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

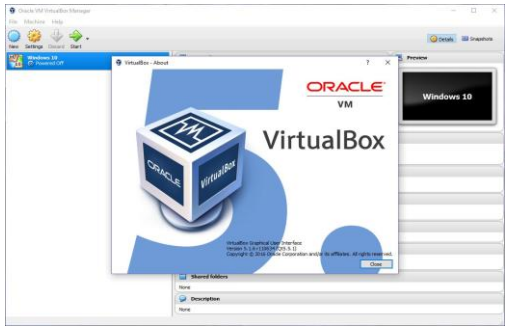
The main objectives of this project are:

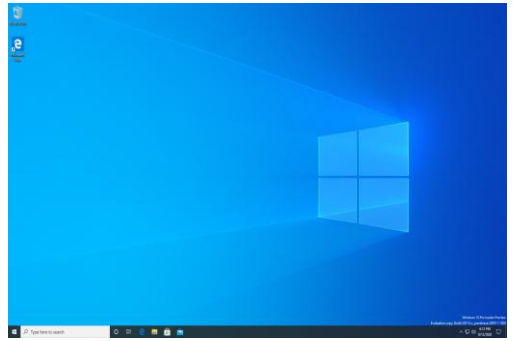
- To identify active hosts in a network
- To perform port scanning using Nmap
- To detect services running on open ports
- To analyze security risks associated with open ports
- To recommend prevention strategies

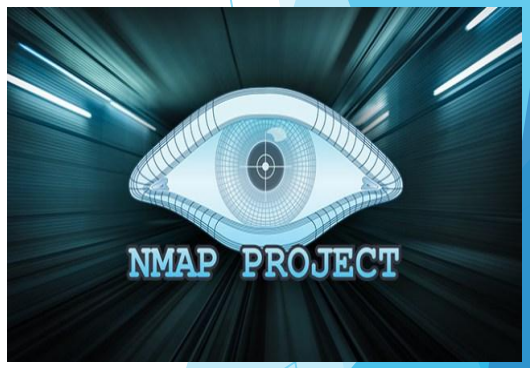
Tools and Environment Setup

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

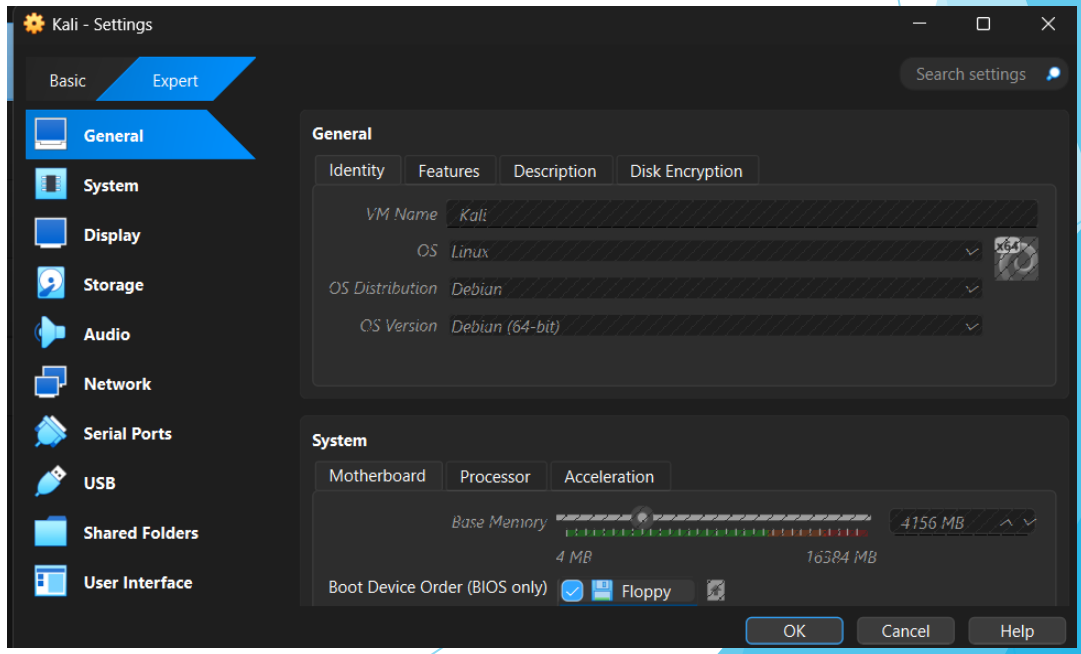
Step 2: Kali Linux Installation

- Download Kali Linux ISO file
- Open VirtualBox
- Click New Virtual Machine
- Set the following configuration:

