Nmap Scan Report – Metasploitable2 Lab

Author: Aman Jiwani

Date: 22 Sep 2025

Target: 192.168.56.104

Network: Host-only

Lab Setup

Lab Setup:

- **Attacker VM:** Kali Linux
- **Target VM:** Metasploitable2
- **Network Type:** Host-only
- **Tools Used:** Nmap

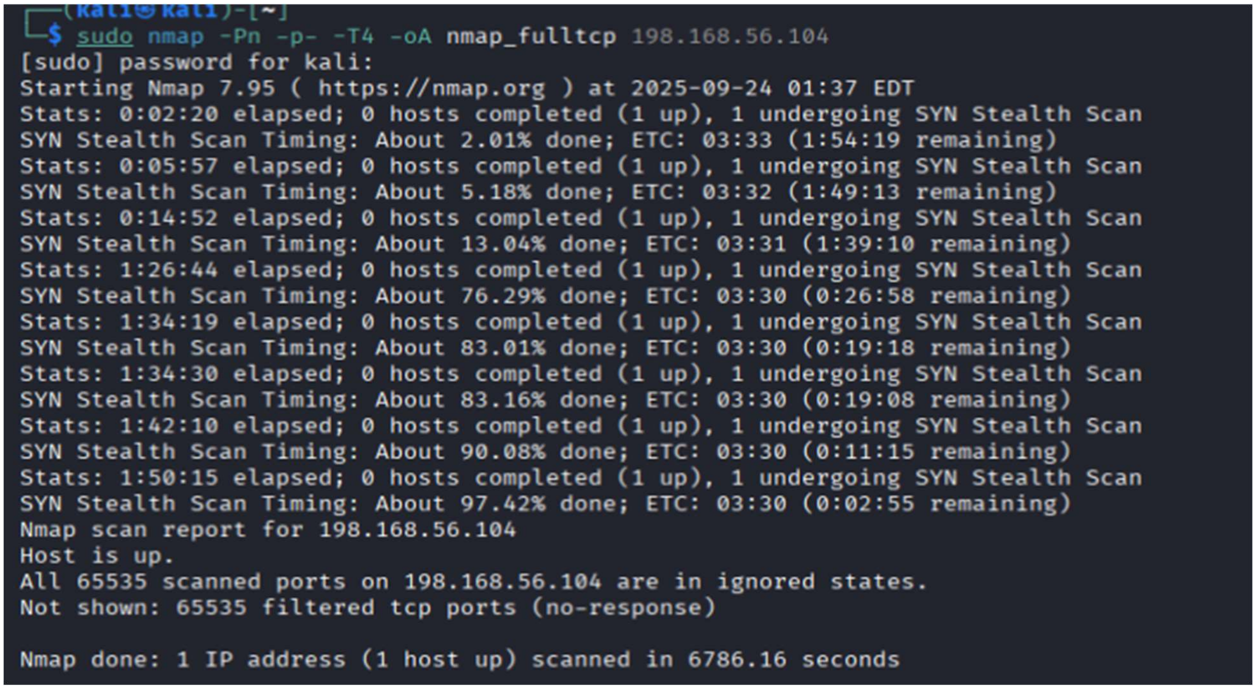
Purpose:

- Perform TCP & UDP scanning, service detection, OS fingerprinting.
- Identify open ports and risky services for analysis**.**

Scan Commands

1.TCP Targeted Scan:

sudo nmap -sS -sV -O -p- -T4 192.168.56.104

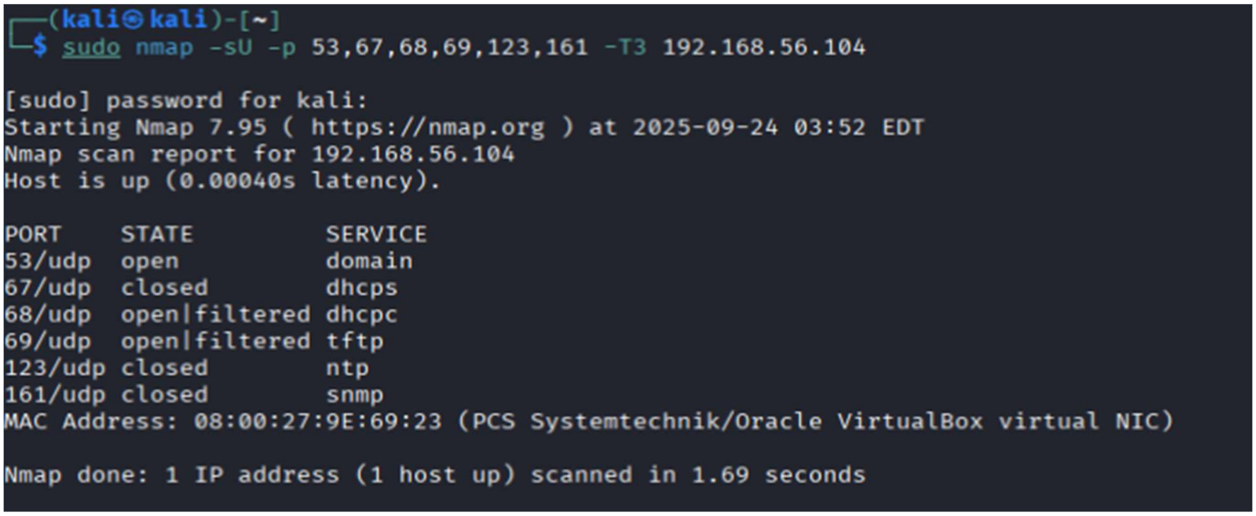


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -p- -T4 -oA nmap_fulltcp 198.168.56.104
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 01:37 EDT
Stats: 0:02:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.01% done; ETC: 03:33 (1:54:19 remaining)
Stats: 0:05:57 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.18% done; ETC: 03:32 (1:49:13 remaining)
Stats: 0:14:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 13.04% done; ETC: 03:31 (1:39:10 remaining)
Stats: 1:26:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 76.29% done; ETC: 03:30 (0:26:58 remaining)
Stats: 1:34:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.01% done; ETC: 03:30 (0:19:18 remaining)
Stats: 1:34:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.16% done; ETC: 03:30 (0:19:08 remaining)
Stats: 1:42:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.08% done; ETC: 03:30 (0:11:15 remaining)
Stats: 1:50:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 97.42% done; ETC: 03:30 (0:02:55 remaining)
Nmap scan report for 198.168.56.104
Host is up.
All 65535 scanned ports on 198.168.56.104 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 6786.16 seconds
```

- -sS: Stealth SYN scan
- -sV: Service version detection
- -O: OS detection
- -p-: Scan all ports
- -T4: Faster scan

2. UDP Targeted Scan:

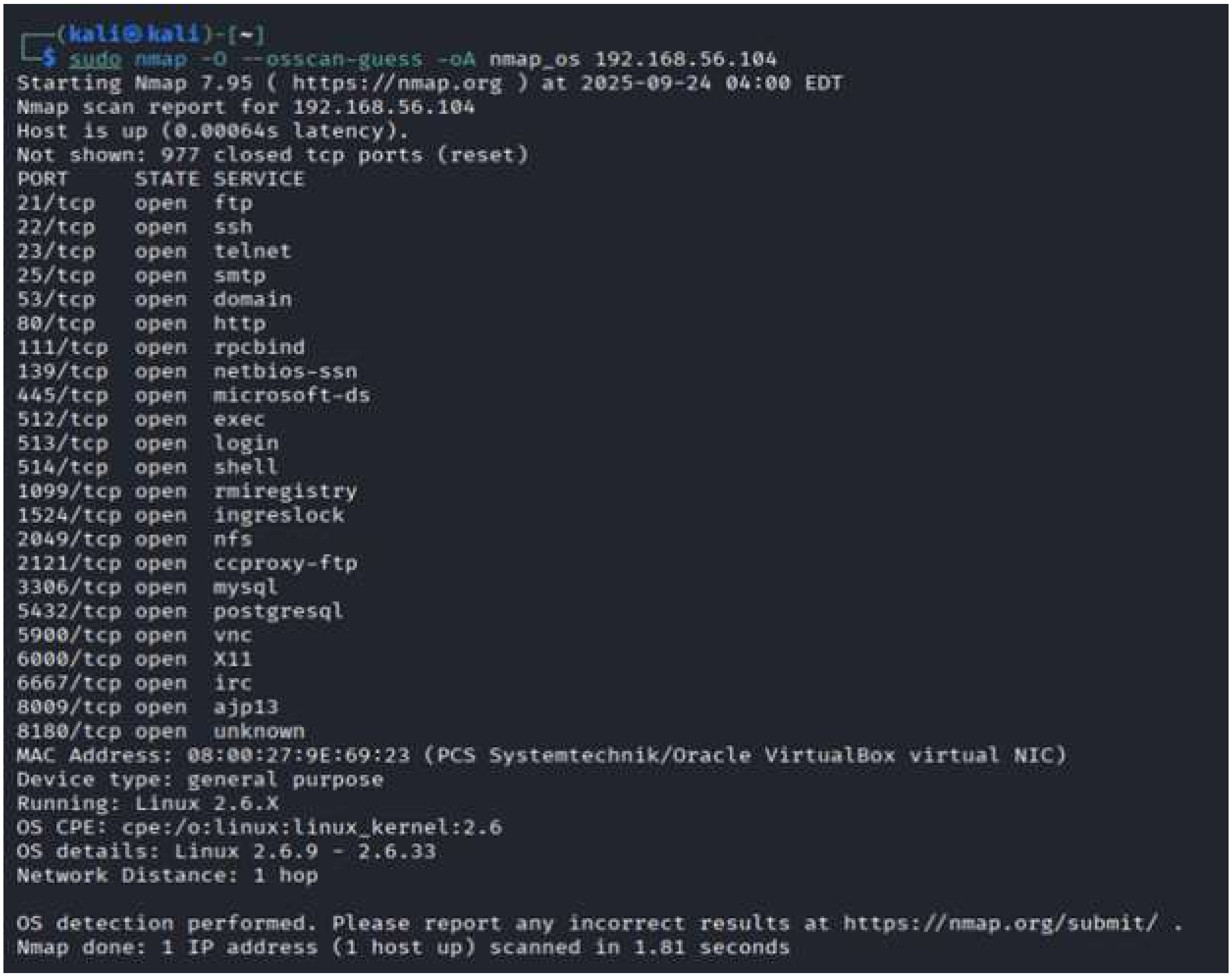
sudo nmap -sU -p 53,67,68,69,123,161 -T3 192.168.56.104



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -p 53,67,68,69,123,161 -T3 192.168.56.104

[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 03:52 EDT
Nmap scan report for 192.168.56.104
Host is up (0.00040s latency).

PORT    STATE         SERVICE
53/udp  open          domain
67/udp  closed        dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
123/udp closed        ntp
161/udp closed        snmp
MAC Address: 08:00:27:9E:69:23 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
```

