Nmap Scan Report

1. Objective

To install and run Nmap on a Kali Linux machine, perform scans on the local network, identify open ports and services, and document the significance of each.

2. Environment

- Host OS: Kali Linux (VM in VirtualBox)
- Target: Local network hosts in 10.255.64.0/24
- Nmap version: 7.95

3. Commands Used

Basic Service Scan:

```
nmap -sV 10.255.64.0/24
```

Advanced Scan:

```
nmap -A <target_ip>
```

-sV: Detects service/version info.
-A: Enables OS detection, version detection, script scanning, and traceroute.

4. Findings

Target IP	Open Port	Protocol	Service / Version	Significance
10.255.64.48	—	—	All filtered (firewall)	Likely protected by firewall, no visible services.
10.255.64.211	53	TCP	dnsmasq 2.51	Used for DNS resolution. Outdated version may be vul
10.255.64.85	—	—	All closed	No active services found.

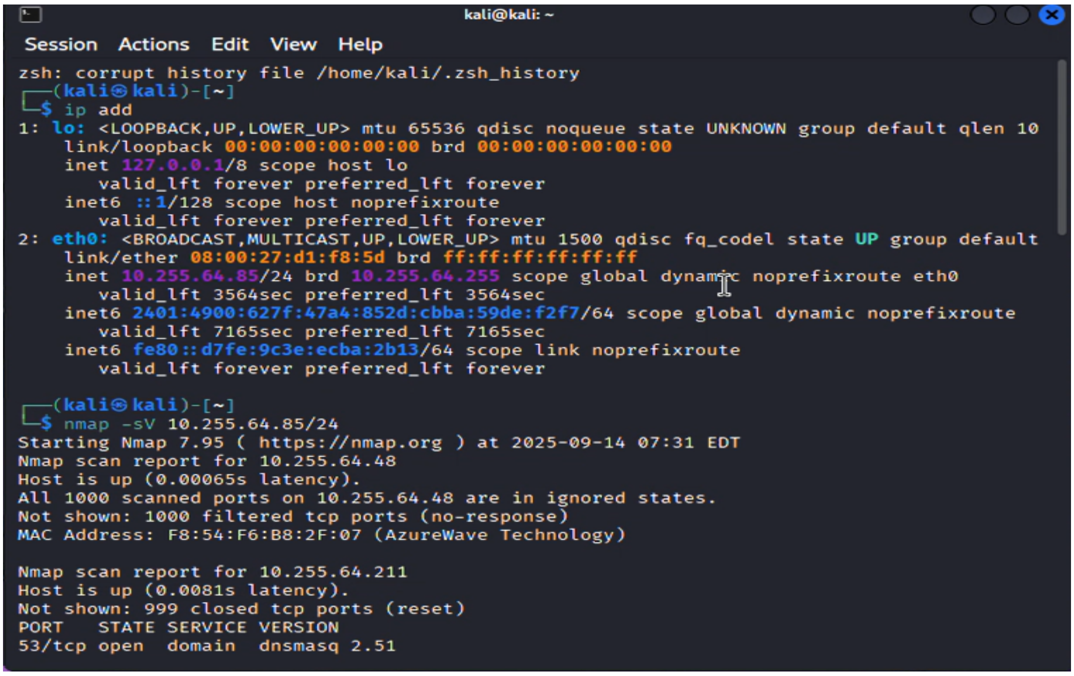
5. Significance of Discovered Ports

- Port 53 (DNS): Critical for resolving hostnames. Outdated versions (e.g., dnsmasq 2.51) may contain security vulnerabilities. - Filtered Ports: Indicate the presence of a firewall, which protects the host by hiding services. - Closed Ports: Means no active services are running on that host.

