

Network Reconnaissance and Port Scanning Using Nmap

By:-Prerna Bhashani

Introduction

What is cyber Reconnaissance ?

Cyber reconnaissance is the initial phase of ethical hacking and security assessment. It involves gathering information about a target system or network to identify potential security weaknesses.

During reconnaissance, a security analyst attempts to:

- .Identify active hosts on the network
- .Discover open ports
- .Detect running services
- .Identify operating systems
- .Understand network structure

Reconnaissance helps organizations understand their exposure to cyber threats.

About Nmap

Nmap (Network Mapper) is an open-source network scanning tool widely used for:

- ▶ Network discovery
- ▶ Security auditing
- ▶ Port scanning
- ▶ Service and version detection
- ▶ Operating system detection

It allows security professionals to analyze network vulnerabilities efficiently.

Project Objectives

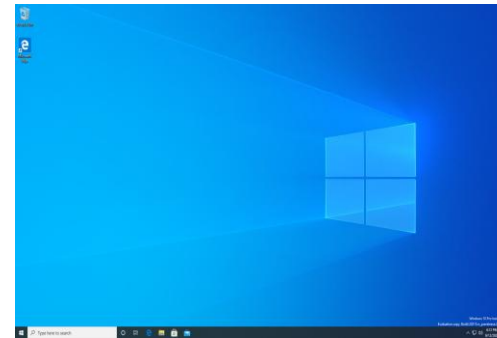
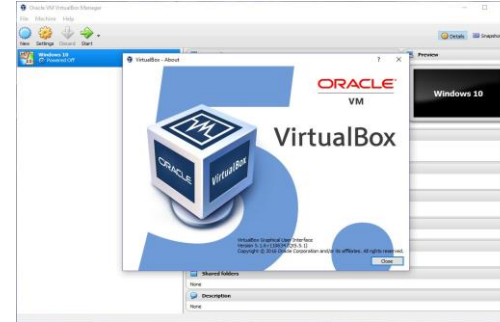
The main objectives of this project are:

- ▶ To identify active hosts in a network
- ▶ To perform port scanning using Nmap
- ▶ To detect services running on open ports
- ▶ To analyze security risks associated with open ports
- ▶ To recommend prevention strategies

Tools and Environment Setup

Tools used

- ▶ VirtualBox (Virtualization Software)
- ▶ Kali Linux (Attacker Machine)
- ▶ Target Machine (Windows 10)
- ▶ Nmap Tool (Pre-installed in Kali Linux)



Virtual lab setup

Step 1: Install VirtualBox

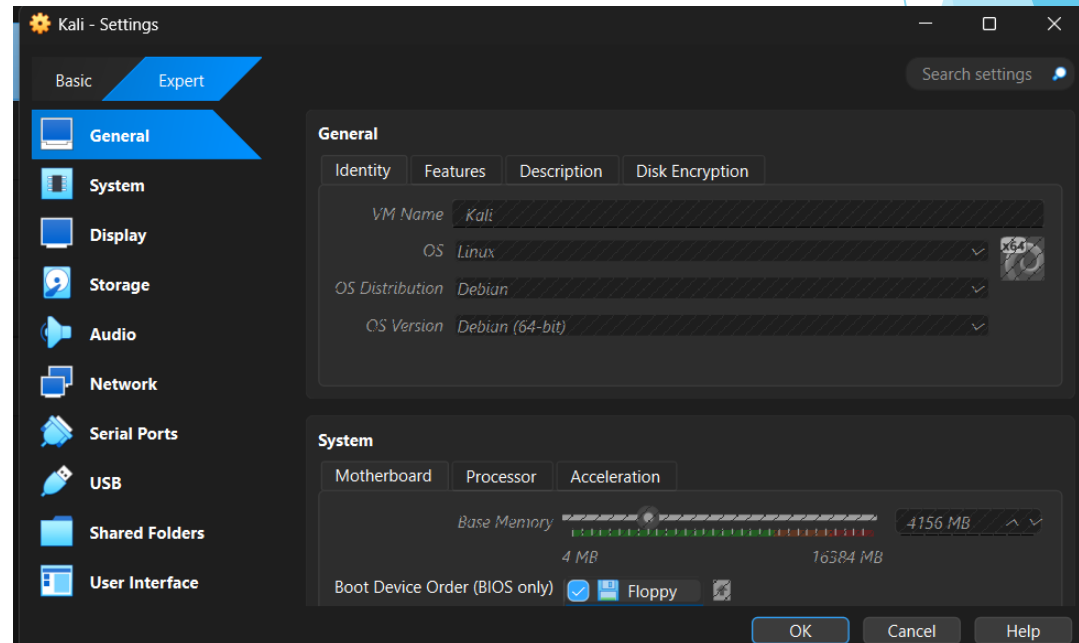
Download Oracle VirtualBox from the official website

