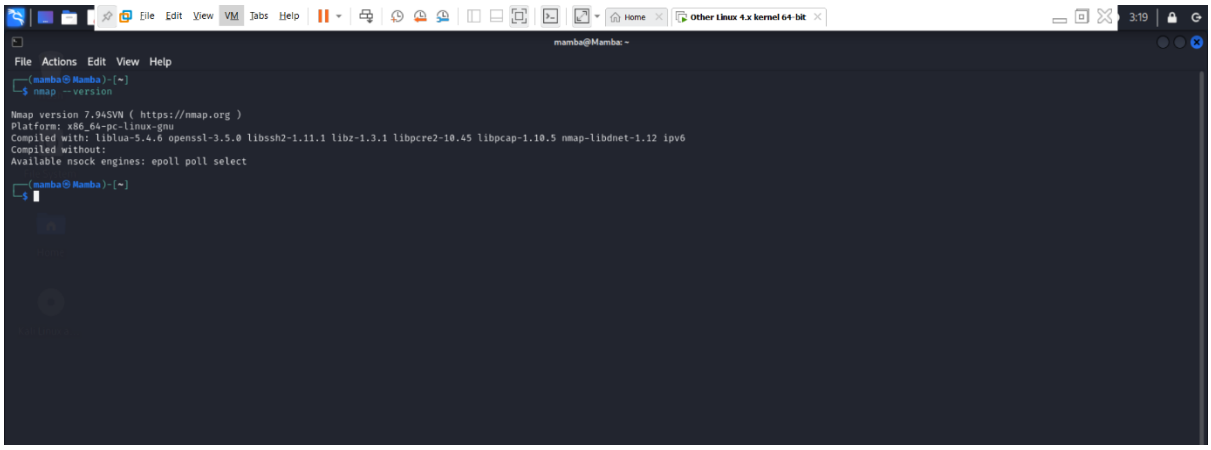
Text Editor: LibreOffice Writer / nano / gedit

🔹 **Step 1: Install Nmap**

Installation Status:
Nmap comes pre-installed in Kali Linux. To confirm, I ran:

```
nmap -version
```

output:



Step 2: Perform a Basic Port Scan.

Command used: `nmap 127.0.0.1`

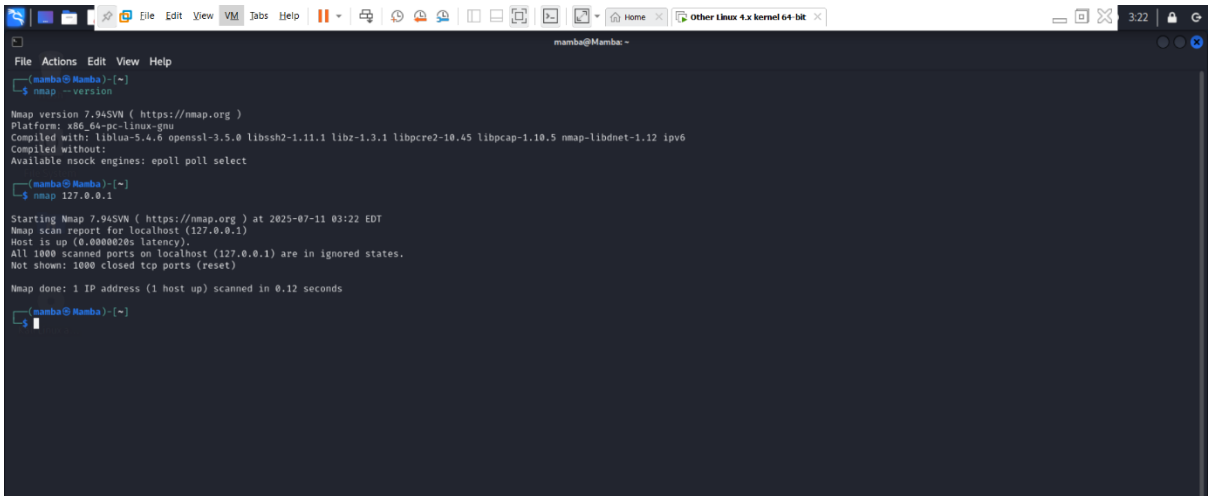
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.

Not shown: 1000 closed ports

Summary :

- The Nmap basic scan on 127.0.0.1 showed no open ports.
- All 1000 commonly scanned ports are currently closed or not listening for incoming connections.
- This is typical if no services (e.g., SSH, web server, database) are running or exposed on your Kali machine.
- It indicates a secure state for localhost with no unnecessary open ports.

output:



Step 3: Service Version Scan.

Command used : `nmap -sV 127.0.0.1`

Summary:

All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.

Not shown: 1000 closed tcp ports (reset) .

The service version scan also found no open ports.

Since all ports are closed, Nmap was unable to detect any services or versions running on the system.

This again shows that the system is not currently running any listening network services on the standard 1000 ports.