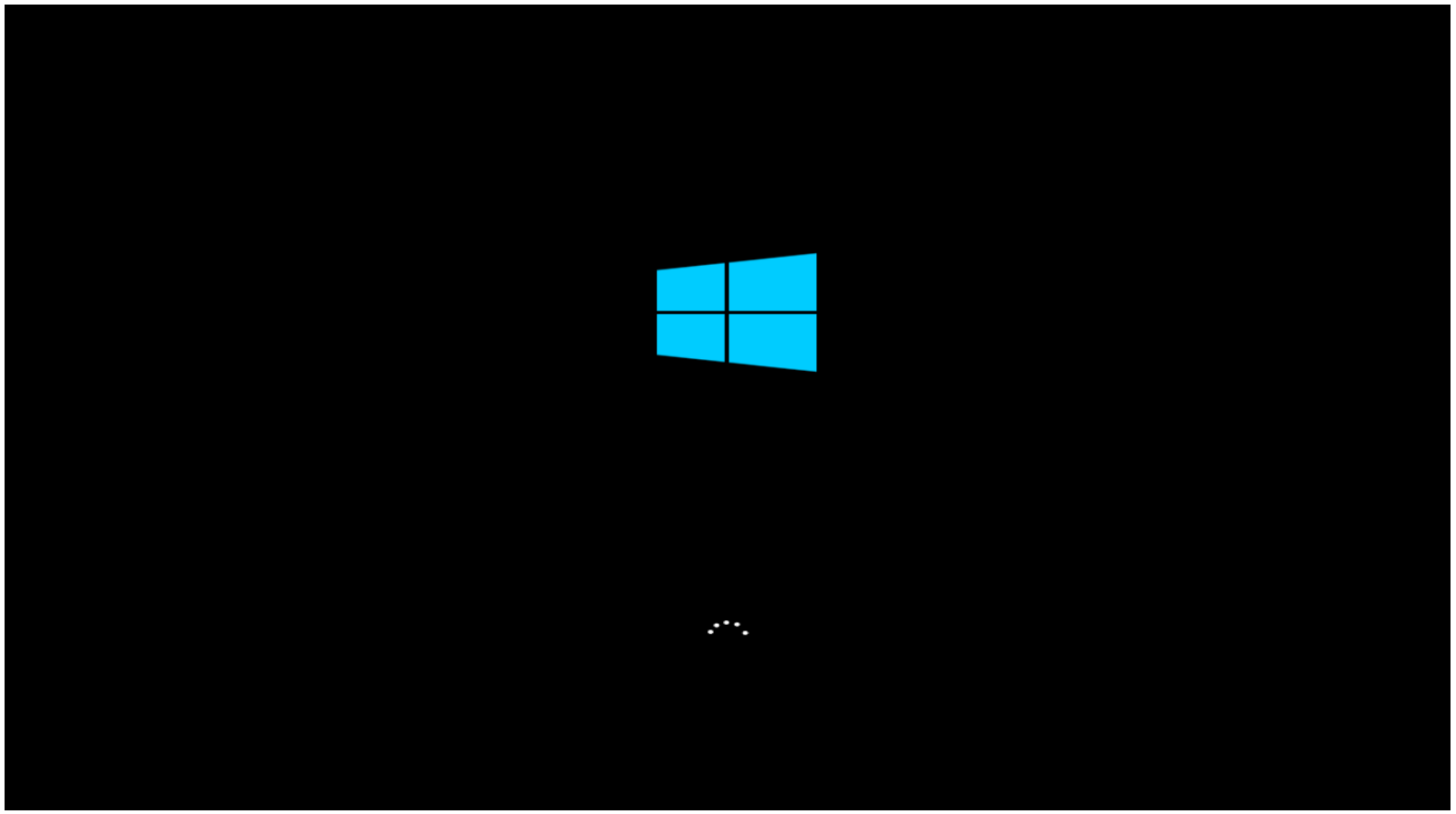
RAM: Minimum 2GB

Storage: Minimum 20GB

- Attach Kali Linux ISO and start installation
- Complete installation using default settings