Install the software using default installation settings

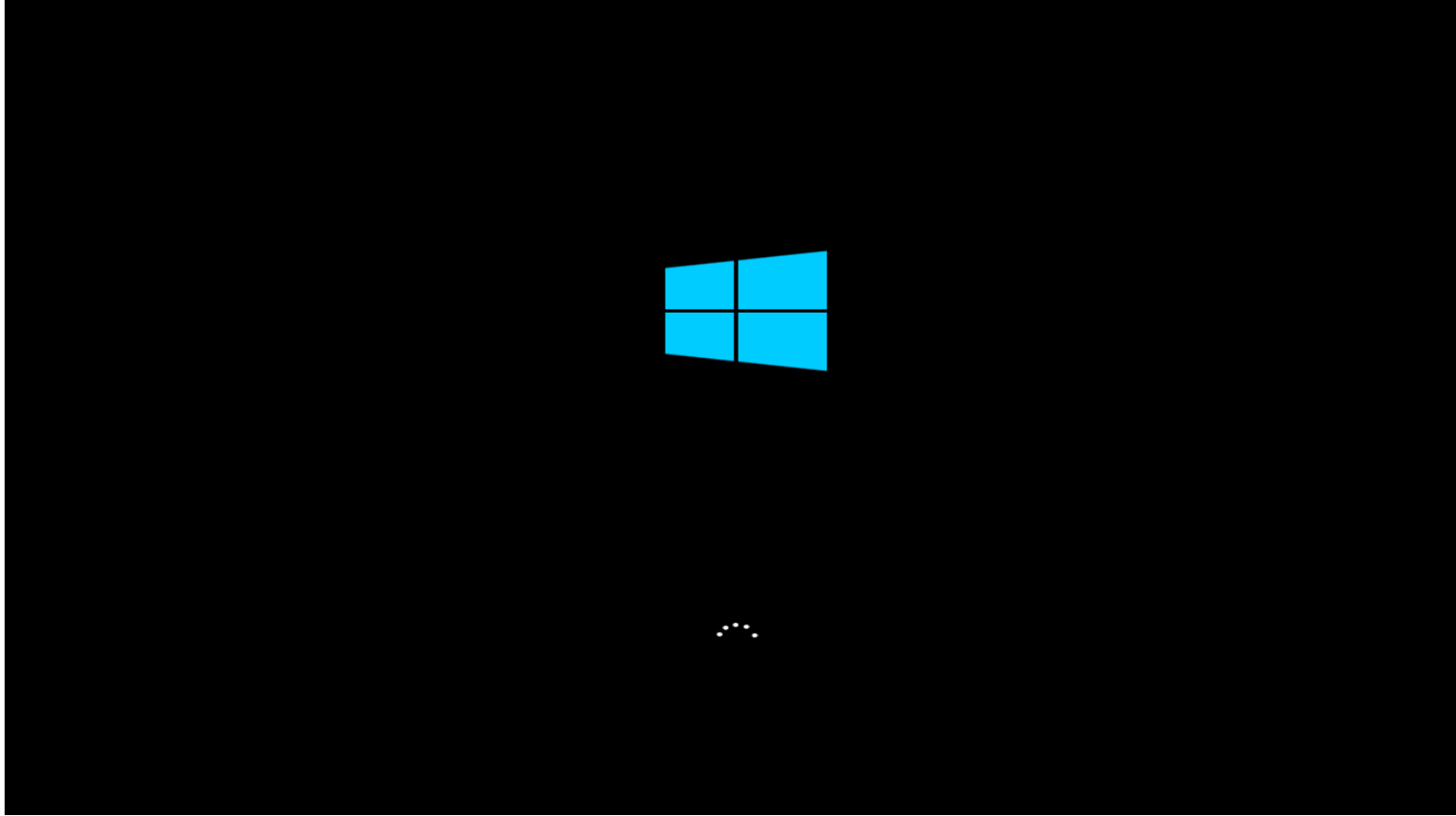
Launch VirtualBox after installation

Step 2: Kali Linux Installation

- ▶ Download Kali Linux ISO file
- ▶ Open VirtualBox
- ▶ Click New Virtual Machine
- ▶ Set the following configuration:
 - RAM: Minimum 2GB
 - Storage: Minimum 20GB
- ▶ Attach Kali Linux ISO and start installation
- ▶ Complete installation using default settings

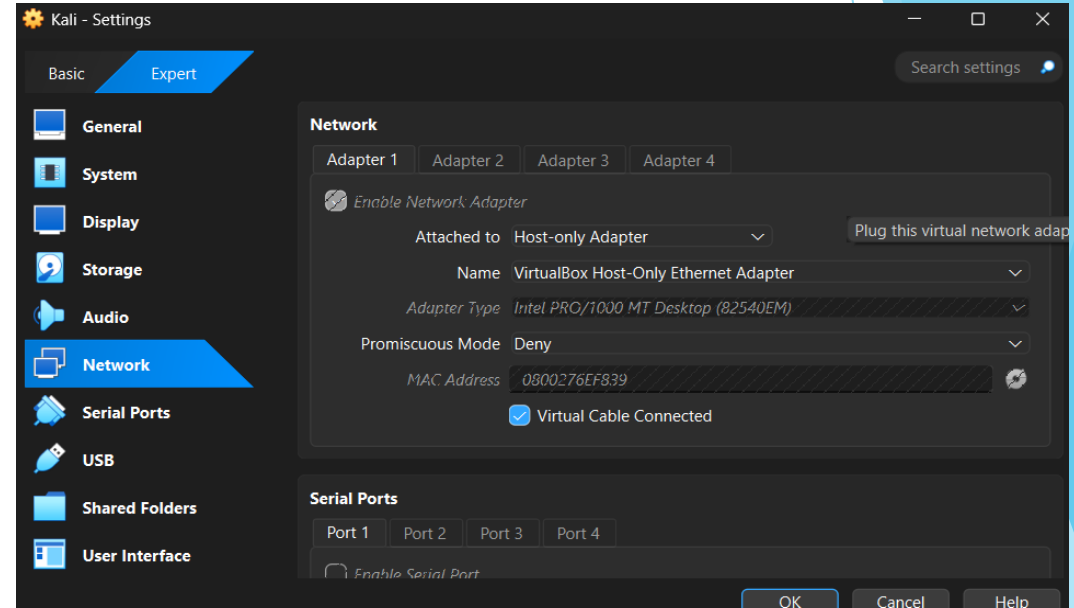
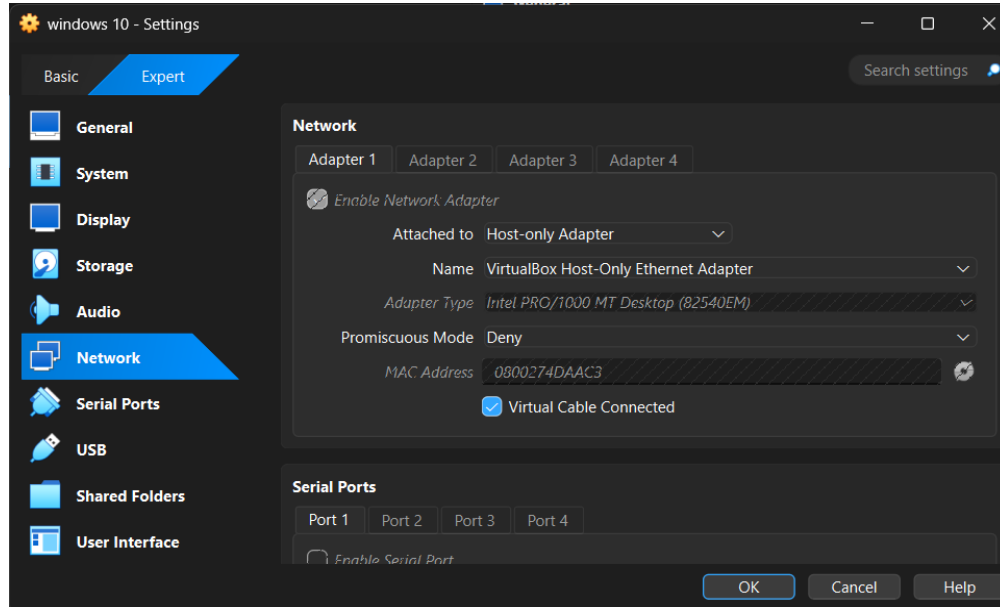


