Task 2 :- Seeing the Unseen - Network Scanning & Enumeration

Name :- Rushikesh Sanjay Kumavat

INTERN ID:- SN1000726

DOMAIN:- Cyber Security

Aim:-

To perform network scanning and service enumeration on the Metasploitable virtual machine using Nmap from Kali Linux in order to identify open ports, running services, and potential security vulnerabilities within a controlled lab environment.

Objective :-

To perform network scanning on the Metasploitable VM using Nmap from Kali Linux and enumerate open ports, running services, and operating system details.

Tools Used :-

- Kali Linux
- Metasploitable 2
- Nmap

Target Information :-

- Target IP Address: 192.168.56.101
- Attacker Machine: Kali Linux

Procedure :-

Step 1 – Basic Port Scan

Command Used:

➔ nmap 192.168.56.101

Purpose:

To identify open ports on the target machine.

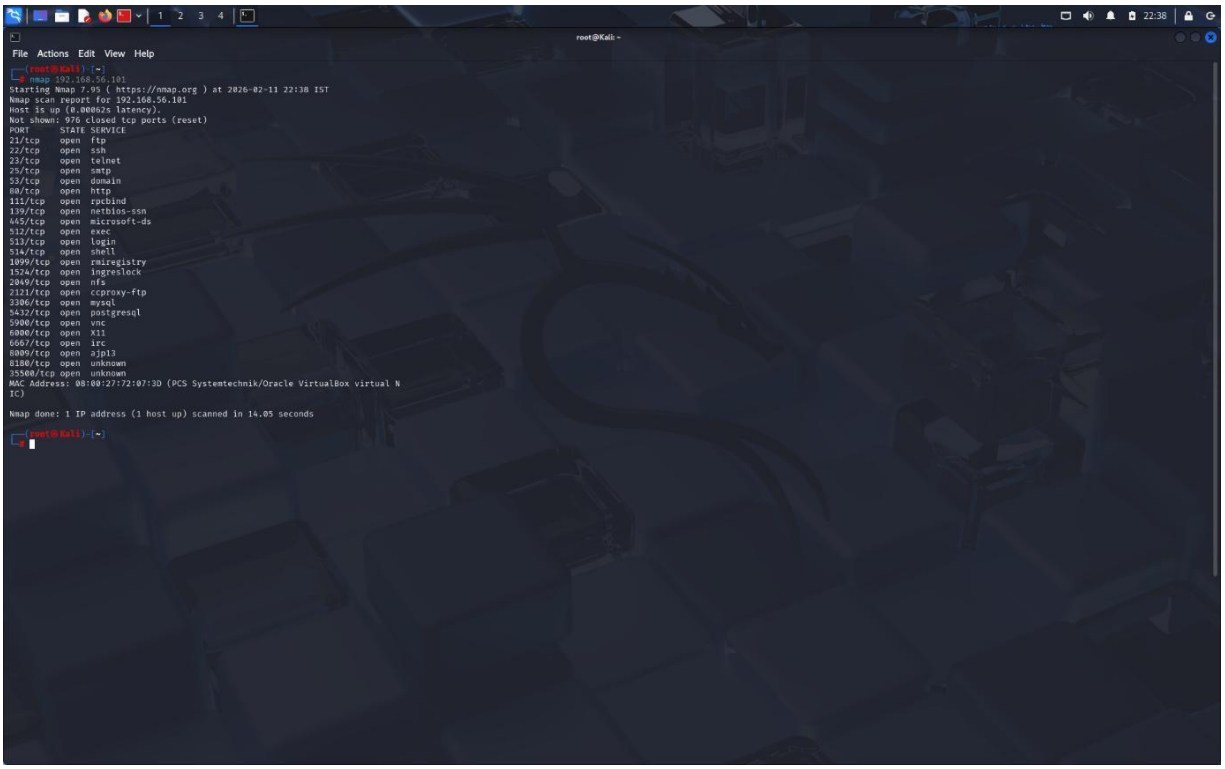


Figure 1: Basic Nmap scan showing open ports

Step 2 – Aggressive Scan (-A)

