**Cybersecurity Project Report**

# Project Title: Localhost Port Scan Using Nmap

## Objective:

The primary goal of this project was to initiate the reconnaissance phase of ethical hacking by scanning the local system (localhost) using the powerful network exploration tool Nmap. The objective was to gain a deeper understanding of open ports, running services, and how attackers or penetration testers can gather valuable information about a target system.

## Tools & Technologies:

**1.Platform:** Windows 10

**2. Nmap (Network Mapper)**

**Purpose:**  
A powerful command-line tool used for network discovery, port scanning, and service enumeration. It's used by security professionals during the reconnaissance phase.

**Common Uses:**

* Find open ports (e.g., 80 for HTTP, 22 for SSH)
* Detect running services (e.g., Apache, MySQL)
* Identify service versions and OS types
* Discover all devices on a network

**Example Commands:**

* nmap 127.0.0.1 → basic scan
* nmap -sV 127.0.0.1 → scan with service version detection
* nmap -A 192.168.1.1 → aggressive scan with OS and script detection

**3. Command Prompt (Windows Terminal)**

**Purpose:**  
Used to run command-line tools like Nmap on Windows. This gives you control over scanning, scripting, and managing systems without a GUI.

**Why it’s important in cybersecurity:**

* Allows automation and scripting
* Direct access to tools without distractions
* Great for system analysis, quick tasks, and testing

**4. Localhost (127.0.0.1)**

**Purpose:**  
A loopback IP address that always points to your own system.

**Why it’s used:**

* Safe to practice on
* Helps test tools and scans without affecting others
* Useful for learning ethical hacking without needing a target machine

**5. IP Address/Subnet (e.g., 192.168.1.0/24)**

**Purpose:**  
Defines a local network range. For example:

* 192.168.1.1 → your router
* /24 → means 256 possible devices (192.168.1.0 to 192.168.1.255)

**Why it’s used in scanning:**

* You can discover all devices connected to your home Wi-Fi or LAN
* Helps practice network-wide reconnaissance