Target Machine:-



- ▶ Windows 10
- ▶ Install and configure the target machine inside VirtualBox.

Step 4: Network Configuration



- ▶ To allow communication between attacker and target machine:
- ▶ Open VirtualBox settings
- ▶ Select Network Adapter
- ▶ Choose Host-Only Adapter
- ▶ Apply same network configuration for both machines

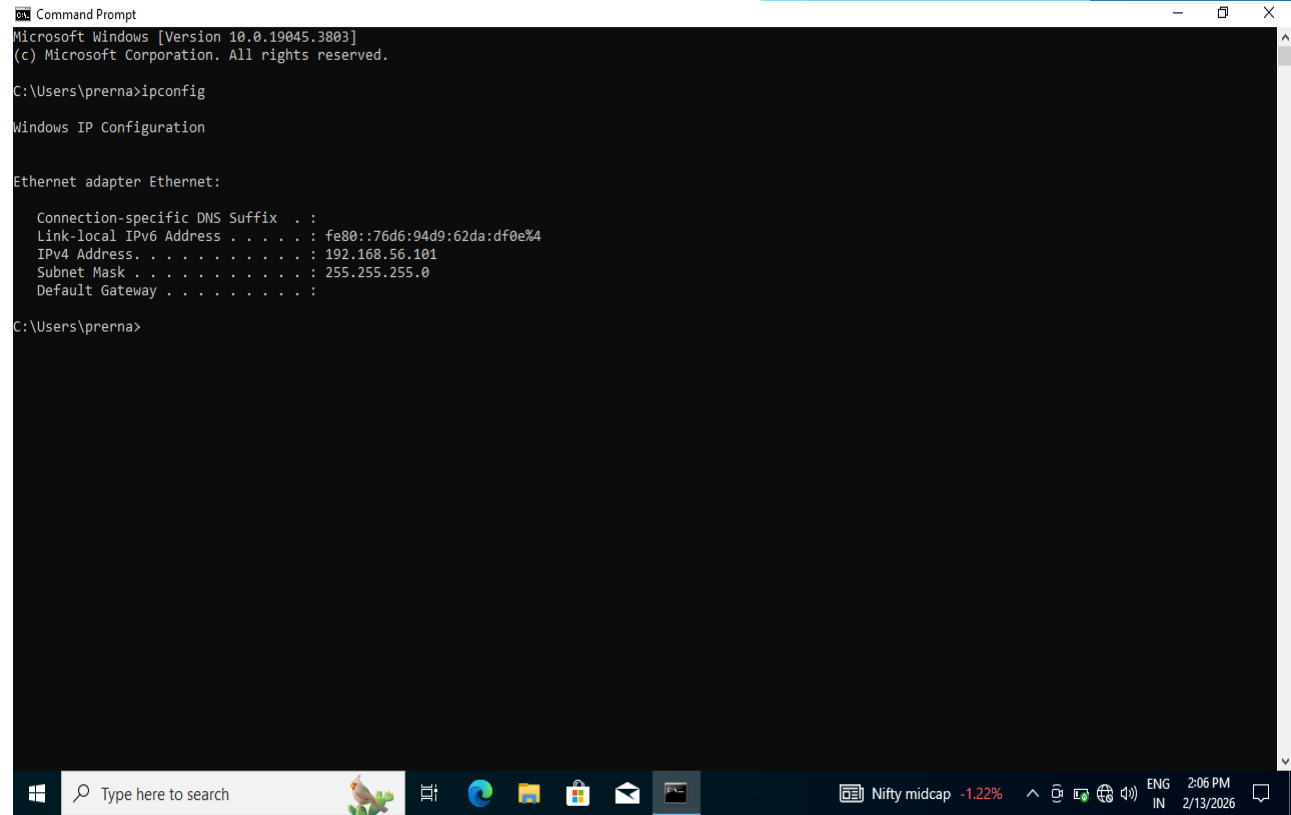
Methodology

:- Identifying Target IP Address

► Windows Target Machine

Open Command Prompt and run:
ipconfig

► This command displays the IP address of the target machine.



```
Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\prerna>ipconfig

Windows IP Configuration

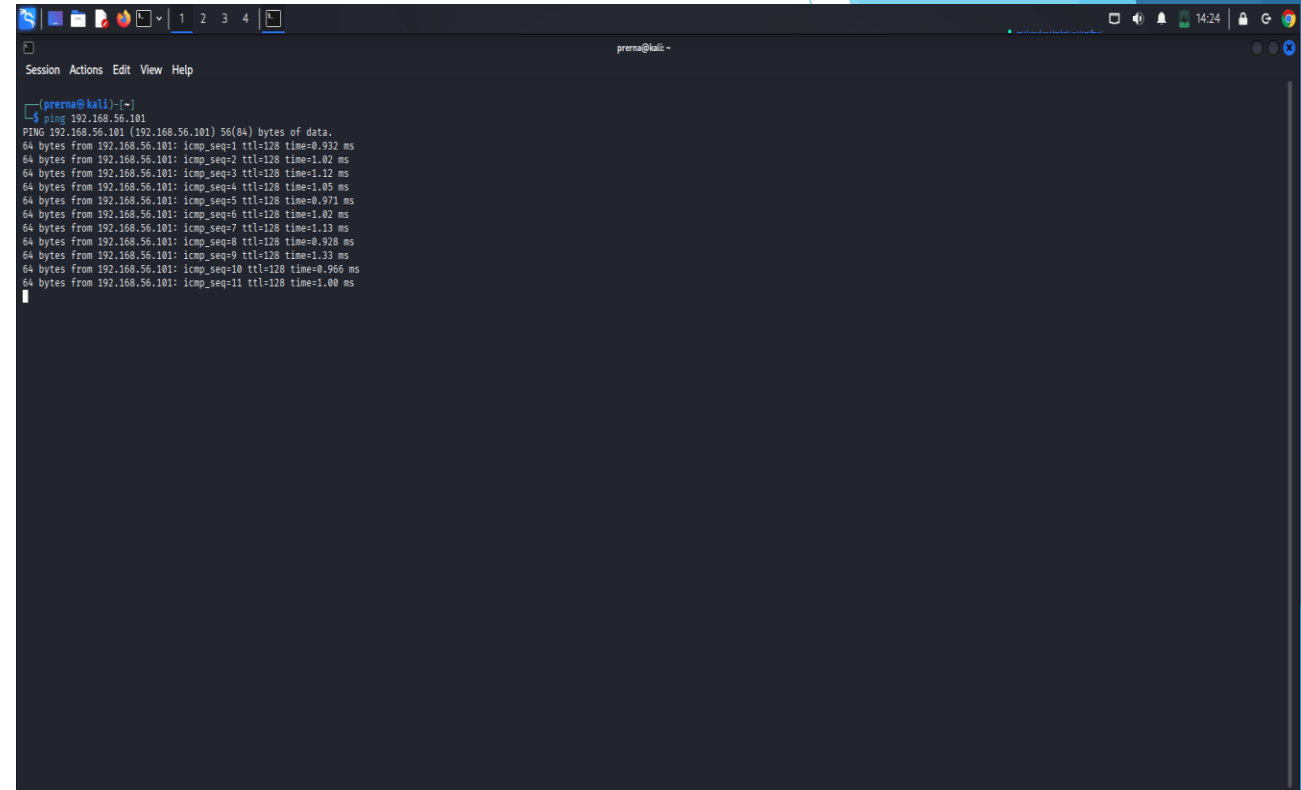
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::76d6:94d9:62da:df0e%4
    IPv4 Address. . . . . : 192.168.56.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Users\prerna>
```

:- Checking Network Connectivity

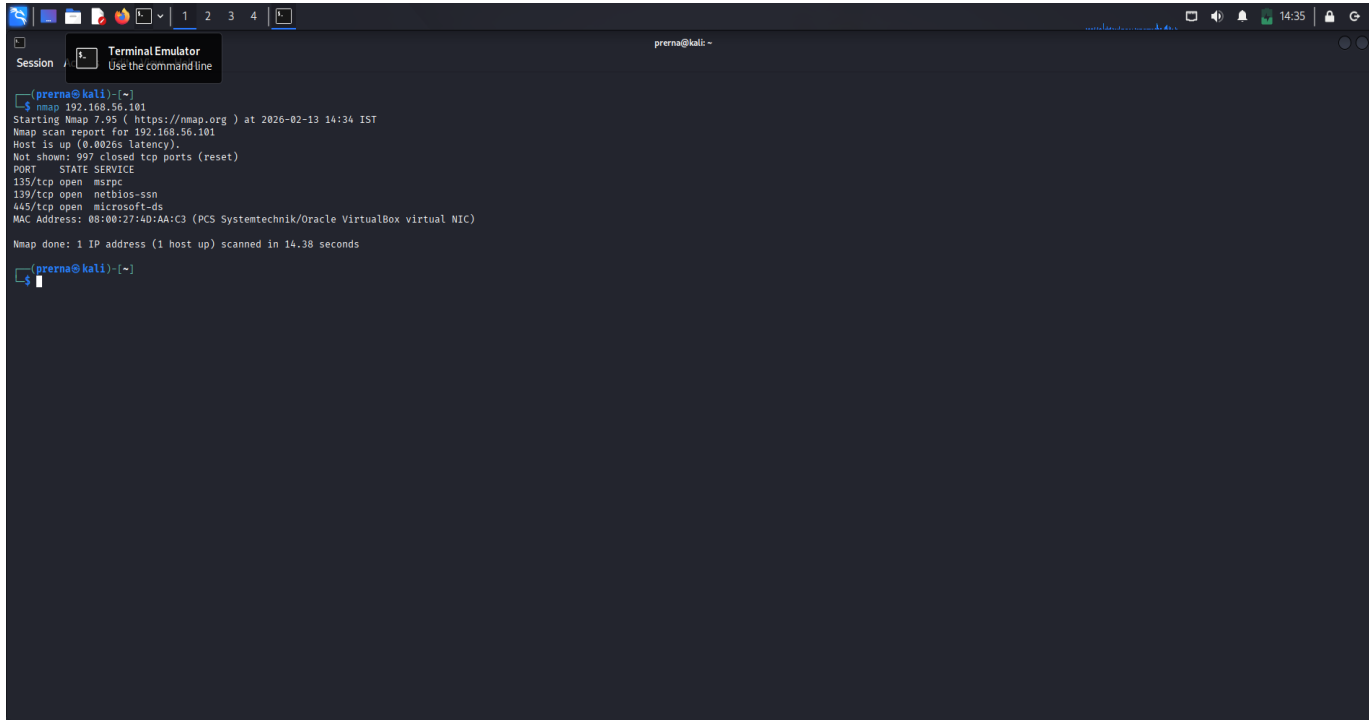
- ▶ Open Kali Linux terminal and execute:
- ▶ ping 192.168.56.101
- ▶ Expected Result:
- ▶ Successful reply confirms connectivity between attacker and target



