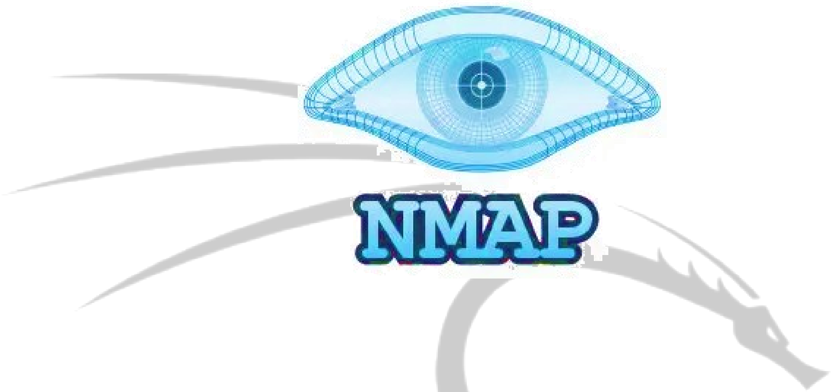
Network Scanner Using



A Project Report

Submitted By

Mano Shruthi S

TABLE OF CONTENTS

1.Abstract

Network scanning is a fundamental technique in the field of **cybersecurity** and network administration, enabling the identification of active hosts, open ports, running services, and potential security vulnerabilities within a network. This project focuses on the practical use of **Nmap (Network Mapper)**, a widely recognized and powerful open-source tool to perform different scanning techniques in a controlled and safe environment. The objective is to provide hands-on experience with essential scanning methods, understand their outputs, and develop the ability to interpret network information effectively.

The work was carried out on a **Kali Linux** virtual machine running on the researcher's personal laptop, with Nmap as the sole scanning tool. Four primary scanning techniques were implemented:

1. **Basic Scan** – to identify open ports on the target system and determine their availability.
2. **Version Detection Scan** – to identify specific versions of services running on open ports.
3. **Operating System (OS) Detection Scan** – to estimate the target machine's operating system using Nmap's OS fingerprinting capabilities.
4. **Aggressive Scan** – to combine OS detection, version detection, script scanning, and traceroute for comprehensive network analysis.

Each scan was executed against the local machine's IP address, ensuring an ethical and controlled testing environment without affecting external systems. Screenshots of the terminal outputs were recorded for each scan to document the process and results. The findings provide valuable insight into the structure of the network, the types of services exposed, and the importance of securing open ports against unauthorized access.

This project demonstrates the significance of network scanning as both a defensive and educational practice. By understanding the details revealed through Nmap, network administrators and security students can take proactive measures to mitigate risks. The detailed procedures, outputs, and interpretations presented in this work ensure that the reader can replicate the process with confidence and gain a practical understanding of network reconnaissance techniques.

2.Objective

- **To develop practical skills in network scanning** by using the open-source tool **Nmap** for detecting and analyzing network services, ports, and system characteristics.
- **To identify active hosts in the network** and determine which devices are reachable and responding to scan requests.
- **To detect open ports** and classify them based on their accessibility, which is crucial for understanding possible entry points into a system.
- **To analyze running services on open ports**, including service names and their version numbers, in order to assess potential vulnerabilities.
- **To perform Operating System (OS) detection** using Nmap’s OS fingerprinting capabilities to estimate the target system’s platform and architecture.
- **To carry out Aggressive Scans** that combine multiple scanning features — such as OS detection, version detection, script scanning, and traceroute — for comprehensive system profiling.
- **To ensure an ethical and safe scanning environment** by targeting only the local machine’s IP address within a Kali Linux virtual machine, thereby preventing any real-world security breaches.
- **To document the entire process in detail** with clear steps, executed commands, and captured screenshots so that the procedure can be easily understood and replicated by others.
- **To highlight the significance of proactive network scanning** as a preventive security measure that helps administrators and learners detect and close potential security gaps before they can be exploited.
- **To enhance understanding of cybersecurity concepts** by linking theoretical knowledge of scanning techniques with real-world practical execution.

.

3.Tools Used

This section describes the software and hardware tools used to complete the network scanning project. Each tool plays an important role in setting up the environment, performing the scans, and analyzing the network.