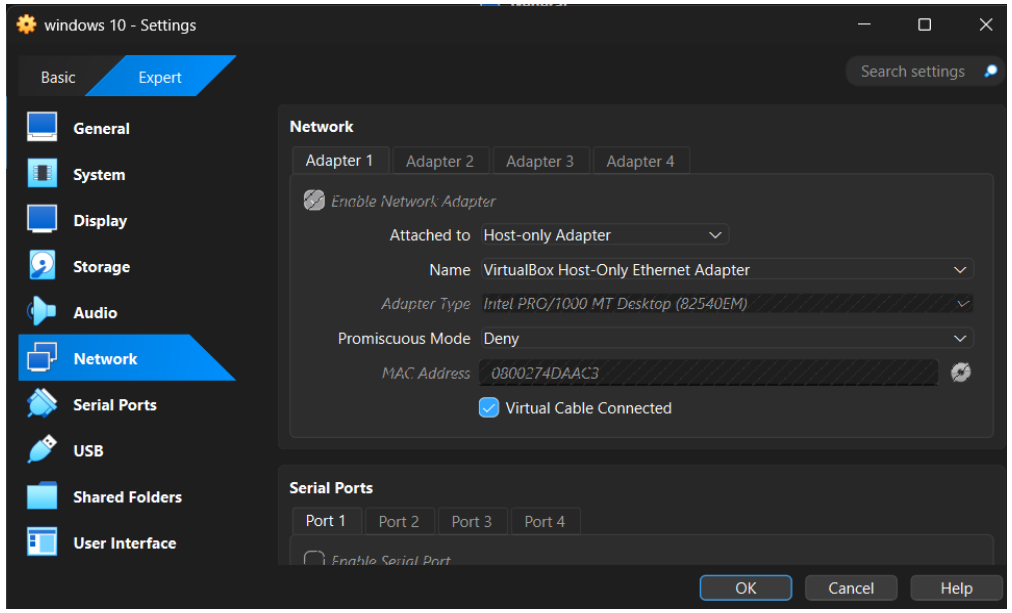


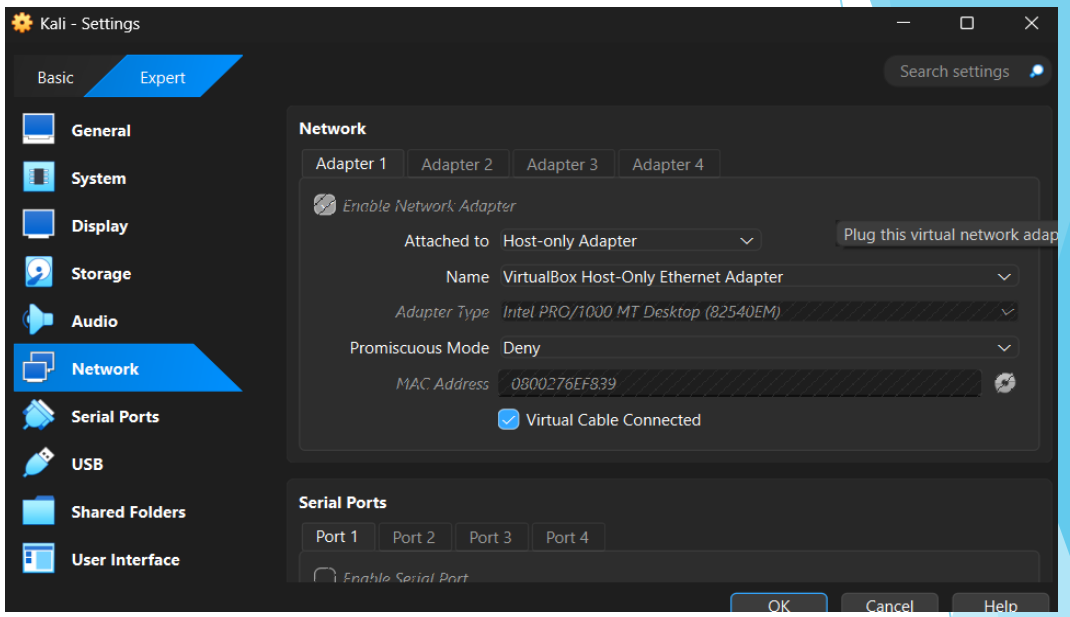
Target Machine:-



- 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