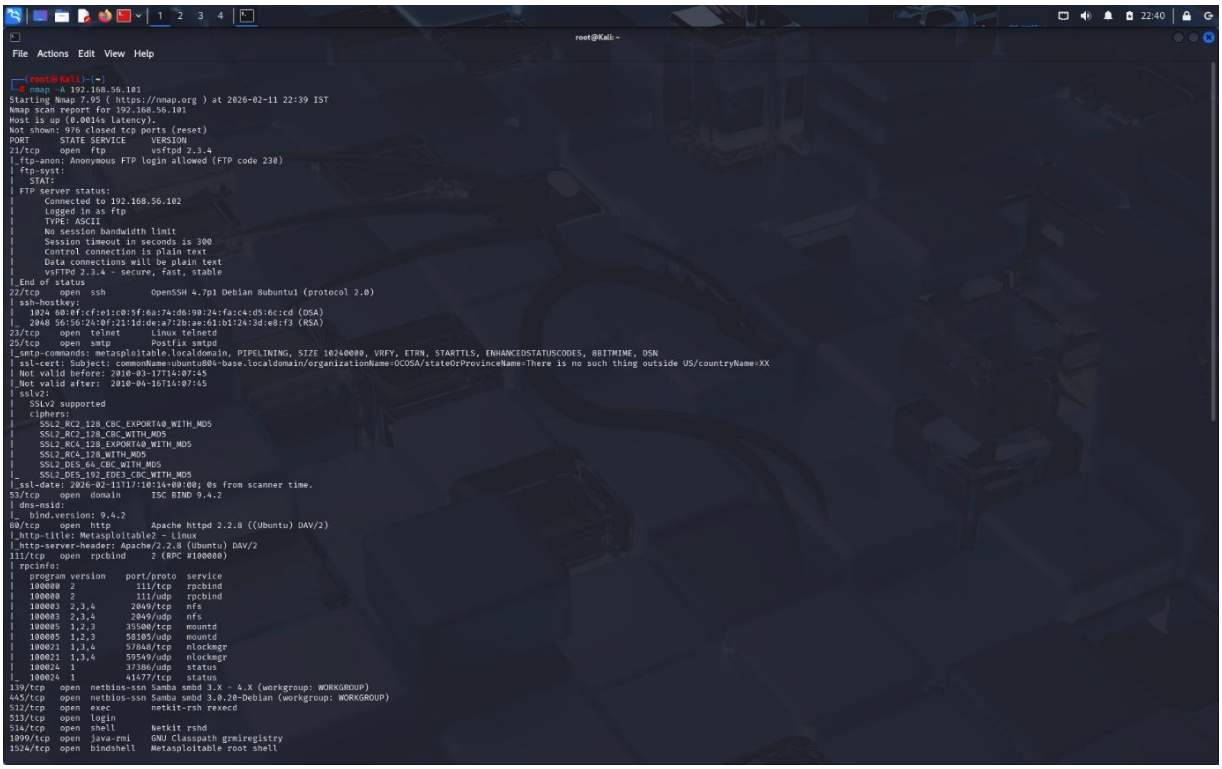
Command Used:

➔ nmap -A 192.168.56.101

Purpose:

To detect:

- Service versions
- Operating system
- Additional script information



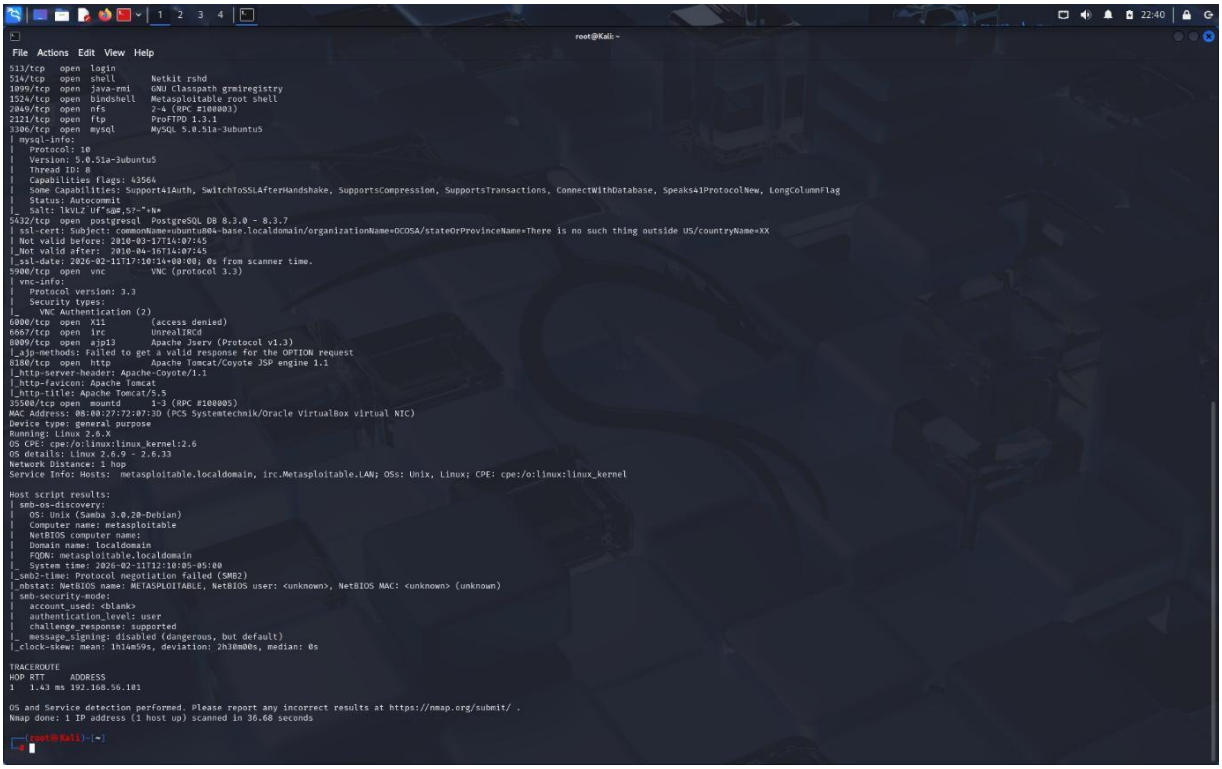


Figure 2: Aggressive Nmap scan showing service versions and OS details

Step 3 – Full Port Scan

Command Used:

➔ nmap -p- 192.168.56.101

Purpose:

To scan all 65535 ports, not just common ones.

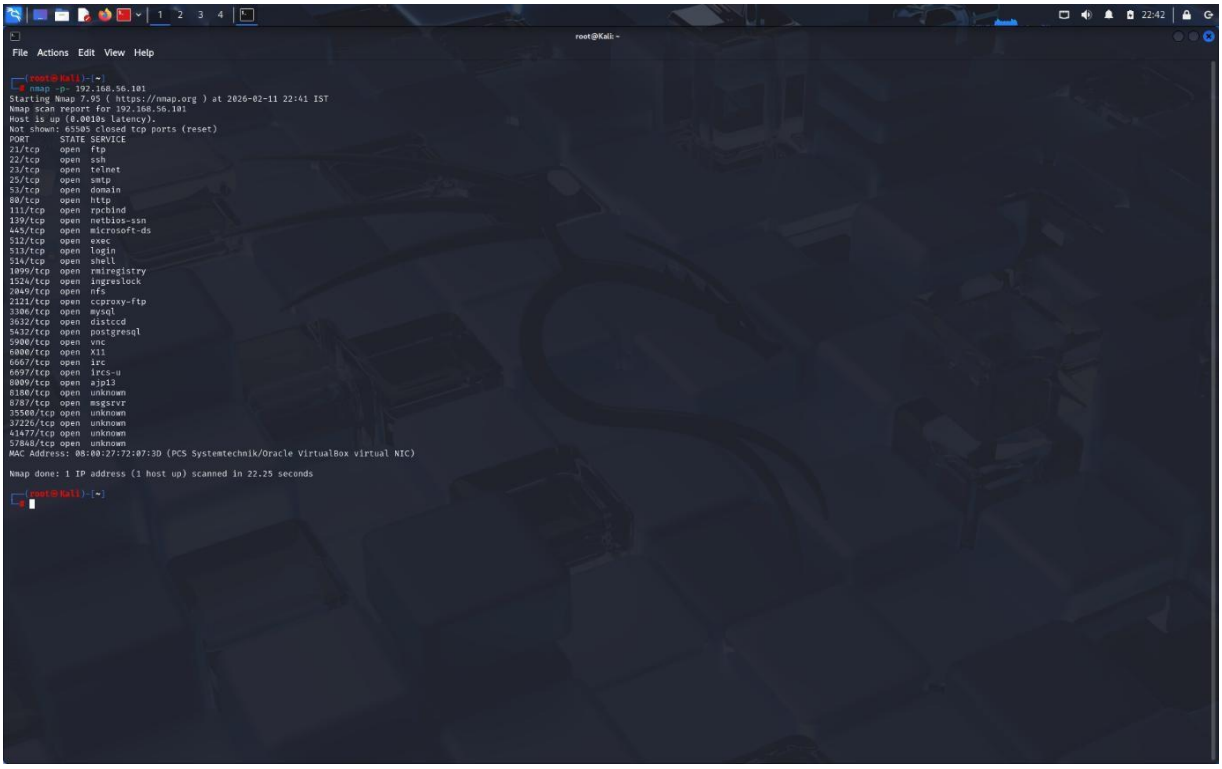


Figure 3: Full port scan identifying additional open services

Enumeration Results :-

The scan revealed:

Port	Service	Version
21	FTP	vsftpd 2.3.4
22	SSH	OpenSSH 4.7p1
23	TELNET	Open Telnet
80	HTTP	Apache 2.2.8
3306	MYSQL	MySQL 5.0
5432	POSTGRESQL	PostgreSQL DB

Analysis :-

The target system has multiple vulnerable services running, including:

- FTP server
- Telnet (insecure protocol)
- Outdated Apache web server
- Database services exposed

This increases the attack surface and makes the system vulnerable to exploitation.

Conclusion :-

The network scanning and enumeration process successfully identified open ports and services running on the Metasploitable VM. This demonstrates how attackers gather intelligence before launching attacks.

Understanding this process helps defenders secure exposed services.