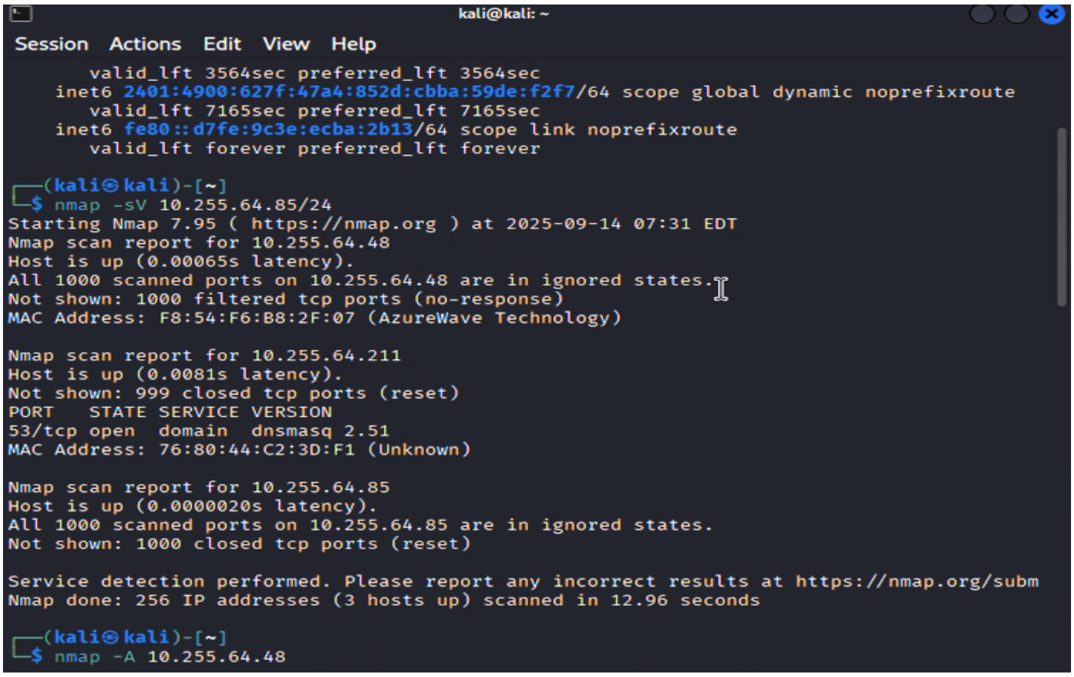
6. Conclusion

The scan revealed one host running a DNS service (dnsmasq 2.51), which may be outdated and vulnerable. Another host was protected by a firewall, and one host had no active services. It is recommended to update the DNS service, maintain firewall protections, and ensure unused services remain closed.