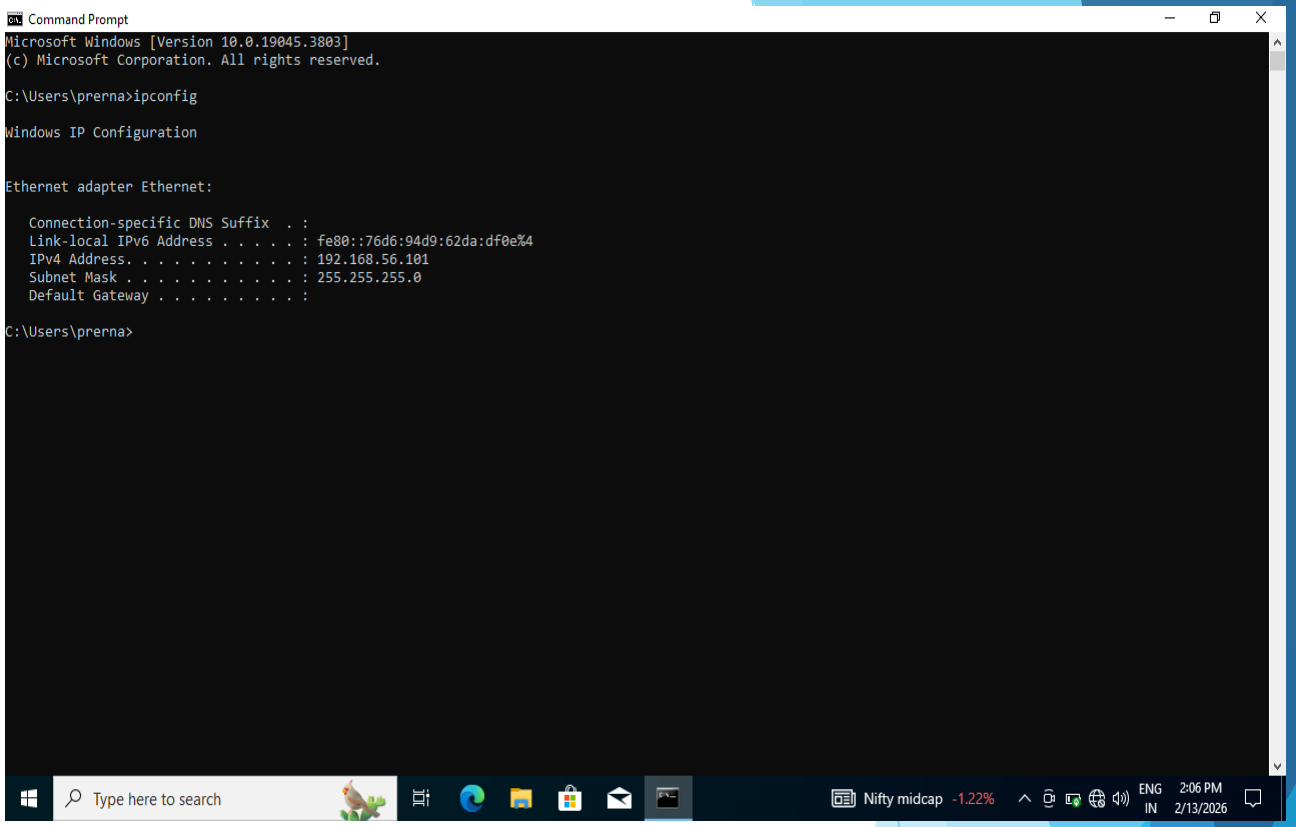
Methodology

:- Identifying Target IP Address

- Windows Target Machine

Open Command Prompt and run:

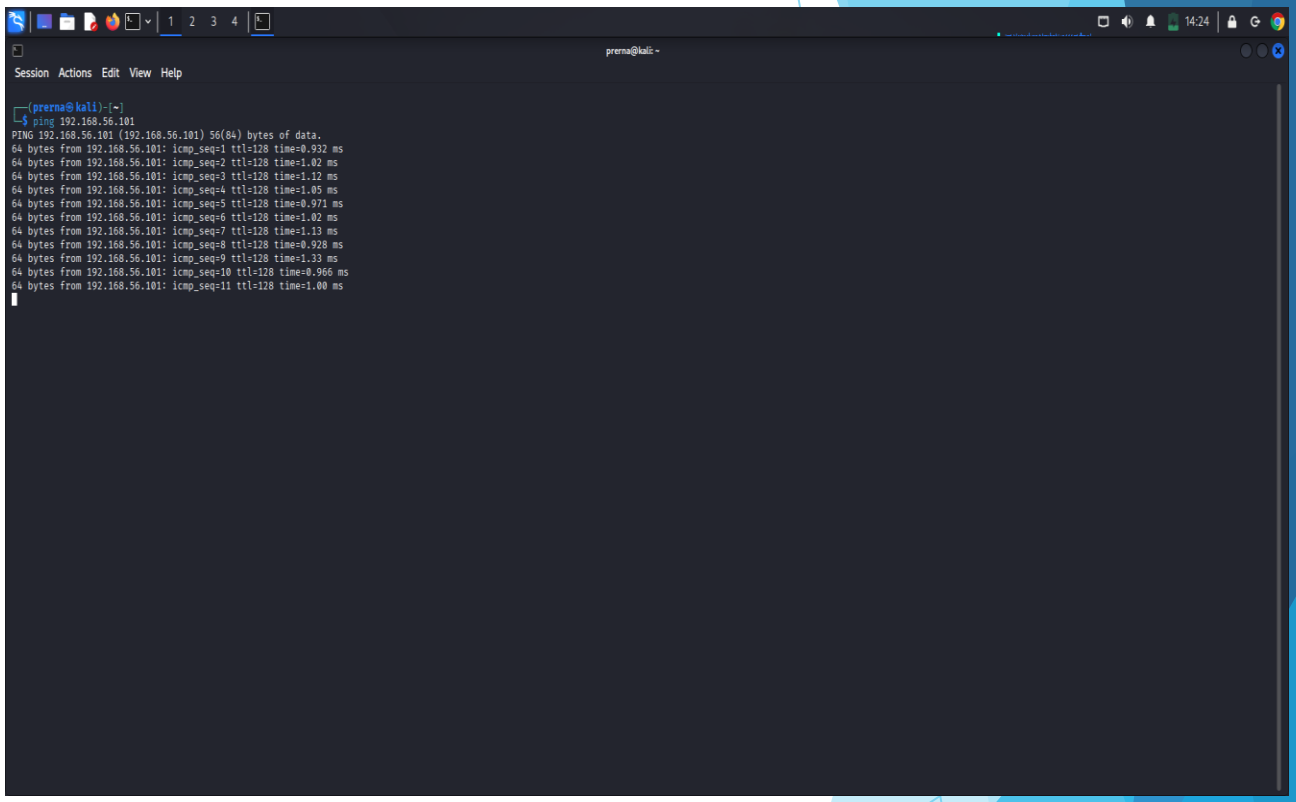
ipconfig



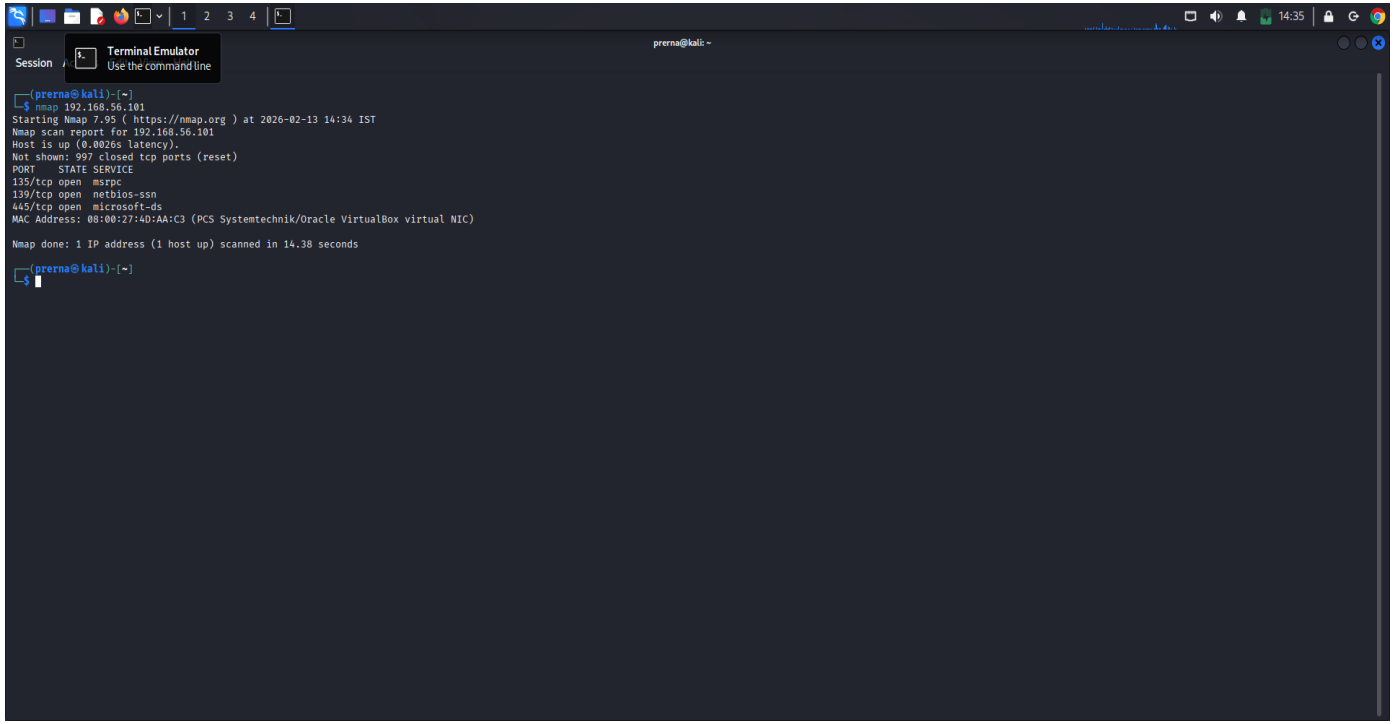
- This command displays the IP address of the target machine.

