Nmap Network Scanning Report

Lab Objective

To perform a network scan using **Nmap** against a vulnerable machine (Metasploitable) and identify open ports, running services, and potential vulnerabilities.

Lab Setup

- **Attacker Machine**: Kali Linux (Nmap pre-installed)
- **Target Machine**: Metasploitable 2
- **Network**: Host-Only / NAT (both VMs on the same network)

Step 1: Identify IP Addresses

Run on both machines:

```
ifconfig
```

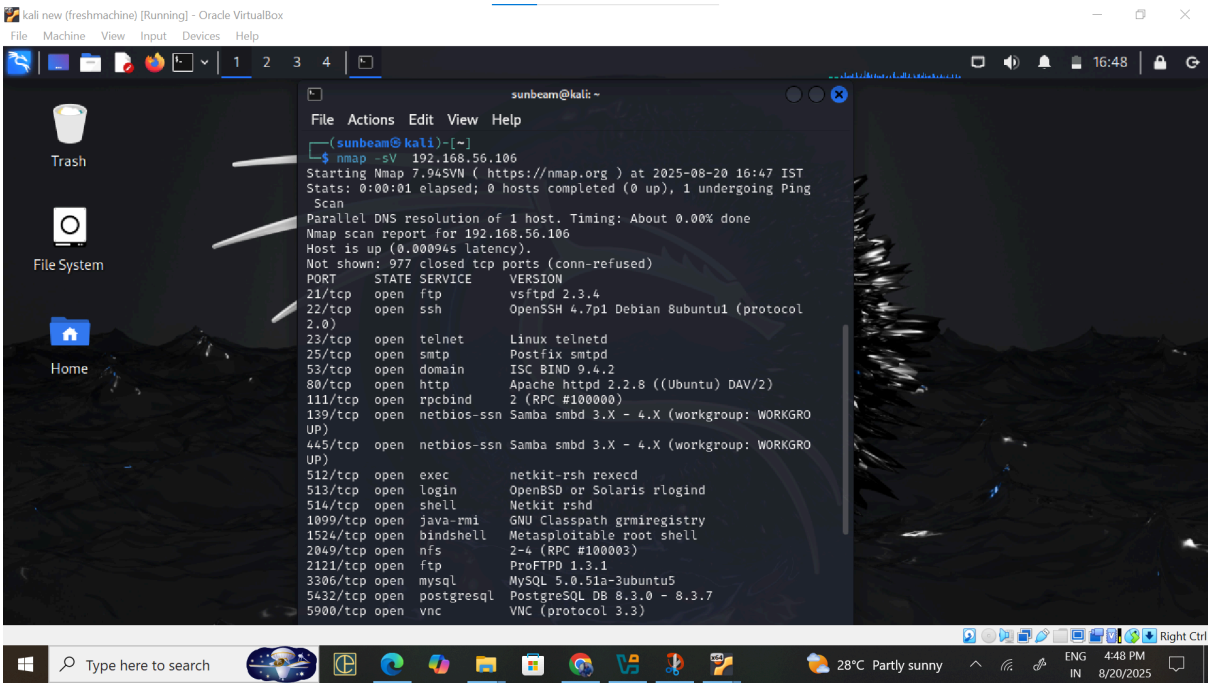
Example:

- Kali: `192.168.56.107`
- Metasploitable: `192.168.56.106`

Step 2:Service & Version Detection

Check if target is live:

```
nmap -sV 192.168.56.106
```

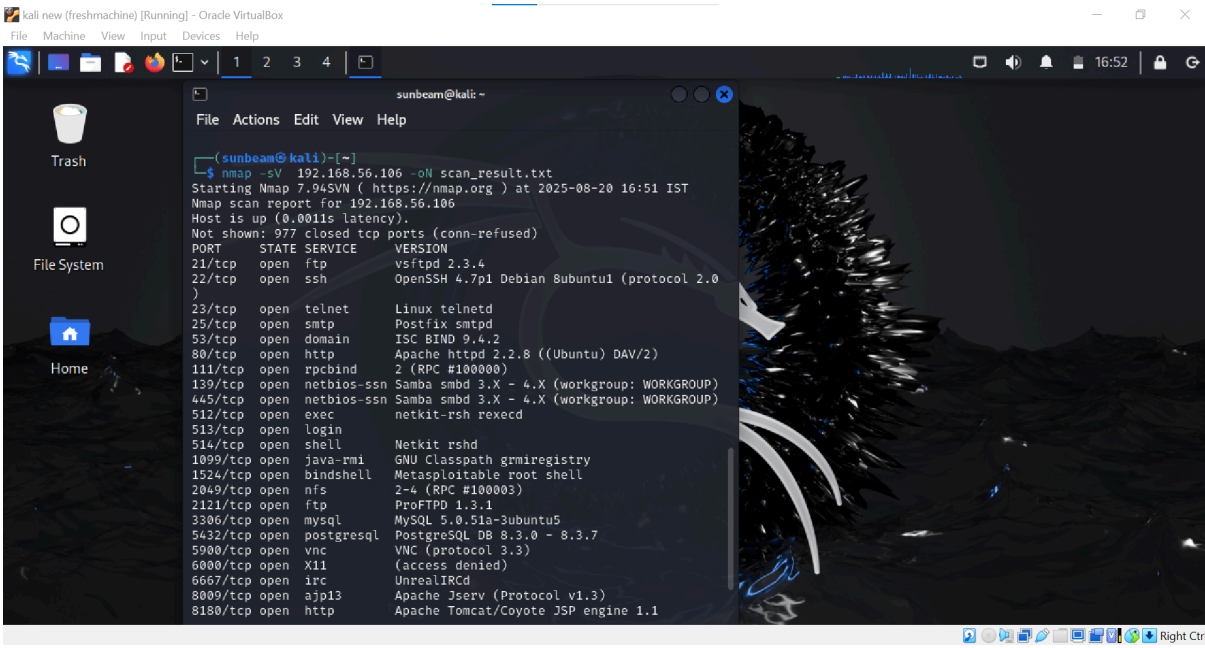


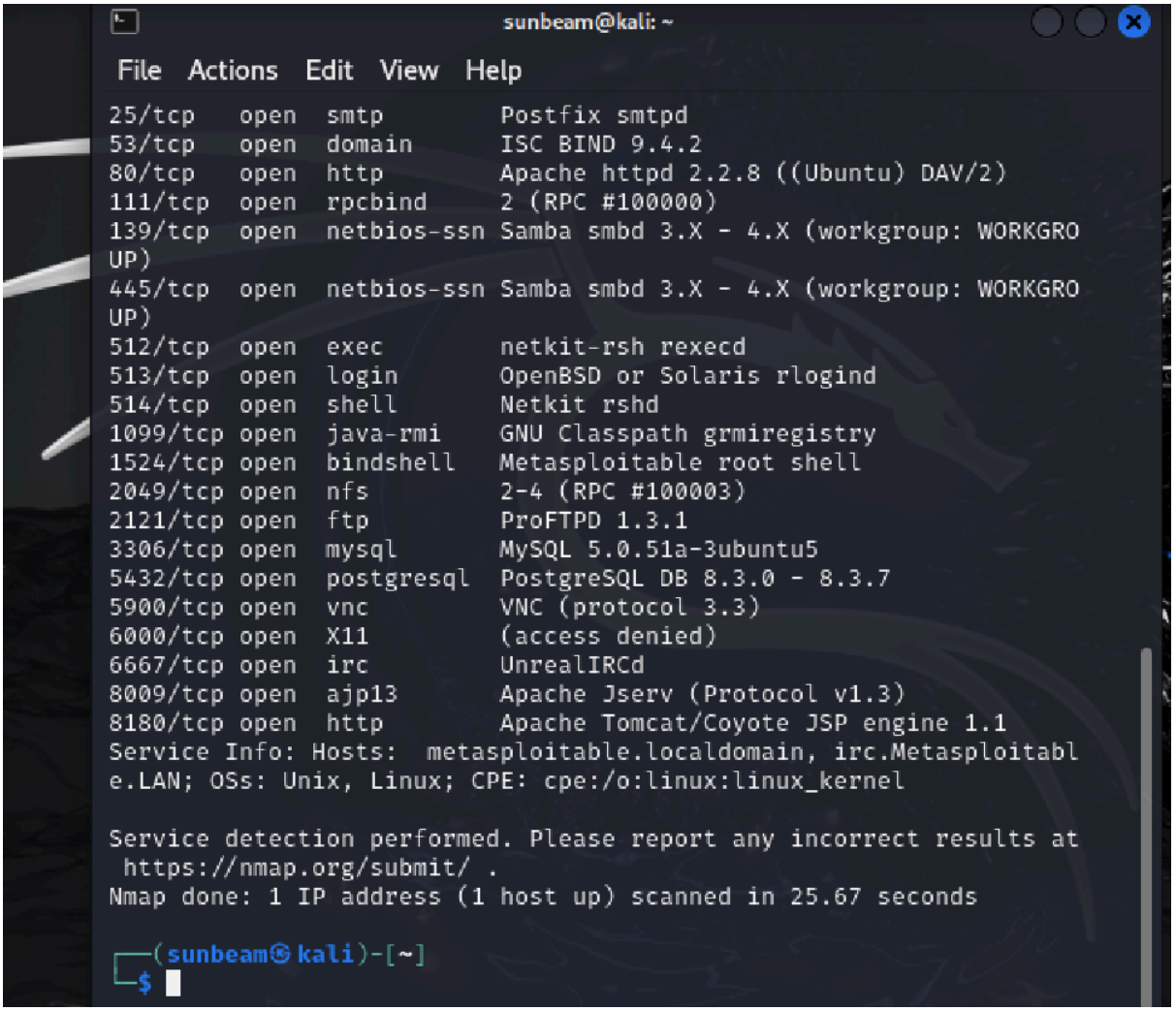
Step 3: Port Scanning

- **Basic Port Scan**
  `nmap 192.168.56.106`

- **Save Report**

  `nmap -A 192.168.56.102 -oN nmap_report.txt`


kali new (freshmachine) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
16:52
Trash
File System
Home
sunbeam@kali: ~
File Actions Edit View Help
(sunbeam㉿kali)-[~]
$ nmap -sV 192.168.56.106 -oN scan_result.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-08-20 16:51 IST
Nmap scan report for 192.168.56.106
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0
)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
Right Ctr


sunbeam@kali: ~
File Actions Edit View Help
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGRO
UP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGRO
UP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitabl
e.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.67 seconds
(sunbeam㉿kali)-[~]
$

Step 4: Analyze Results

Nmap output may show:

- Open ports (e.g., **21/FTP, 22/SSH, 80/HTTP, 3306/MySQL**)
- Running services (e.g., Apache, MySQL, SSH)
- Service versions (useful for finding vulnerabilities)
- OS guess (e.g., Linux 2.6.X)

Step 5: Reporting

Include in your report:

- 📸 **Screenshots** of Nmap scan results
- 🔎 **List of open ports and services**
- 🛠️ **Potential security issues**:
    - FTP/SSH weak authentication
    - Outdated Apache/MySQL versions
    - Unnecessary services running
    -

Conclusion

Nmap is a powerful tool for **network reconnaissance and vulnerability assessment**.
It helps identify open ports, services, and OS details, which are crucial for penetration testing and securing systems.