The screenshot shows a Kali Linux terminal window with the following output:

```
prema@kali: ~  
$ ping 192.168.56.101  
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:  
64 bytes from 192.168.56.101: icmp_seq=1 ttl=128 time=0.932 ms  
64 bytes from 192.168.56.101: icmp_seq=2 ttl=128 time=1.02 ms  
64 bytes from 192.168.56.101: icmp_seq=3 ttl=128 time=1.12 ms  
64 bytes from 192.168.56.101: icmp_seq=4 ttl=128 time=1.05 ms  
64 bytes from 192.168.56.101: icmp_seq=5 ttl=128 time=0.971 ms  
64 bytes from 192.168.56.101: icmp_seq=6 ttl=128 time=1.02 ms  
64 bytes from 192.168.56.101: icmp_seq=7 ttl=128 time=1.13 ms  
64 bytes from 192.168.56.101: icmp_seq=8 ttl=128 time=0.928 ms  
64 bytes from 192.168.56.101: icmp_seq=9 ttl=128 time=1.33 ms  
64 bytes from 192.168.56.101: icmp_seq=10 ttl=128 time=0.966 ms  
64 bytes from 192.168.56.101: icmp_seq=11 ttl=128 time=1.00 ms
```

:- Performing Basic Nmap Scan



```
(prema@kali)-[~]
$ nmap 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-02-13 14:34 IST
Nmap scan report for 192.168.56.101
Host is up (0.0026s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:40:AA:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds
(prema@kali)-[~]
```

Execute the following command:

```
nmap 192.168.56.101
```

Purpose:

- ▶ Identify open ports
- ▶ Detect services running on those ports

Port 135 - RPC

Working:

- ▶ Used for Remote Procedure Call communication
- ▶ Supports remote system management
- ▶ Helps Windows services communicate internally

Risk:

- ▶ Can allow remote system exploitation
- ▶ May expose system information
- ▶ Can be used by malware to gain access

Port 139 - NetBIOS

Working:

- ▶ Supports file and printer sharing
- ▶ Enables communication between Windows devices
- ▶ Used for network authentication

Risk:

- ▶ Unauthorized access to shared files
- ▶ Password and user information exposure
- ▶ Helps attackers gather network details

Port 445 - SMB

Working:

- ▶ Used for file and folder sharing
- ▶ Supports remote access and network authentication
- ▶ Enables resource sharing in Windows networks

Risk:

- ▶ Common target for ransomware and malware attacks
- ▶ Can allow data theft and remote code execution
- ▶ Can spread network worms and viruses

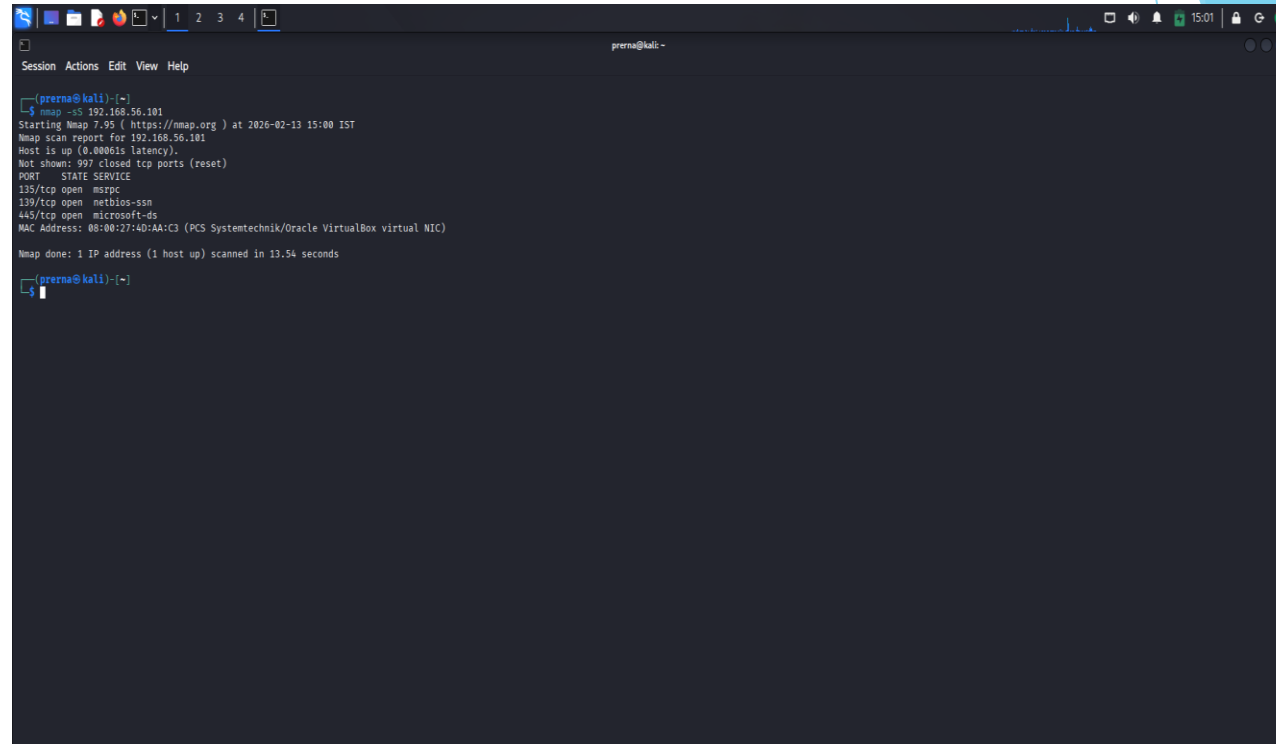
:- SYN Scan (Stealth Scan)

