

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.

```
(root㉿kali)-[~] nmap -A 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-11 22:38 IST
Nmap scan report for 192.168.56.101
Host is up (0.0002s latency).
Not shown: 976 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  dns
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  exec
3724/tcp  open  login
5349/tcp  open  mailnull
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2000/tcp  open  http-proxy
2321/tcp  open  cproxxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8000/tcp  open  ejb3
8180/tcp  open  unknown
35508/tcp open  unknown
MAC Address: 08:00:27:72:07:30 (PC Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.05 seconds
```

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

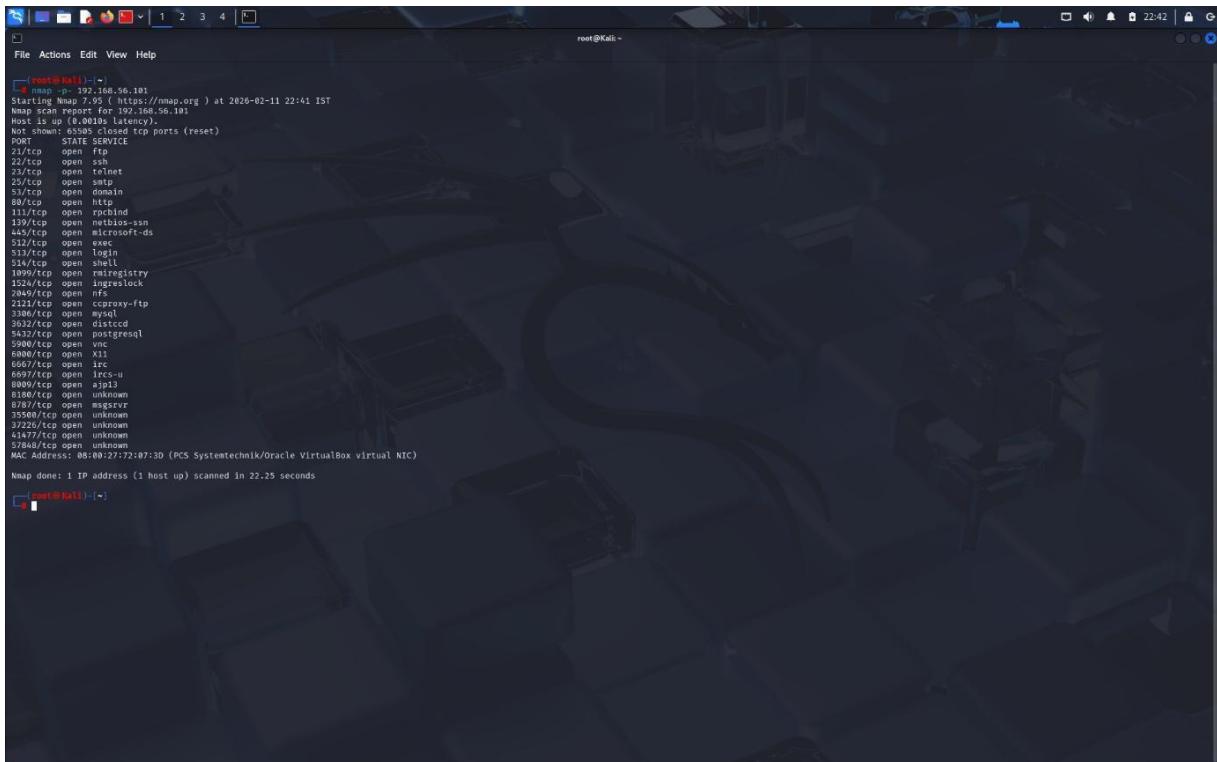
Step 3 – Full Port Scan

Command Used:

→ nmap -p- 192.168.56.101

Purpose:

To scan all 65535 ports, not just common ones.



```
[root@Kali:~]# nmap -p- 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-11 22:41 IST
Nmap scan report for 192.168.56.101
Host is up (0.000s latency).
Not shown: 65535 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  exec
513/tcp   open  login
53/tcp    open  shell
109/tcp   open  pop3
152/tcp   open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  proxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5930/tcp  open  unknown
6000/tcp  open  X11
6667/tcp  open  irc
6900/tcp  open  ircs-ii
8000/tcp  open  ajp13
6186/tcp  open  unknown
8787/tcp  open  msfsrvr
35353/tcp open  unknown
37226/tcp open  unknown
41477/tcp open  unknown
57849/tcp open  unknown
MAC Address: 08:00:27:72:07:3D (PC Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 22.25 seconds
[root@Kali:~]
```

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.