

**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: ~  
[root@kali] (~)  
# nmap 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 (S.Nmap's latency).  
Not shown: 976 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  
119/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1899/tcp  open  rairegistry  
1934/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
2186/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  x11  
6667/tcp  open  irc  
8080/tcp  open  http  
8180/tcp  open  unknown  
35568/tcp open  unknown  
MAC Address: 08:00:27:72:07:3D (PCS Systemtechnik/Oracle VirtualBox virtual N IC)  
Nmap done: 1 IP address (1 host up) scanned in 14.05 seconds  
[root@kali] (~)
```

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

```
root@kali:~# nmap -A 192.168.56.181
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-11 22:39 IST
Nmap scan report for 192.168.56.181
Host is up (0.001s latency).
Not shown: 976 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp           vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.56.181
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_  1024 60:ff:cfe1:c0:5f:6a:7a:2d:06:09:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
29/tcp    open  smtp         Postfix smtpd
|_smtp-command: setlocaldomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-cert: Subject: commonName=ubuntu@84-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-10T14:07:45
|_ssl2:
|_  SSLv2 supported
|_  ciphers:
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_DES_192_CBC3_CBC_WITH_MD5
|_ssl-date: 2026-02-11T17:10:14+00:00; 0s from scanner time.
53/tcp    open  domain       ISC BIND 9.4.2
|_dnsmid:
|_  bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
|_rpcinfo:
|_  program version port/proto service
|_  100000 2 111/tcp rpcbind
|_  100000 2 111/udp rpcbind
|_  100003 2,3,4 2049/tcp nfs
|_  100003 2,3,4 2049/udp nfs
|_  100005 1,2,3 35500/tcp mountd
|_  100005 1,2,3 58105/udp mountd
|_  100021 1,3,4 59848/tcp nlockmgr
|_  100021 1,3,4 59549/udp nlockmgr
|_  100024 1 37386/udp status
|_  100024 1 41677/tcp status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.28-Debian (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshexec
513/tcp   open  login        netkit-rsh rshd
514/tcp   open  shell        netkit-rsh rshd
1899/tcp  open  java-rmi     GNU Classpath gmiRegistry
1924/tcp  open  bindshell    Metasploitable root shell

OS: Linux 2.6.9

```

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: ~
File Actions Edit View Help

root@kali:~# nmap -p- 192.168.56.181
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-11 22:41 IST
Nmap scan report for 192.168.56.181
Host is up (0.0010s latency).
Not shown: 65585 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
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  dingdlock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5986/tcp  open  vnc
6808/tcp  open  x11
6867/tcp  open  irc
6897/tcp  open  irc-u
8809/tcp  open  sip3
8186/tcp  open  unknown
8787/tcp  open  msgsrvr
95508/tcp open  unknown
97226/tcp open  unknown
61477/tcp open  unknown
57848/tcp open  unknown
NAC Address: 8818:27:72:87:3D (PCS 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.