Why this happens since I am a cybersecurity undergraduate student I can explain?

This is typical if services like Apache, SSH, MySQL, etc., are not running.

On Kali Linux, many services are not started by default to minimize attack surface.

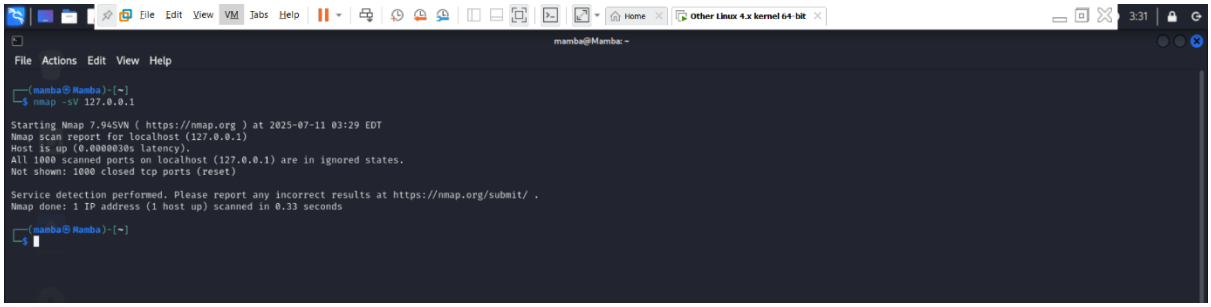
Normally Detected Services (If Open): If ports were open, Nmap would show details like:

22/tcp open ssh OpenSSH 9.2p1

80/tcp open http Apache 2.4.x

3306/tcp open mysql MySQL 8.x

Output:



Step 4. Perform a Stealth SYN Scan

Command: `sudo nmap -sS 127.0.0.1`

Summary:

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

What is a Stealth Scan?

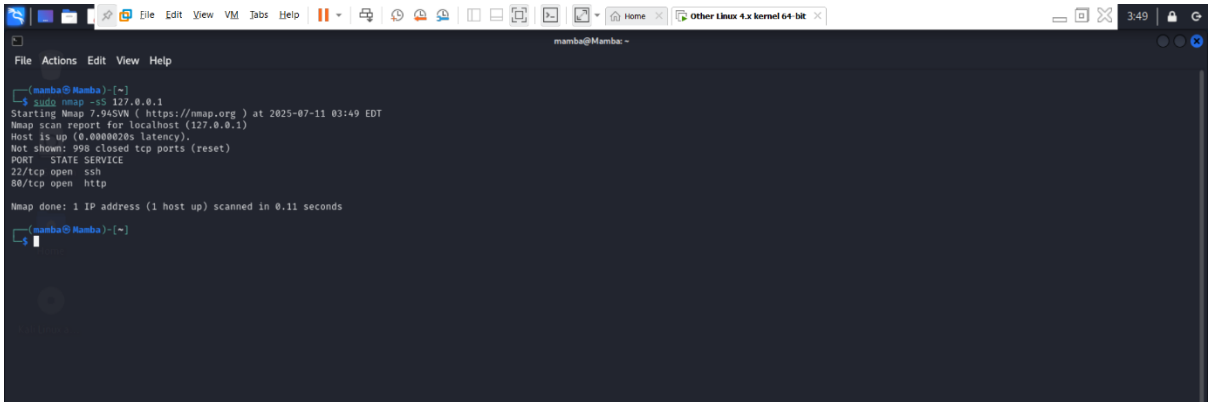
- A stealth SYN scan (also known as a half-open scan) sends only the SYN packet — the first part of the TCP handshake — and waits for a SYN-ACK response.
- It does not complete the connection, making it less likely to be detected by firewalls and intrusion detection systems (IDS).
- It's faster and stealthier than a full TCP connect scan.
- **Comparison with Basic Scan:**

Scan Type	Result Summary
Basic Scan	No open ports found initially (before services started)
Stealth Scan	Detected 2 open ports: **22 (ssh)** and **80 (http)**
Key Difference	Stealth scan detected running services after services were manually started

Port 22 (ssh): OpenSSH server is running, allowing secure terminal access.

Port 80 (http): Python HTTP server is running, serving content over HTTP.

Output:



Explaination:

Initially, all ports on localhost were closed during earlier scans. To simulate a more realistic scan and observe open services, I manually started the following services using:

Command 1: `sudo systemctl start ssh`

Command 2: `sudo python3 -m http.server 80`

This activated:

- **SSH** service on port **22**
- **HTTP** server on port **80**

Once the services were running, I performed a **stealth SYN scan** using the -sS option in Nmap.

What I Learned from This Exercise

- How to use Nmap effectively for different types of port and service scanning.
- The security importance of closed/filtered ports by default.
- Realized the difference between basic scans and stealth scans.
- Learned how to simulate real-world scenarios by manually starting services.
- Understood the power of Nmap in network enumeration and security assessments.