3.1 Oracle VirtualBox

Oracle VirtualBox is free virtualization software that lets you run multiple operating systems on one computer. It was used to install and run Kali Linux in a virtual machine, isolating the scanning environment from the host system.
Download link: https://www.virtualbox.org/wiki/Downloads

3.2 Kali Linux

Kali Linux is a specialized Linux distribution for penetration testing and network security. It includes many security tools like Nmap. Kali was installed inside VirtualBox to provide a secure platform for scanning.
Download link: https://www.kali.org/get-kali/

3.3 Nmap (Network Mapper)

Nmap is an open-source network scanner that detects hosts, open ports, services, and operating systems. It was the main tool used for scanning, and comes pre-installed on Kali Linux.
Official website: https://nmap.org/

3.4 Windows Command Prompt (cmd)

The Windows Command Prompt is a command-line tool used here to find the host PC's IP address with the `ipconfig` command. This IP address was used as the scan target..

Typical command used: ipconfig

This command displays the network configuration details, including the IPv4 address needed for Nmap scans.

3.5 Host Computer

The physical machine running VirtualBox and Kali Linux, providing CPU, RAM, and network access needed for the virtual environment

4.Introduction

In today’s world, computers and devices are connected to each other through networks. These networks allow us to share information, communicate, and use many services like websites, emails, and online apps. But as networks grow bigger, they also become targets for cyber attacks. Hackers can try to access these networks to steal information or cause damage. That is why it is very important to keep networks safe and secure.

One way to improve network security is through **network scanning**. Network scanning is the process of checking a network to find out which devices are connected and active. It also helps to discover which communication points, called ports, are open and what services are running on those ports. This information is very useful for network administrators because it helps them understand how the network works and identify any weak spots that hackers might use to enter the system.

In this project, we used a powerful tool called **Nmap** (Network Mapper). Nmap is a free and open-source software widely used by security professionals and network administrators. It can scan a network and provide details about devices, open ports, running services, and even the operating system of the devices. Using Nmap, we can perform different types of scans like basic scans to find open ports, scans to detect service versions, scans to find out the operating system, and aggressive scans that combine many techniques for detailed information.

To make sure everything was done safely and legally, all scanning was done only on the local machine inside a virtual environment called **Kali Linux**, running on VirtualBox. This setup ensures no harm to other computers or networks.

This project is a great way for beginners to get hands-on experience with network scanning. It teaches how to use Nmap, understand its results, and realize the importance of regularly scanning networks to protect them from security threats.

5.Theory

Network scanning helps find active devices, open ports, running services, and operating systems on a network. The tool used in this project, **Nmap**, provides different scanning options to gather this information.

Here are the main scan types used, along with their purposes and example commands:

5.1 Basic Scan

- **Purpose:** To find open ports on the target machine. Ports are communication endpoints; open ports indicate available services.
- **Command:** nmap <target-ip>
- **Example:** nmap 192.168.1.10
  This command scans the target IP and lists the open ports and basic information.

5.2 Version Detection Scan

- **Purpose:** To identify the specific software and version running on each open port. This helps assess security risks related to outdated or vulnerable software.
- **Command:** nmap -sV <target-ip>
- **Example:** nmap -sV 192.168.1.10
  This command scans open ports and attempts to detect service versions.

5.3 Operating System (OS) Detection Scan

- **Purpose:** To estimate the target machine's operating system using Nmap's OS fingerprinting technique.
- **Command:** sudo nmap -O <target-ip>
- **Example:** sudo nmap -O 192.168.1.10
  This command tries to determine the OS of the target device.

5.4 Aggressive Scan

- **Purpose:** Combines OS detection, version detection, script scanning, and traceroute for a detailed analysis.
- **Command:** sudo nmap -A <target-ip>
- **Example:** sudo nmap -A 192.168.1.10
  This command runs a comprehensive scan that provides extensive information about the target.

Note: Replace <target-ip> with the actual IP address of the machine you want to scan. In this project, scans were run against the local machine IP obtained via the Windows Command Prompt.

6. Step-by-Step Procedure

This section describes how to perform network scanning using Nmap on Kali Linux running inside Oracle VirtualBox. Each step is supported by screenshots to clearly show the process.