▶ Execute:

`nmap -sS 192.168.56.101`

Purpose:

- ▶ Performs stealth scanning
- ▶ Sends partial TCP handshake
- ▶ Harder to detect by firewalls



```
prerna@kali:~$ nmap -sS 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-13 15:00 IST
Nmap scan report for 192.168.56.101
Host is up (0.00061s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  mtrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:4D:AA:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.54 seconds
prerna@kali:~$
```

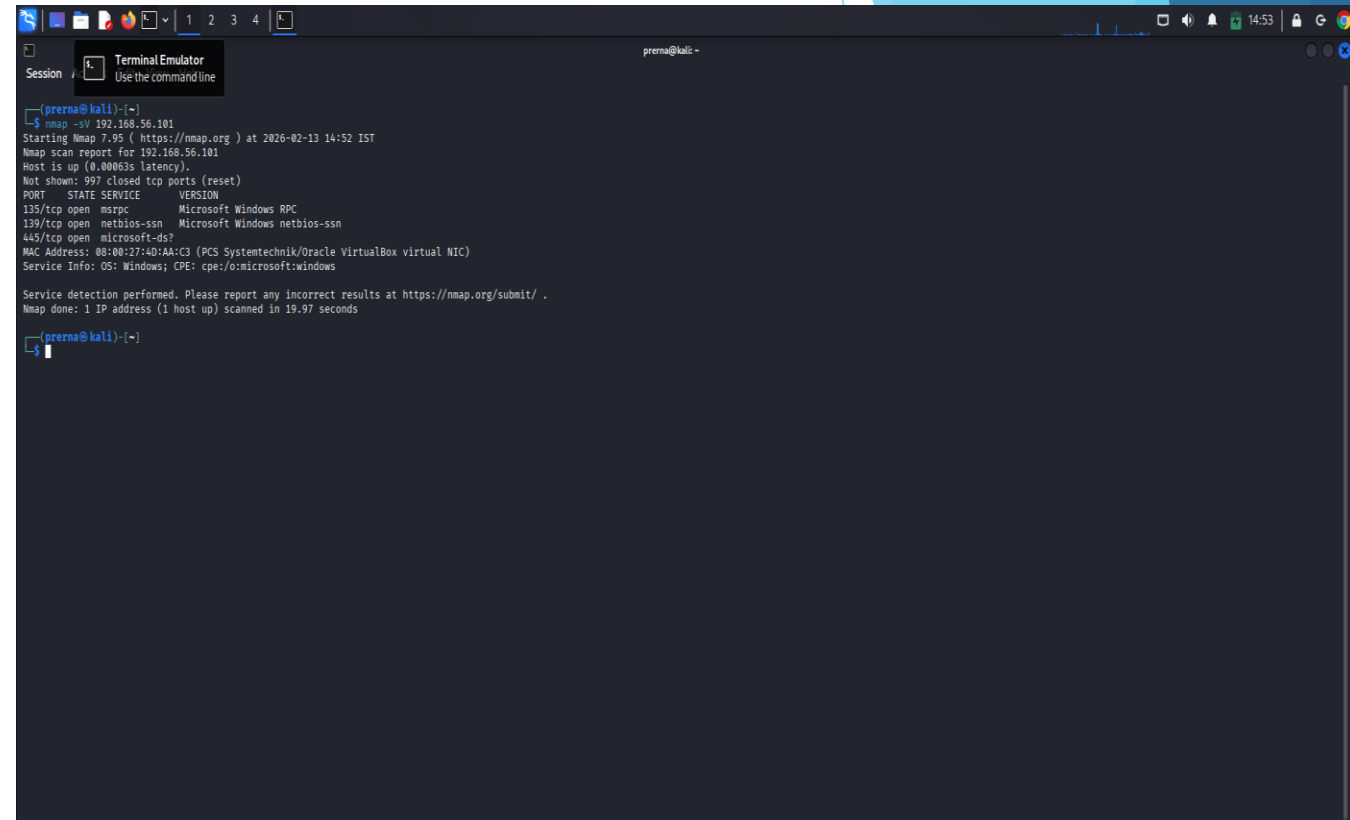

:- Service Version Detection

Execute:

```
nmap -sV 192.168.X.X
```

Purpose:

- ▶ Identifies exact service versions running on ports
- ▶ Helps detect outdated or vulnerable services