- -sU: UDP scan
- -p <ports>: Common UDP ports
- -T3: Moderate speed

3.OS Detection

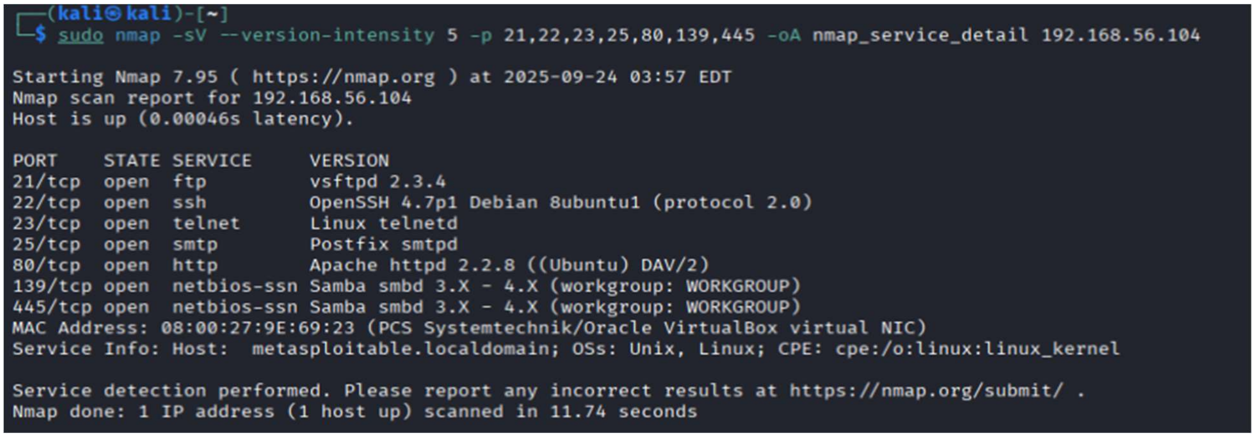


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O --osscan-guess -oA nmap_os 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 04:00 EDT
Nmap scan report for 192.168.56.104
Host is up (0.00064s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:9E:69:23 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
```

OS Detection Info:

- Output from `-O` showing detected OS

4.Service Version



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV --version-intensity 5 -p 21,22,23,25,80,139,445 -oA nmap_service_detail 192.168.56.104

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 03:57 EDT
Nmap scan report for 192.168.56.104
Host is up (0.00046s latency).

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
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
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)
MAC Address: 08:00:27:9E:69:23 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host:  metasploitable.localdomain; 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 11.74 seconds
```

Service Version Info:

- Show output from -sV for key services (FTP, SSH, Telnet, HTTP, SMB).

Observations & Analysis

- **Critical ports:** FTP (21), Telnet (23) – attackers can exploit easily
- **High risk:** SSH, SMB – potential brute-force or misconfiguration exploitation
- **Medium risk:** HTTP – outdated Apache version
- **UDP services:** DNS & NTP – can be abused for info or DoS

Attacker Perspective:

- An attacker can use this info to plan vulnerabilities:
    1. Identify running services
    2. Target vulnerable ports
    3. Exploit for unauthorized access, DoS, or data theft

Recommendations:

- Close unnecessary ports
- Patch vulnerable services
- Monitor exposed services closely

Summary

- **Target:** 192.168.56.104
- **Tools:** Nmap TCP/UDP scans
- **Key Findings**: Open ports: 21, 23, 22, 139, 445; FTP & Telnet highly risky
- **Learning Outcome:** Hands-on understanding of reconnaissance, scanning, and attack surface