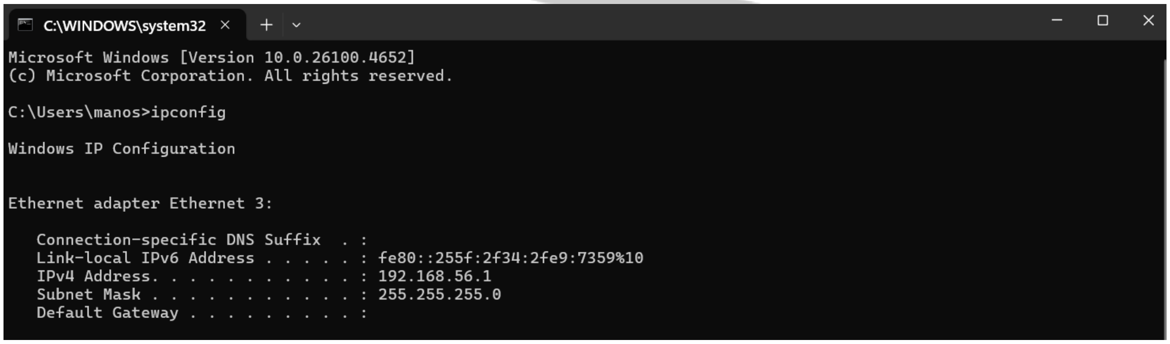
Step 1: Install Oracle VirtualBox and Kali Linux

- Download and install Oracle VirtualBox from https://www.virtualbox.org/wiki/Downloads.
- Download Kali Linux ISO from https://www.kali.org/get-kali/ and install it as a virtual machine in VirtualBox.

Step 2: Find Host IP Address on Windows

- Open Windows Command Prompt by pressing `Windows + R`, type `cmd`, and press Enter.
- Run `ipconfig` to display network details.
- Note the **IPv4 Address** of your active network adapter (e.g., 192.168.1.10).

Screenshot:



```
Microsoft Windows [Version 10.0.26100.4652]
(c) Microsoft Corporation. All rights reserved.

C:\Users\manos>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::255f:2f34:2fe9:7359%10
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

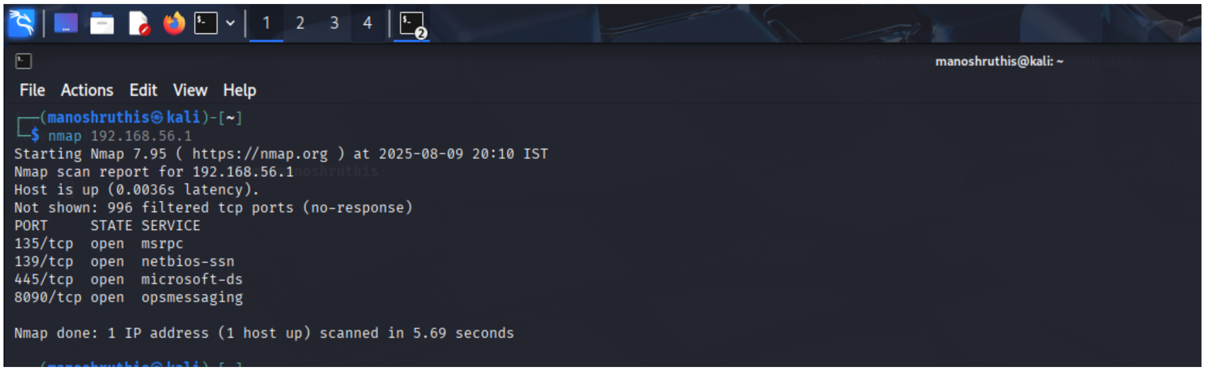
Step 3: Open Terminal in Kali Linux

- Start the Kali Linux VM and open the Terminal application.

Step 4: Run Basic Scan

- In Terminal, enter `nmap <target-ip>` (replace `<target-ip>` with your IP).
- This scans for open ports.

Screenshot:

- 

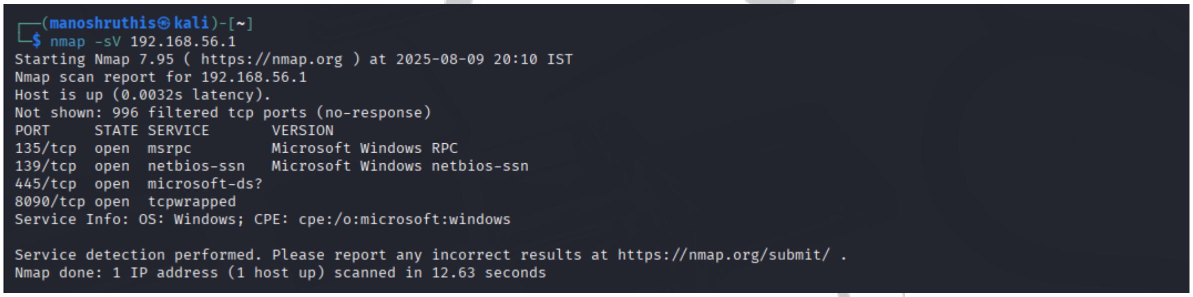
```
┌──(manoshruthis㉿kali)-[~]
└─$ nmap 192.168.56.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 20:10 IST
Nmap scan report for 192.168.56.1
Host is up (0.0036s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8090/tcp open  opsmessaging