The screenshot shows a terminal window titled "Terminal Emulator" with the prompt "prerna@kali:". The user has executed the command `nmap -sV 192.168.56.101`. The output displays the Nmap scan results for 192.168.56.101, including the scan time (2026-02-13 14:52 IST), host status (up), and a table of open ports with their respective services and versions. The scan also shows the MAC address and service information for the host.

```
(prerna@kali)-[~]
$ nmap -sV 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-13 14:52 IST
Nmap scan report for 192.168.56.101
Host is up (0.000063s latency).
Not shown: 997 closed tcp ports (reset)
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?
MAC Address: 08:00:27:4D:AA:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 19.97 seconds

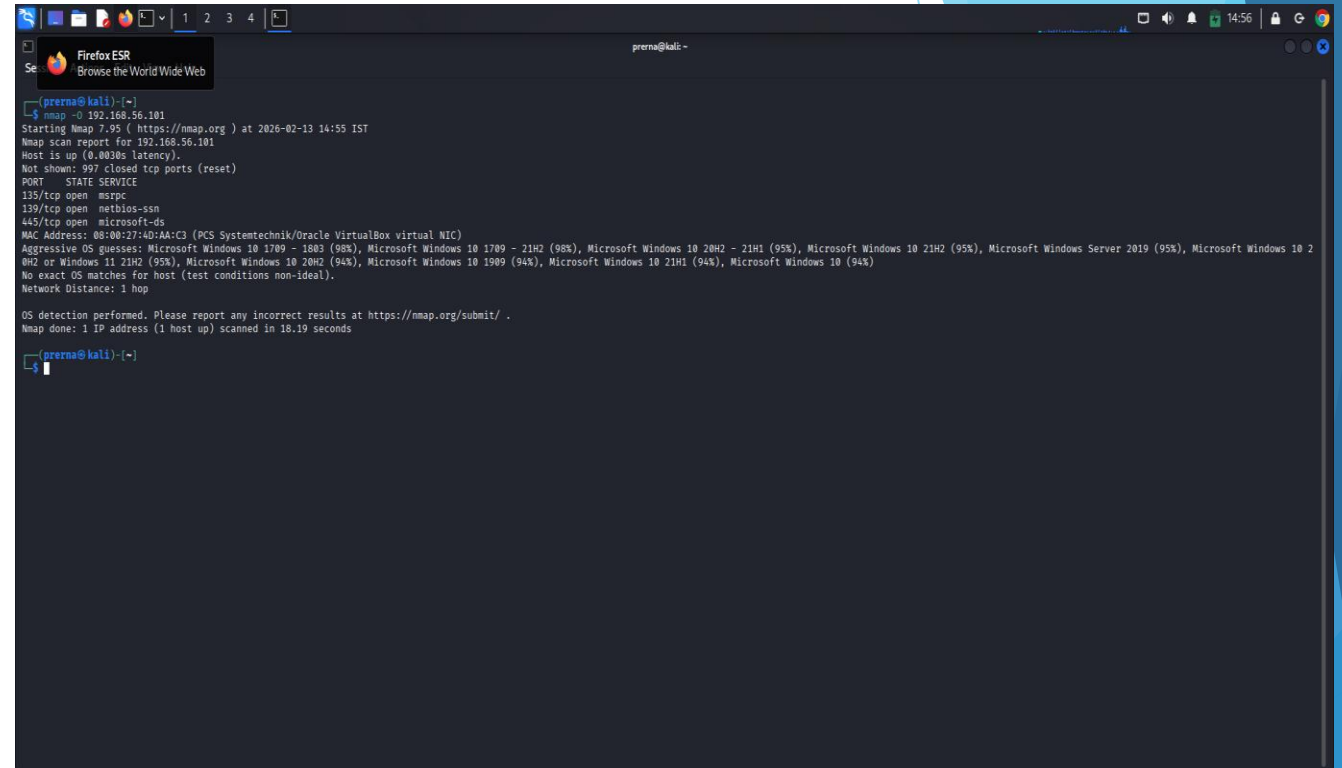
(prerna@kali)-[~]
$
```

:- Operating System Detection

Execute:

`nmap -O 192.168.X.X`

- ▶ Purpose:
- ▶ Detects operating system of target machine
- ▶ Helps attackers plan targeted attacks



```
prerna@kali:~$ nmap -O 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-13 14:55 IST
Nmap scan report for 192.168.56.101
Host is up (0.0030s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:40:AA:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Microsoft Windows 10 1709 - 1803 (98%), Microsoft Windows 10 1709 - 21H2 (98%), Microsoft Windows 10 20H2 - 21H1 (95%), Microsoft Windows 10 21H2 (95%), Microsoft Windows Server 2019 (95%), Microsoft Windows 10 20H2 or Windows 11 21H2 (95%), Microsoft Windows 10 20H2 (94%), Microsoft Windows 10 1909 (94%), Microsoft Windows 10 21H1 (94%), Microsoft Windows 10 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.19 seconds

prerna@kali:~$
```

:- Aggressive Scan

Execute:

`nmap -A 192.168.X.X`

► Purpose:

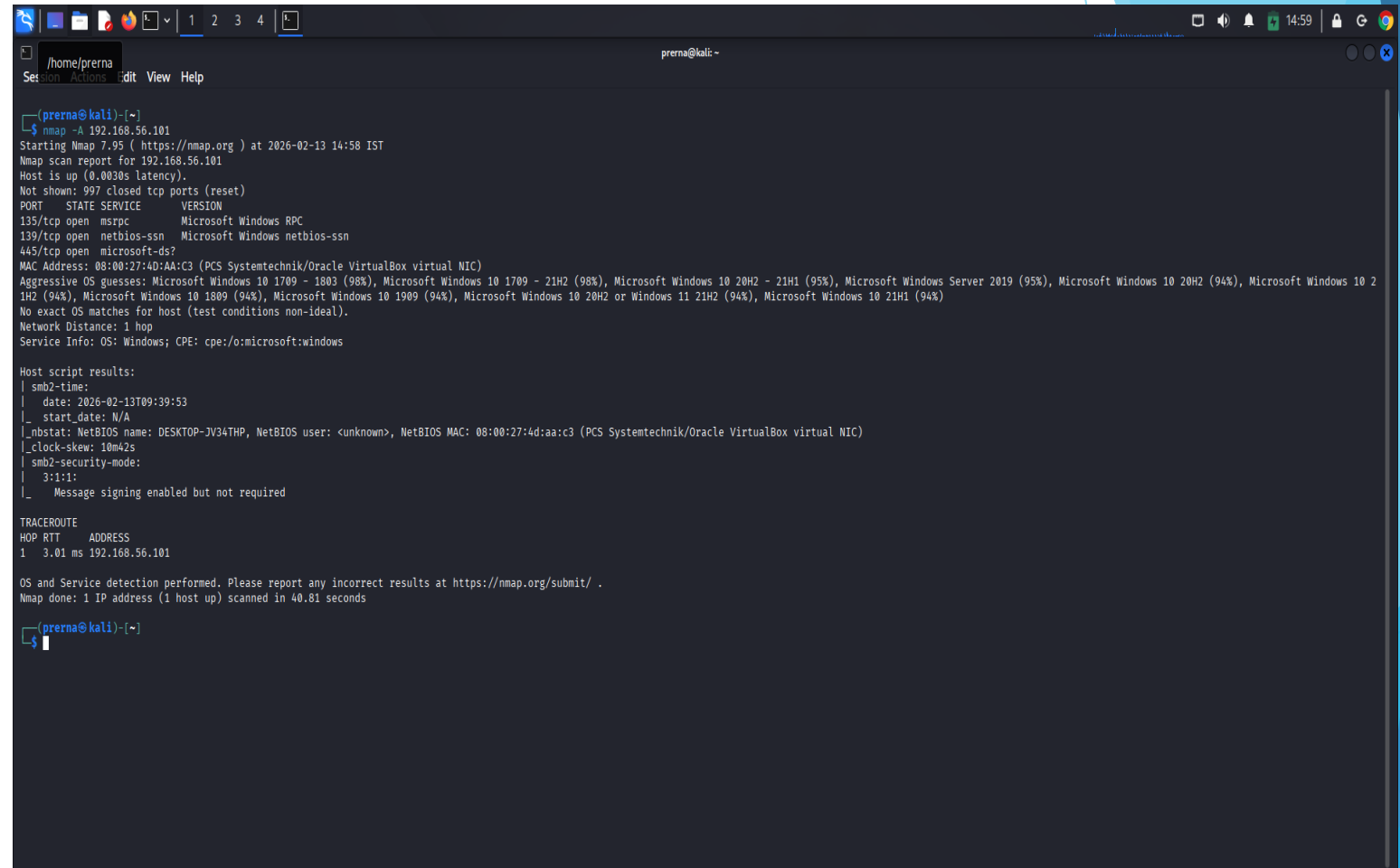
► This scan performs:

► OS detection

► Version detection

► Script scanning

► Traceroute

A screenshot of a Kali Linux terminal window. The terminal shows the execution of the command `nmap -A 192.168.56.101`. The output includes a standard Nmap scan report for 192.168.56.101, indicating the host is up with a latency of 0.0030s. It lists open ports: 135/tcp (msrpc), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds?). The OS detection section shows aggressive OS guesses for Microsoft Windows 10 and Windows Server 2019. Below this, the host script results for smb2-time are shown, including start date, NetBIOS name, and security mode. A traceroute is also displayed, showing a single hop to the target IP. The scan concludes with OS and service detection performed in 40.81 seconds.

```
(prerna@kali)~$ nmap -A 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-13 14:58 IST
Nmap scan report for 192.168.56.101
Host is up (0.0030s latency).
Not shown: 997 closed tcp ports (reset)
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?
MAC Address: 08:00:27:4D:AA:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Microsoft Windows 10 1709 - 1803 (98%), Microsoft Windows 10 1709 - 21H2 (98%), Microsoft Windows 10 20H2 - 21H1 (95%), Microsoft Windows Server 2019 (95%), Microsoft Windows 10 20H2 (94%), Microsoft Windows 10 21H2 (94%), Microsoft Windows 10 1809 (94%), Microsoft Windows 10 1909 (94%), Microsoft Windows 10 20H2 or Windows 11 21H2 (94%), Microsoft Windows 10 21H1 (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: 2026-02-13T09:39:53
|   start_date: N/A
|_ nbstat: NetBIOS name: DESKTOP-JV34THP, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:4d:aa:c3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
|_ clock-skew: 10m42s
|_ smb2-security-mode:
|   3.1.1:
|_   Message signing enabled but not required

TRACEROUTE
HOP RTT ADDRESS
1 3.01 ms 192.168.56.101

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 40.81 seconds

(prerna@kali)~$
```

Result Analysis

After performing scans, the following observations can be made:

- ▶ Multiple open ports were detected
- ▶ Several services were running on the target system
- ▶ Some services may contain outdated versions
- ▶ OS detection revealed system type and configuration

These results help in identifying system vulnerabilities.

Risk Analysis

Open ports can create multiple security risks such as:

- ▶ **Unauthorized Access**

Attackers may exploit open ports to gain system access.

- ▶ **Data Leakage**

Sensitive information can be exposed through vulnerable services.

- ▶ **Malware Attacks**

Attackers can deliver malicious payloads through open services.

- ▶ **Network Exploitation**

Weak services may allow lateral movement inside the network.

Security Recommendation

To improve system security, the following measures are recommended:

- ▶ Close unused ports
- ▶ Enable firewall protection
- ▶ Update software and services regularly
- ▶ Implement intrusion detection systems
- ▶ Monitor network traffic continuously

Learning Outcome

Through this project, the following knowledge was gained:

- ▶ Understanding of network reconnaissance
- ▶ Practical experience with Nmap scanning techniques
- ▶ Ability to analyze security risks
- ▶ Knowledge of vulnerability prevention strategies

conclusion

- ▶ Nmap is a powerful tool for network scanning and vulnerability identification. This project demonstrated how open ports and services can expose systems to cyber threats. Proper security measures can significantly reduce these risks.