:- Checking Network Connectivity

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



:- Performing Basic Nmap Scan



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

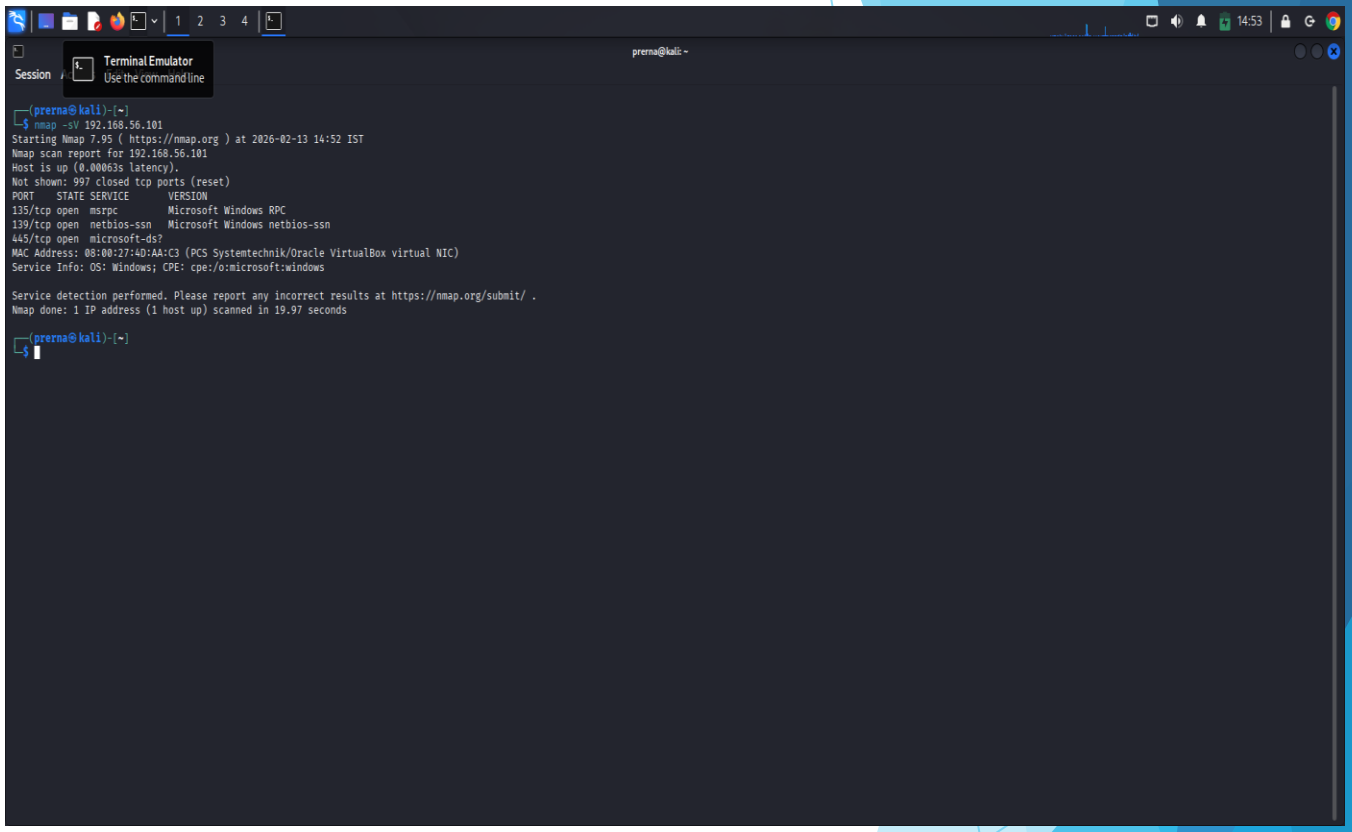