**6. -sV Flag (Nmap Command)**

**Purpose:**  
This flag tells Nmap to attempt service version detection on open ports.

**Output:**

22/tcp open ssh OpenSSH 7.9

80/tcp open http Apache httpd 2.4.29

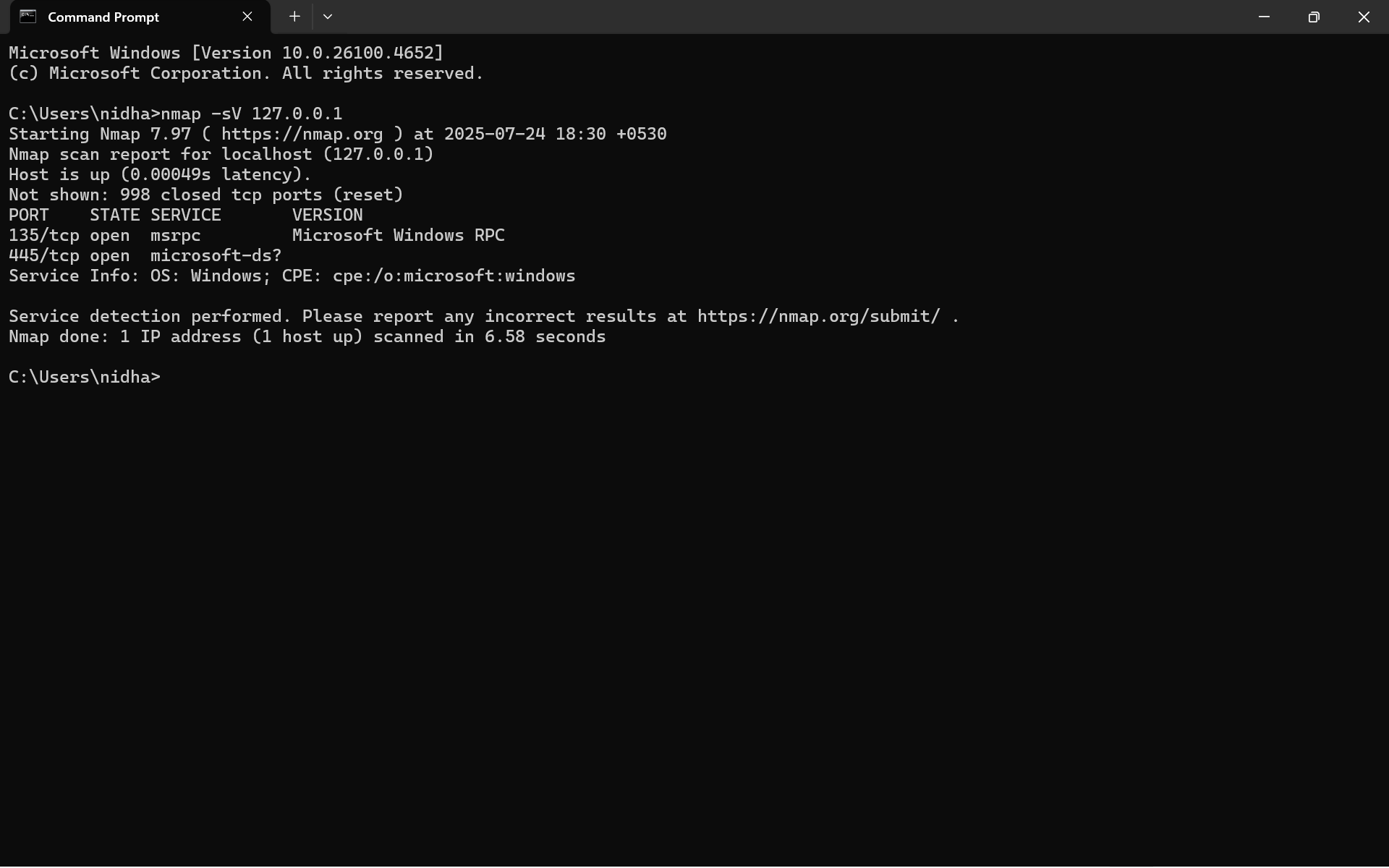
**Why it's important:**

* Knowing the version helps identify if a service is outdated or vulnerable
* Used in vulnerability assessments

**What I Did:**

1. Installed Nmap 7.97 on a Windows 10 machine ensuring the executable path was set correctly.  
2. Opened Command Prompt and ran a scan against the loopback IP (127.0.0.1) using the -sV flag.  
3. Interpreted the scan results to identify which ports were open and what services were active.  
4. Analyzed service versions and considered the implications of exposing certain services.  
5. Documented all findings, understood potential entry points, and the importance of securing unnecessary ports.

## Output:



**Key Learning:**

* Understood how reconnaissance forms the foundation of ethical hacking and penetration testing.
* Learned to use Nmap effectively to discover running services and open ports.
* Realized the significance of minimizing open ports and keeping services up-to-date to reduce security risk.
* Gained confidence in using command-line tools and analyzing network responses.
* Recognized the real-world relevance of tools like Nmap in red team and blue team operations.

## Understanding Reconnaissance:

Reconnaissance is the first step in the cybersecurity kill chain. It involves gathering information about a target system or network, either passively (without direct interaction) or actively (directly probing the system). In this project, an active reconnaissance technique was used. Understanding the reconnaissance phase helps defenders think like attackers and patch vulnerabilities before they can be exploited.

**Conclusion:**

This project marked my first hands-on experience in the reconnaissance phase of ethical hacking using Nmap. I successfully scanned my own system (localhost) to identify open ports and active services, gaining practical insight into how attackers and security professionals gather intelligence. This foundational exercise improved my understanding of network scanning, tool usage, and system exposure — laying the groundwork for more advanced cybersecurity exploration