Nmap done: 1 IP address (1 host up) scanned in 5.69 seconds
```

Step 5: Run Version Detection Scan

- Enter `nmap -sV <target-ip>` in Terminal.
- This reveals software and version info for open ports.

Screenshot:



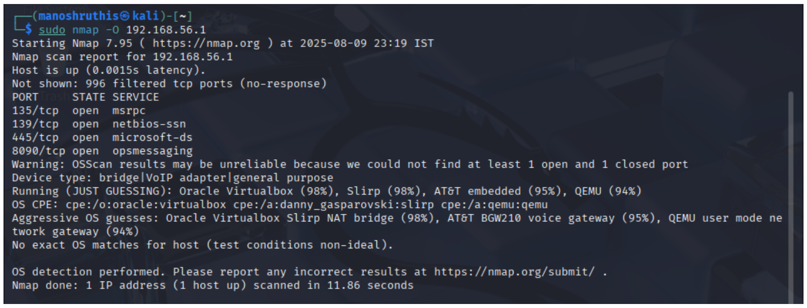
```
┌──(manoshruthis㉿kali)-[~]
└─$ nmap -sV 192.168.56.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 20:10 IST
Nmap scan report for 192.168.56.1
Host is up (0.0032s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
8090/tcp open  tcpwrapped
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.63 seconds
```

Step 6: Run OS Detection Scan

- Enter `sudo nmap -O <target-ip>`.
- This tries to identify the target's operating system.

Screenshot:



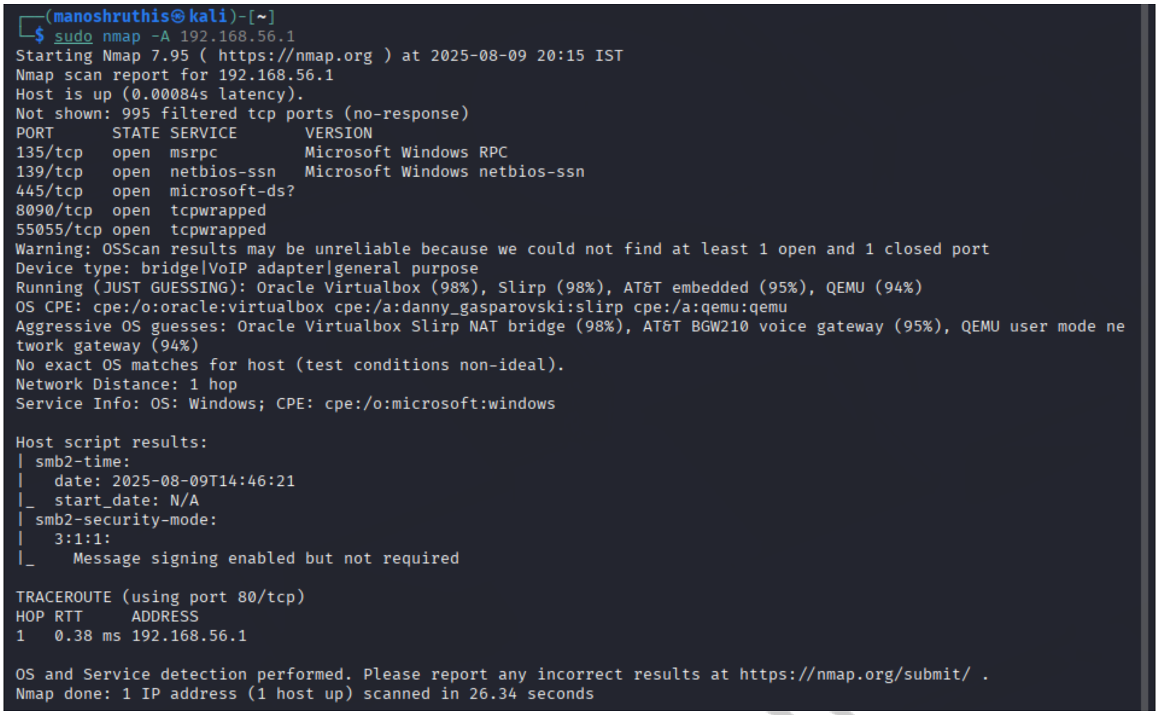
```
┌──(manoshruthis㉿kali)-[~]
└─$ sudo nmap -O 192.168.56.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 23:19 IST
Nmap scan report for 192.168.56.1
Host is up (0.0015s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8090/tcp open  opsmessaging
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode ne
twork gateway (94%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.86 seconds
```

Step 7: Run Aggressive Scan

- Enter `sudo nmap -A <target-ip>`.
- This comprehensive scan shows detailed information including traceroute and scripts.

Screenshot:



```
┌──(manoshruthis㉿kali)-[~]
└─$ sudo nmap -A 192.168.56.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 20:15 IST
Nmap scan report for 192.168.56.1
Host is up (0.00084s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
8090/tcp  open  tcpwrapped
55055/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode ne
twork gateway (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-08-09T14:46:21
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.38 ms 192.168.56.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.34 seconds
```

6. Analysis

The network scans performed using Nmap provided valuable insights into the target machine's network configuration and security status.

Open Ports:
The basic scan revealed several open ports on the target system. Open ports indicate services that are actively listening for network connections. While some ports are necessary for normal operation (such as ports for web servers or file sharing), each open port can potentially be an entry point for attackers if not properly secured.

Service Versions:
Version detection helped identify the specific software and their versions running on the open ports. This information is important because outdated or vulnerable software versions can be exploited by attackers. Regularly updating services can reduce security risks.

Operating System Detection:
The OS detection scan estimated the target machine's operating system accurately. Knowing the OS helps in understanding which vulnerabilities may apply and what security measures are appropriate.

Aggressive Scan Findings:
The aggressive scan combined several techniques to provide a detailed view of the network. It also included script scanning and traceroute information, which help map network paths and identify additional security details. This comprehensive approach aids in thorough network assessment.

Security Implications:

- Open ports should be minimized and monitored to reduce attack surfaces.
- Services should be updated and patched regularly.
- Network administrators should use scanning tools like Nmap routinely to detect unexpected changes or vulnerabilities.
- Ethical and authorized scanning ensures security testing does not harm other systems or violate privacy.

Overall, the scans demonstrated the importance of network reconnaissance in cybersecurity. Understanding what devices and services are exposed allows for proactive defense and better network management.

7.Conclusion

This project showed how Nmap can be used as a powerful tool to scan networks. We used it to find open ports, running services, and the operating system of a target computer in a safe, controlled setup.

We tried different types of scans—basic scans, version checks, OS detection, and aggressive scans—to get a full picture of the target's network details.

Running these scans on a Kali Linux virtual machine made sure the process was safe and ethical. The results showed possible security problems like open ports and old services that hackers could use if not fixed.

From this, we learned that regular network scanning is important for finding and fixing weaknesses early. Network administrators can use these methods to protect their systems.

In short, learning to scan networks with tools like Nmap helps students and professionals build important skills to understand and secure computer networks.