:- Service Version Detection

Execute:

nmap -sV 192.168.X.X

Purpose:

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

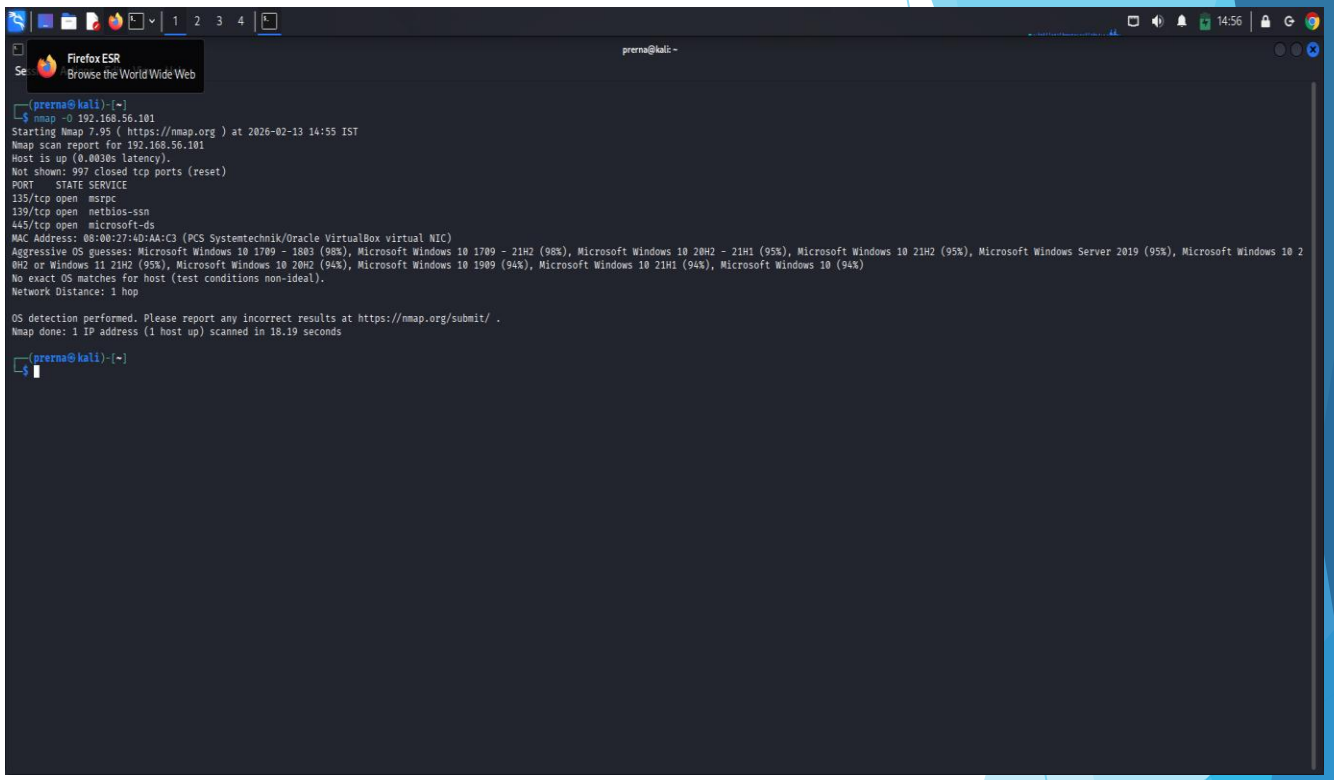


:- Operating System Detection

Execute:

nmap -O 192.168.X.X

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

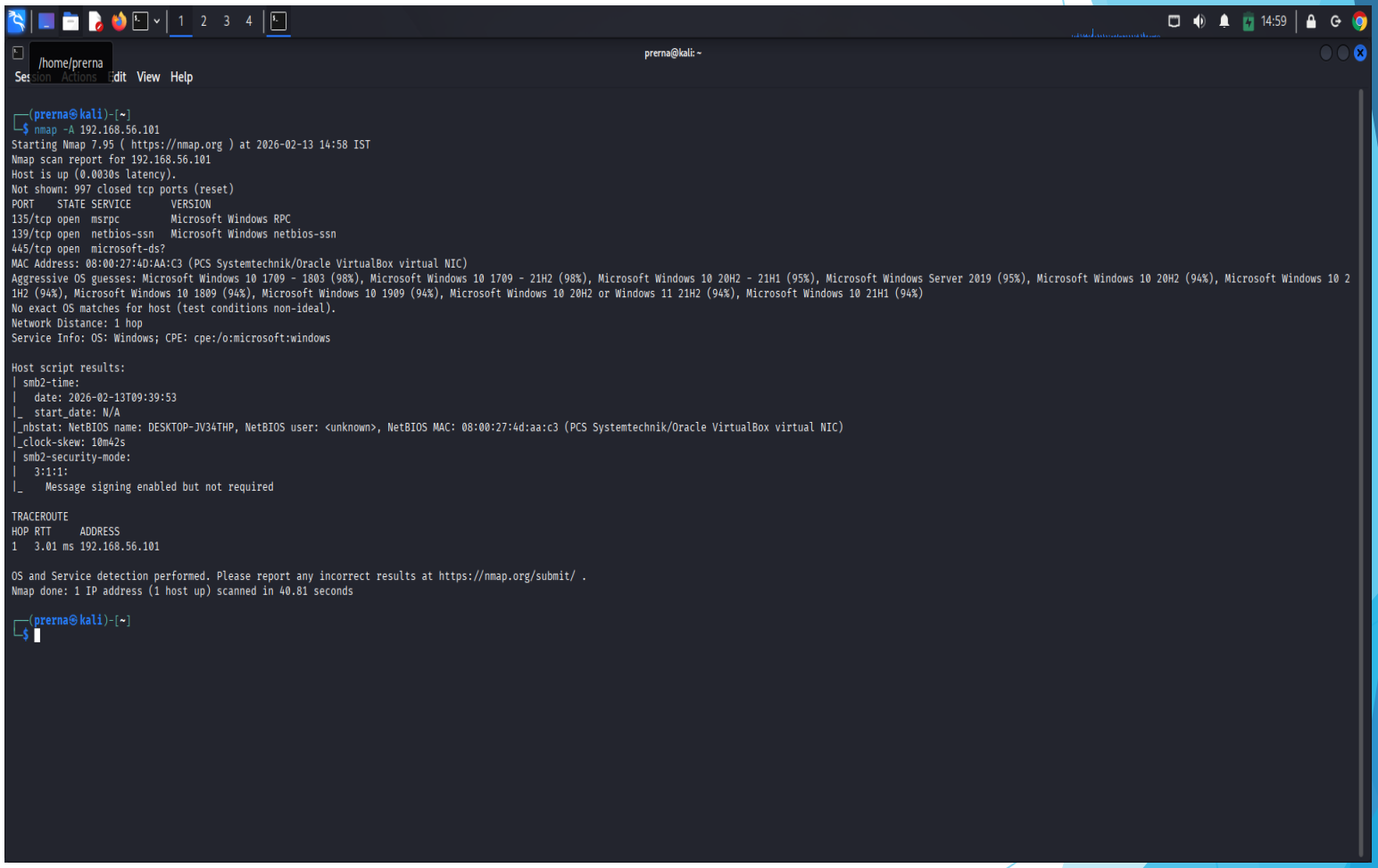


:- Aggressive Scan

Execute:

nmap -A 192.168.X.X

- Purpose:
- This scan performs:
- OS detection
- Version detection
- Script scanning
- Traceroute



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.