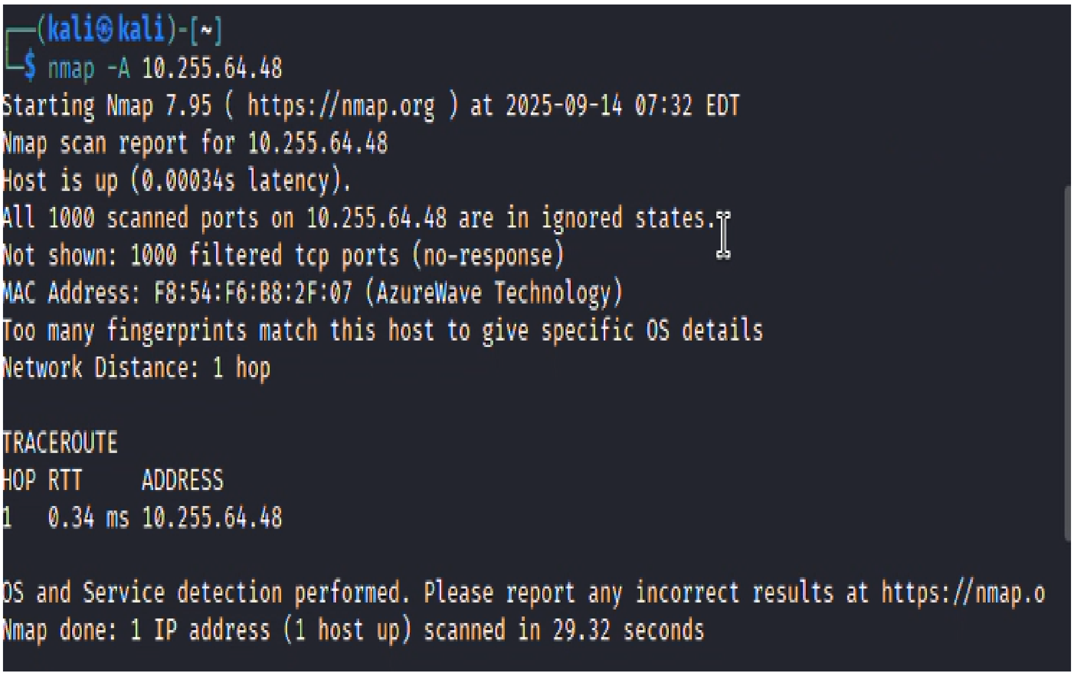
Appendix: Nmap Scan Screenshots



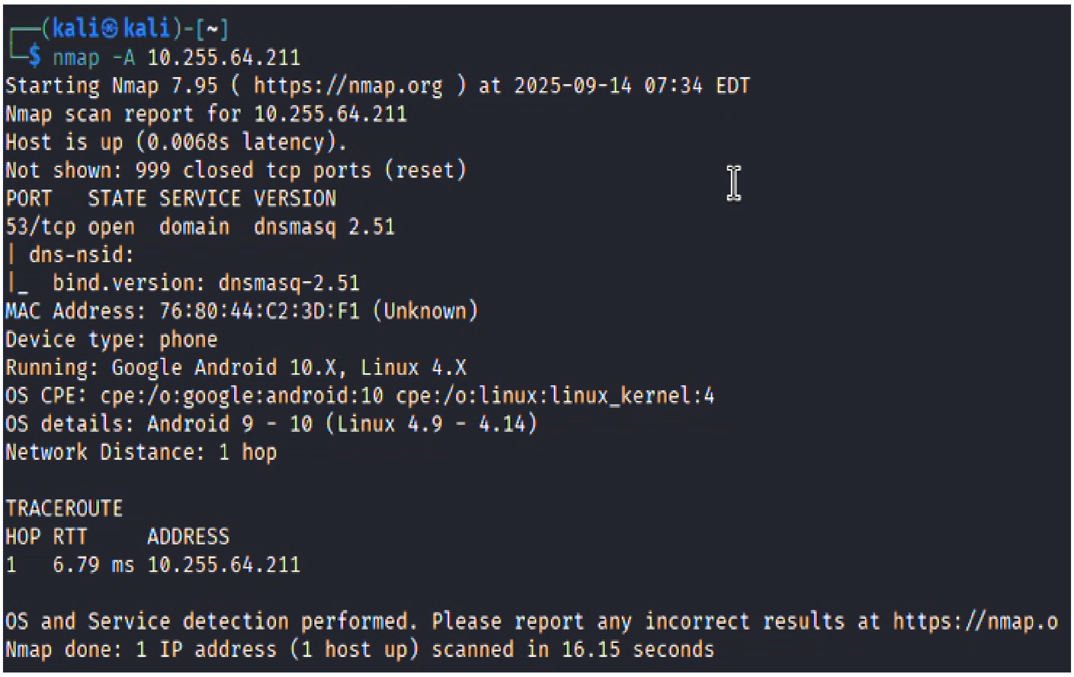
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 10.255.64.85/24 brd 10.255.64.255 scope global dynamic noprefixroute eth0
       valid_lft 3564sec preferred_lft 3564sec
    inet6 2401:4900:627f:47a4:852d:cbba:59de:f2f7/64 scope global dynamic noprefixroute
       valid_lft 7165sec preferred_lft 7165sec
    inet6 fe80::d7fe:9c3e:ecba:2b13/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.255.64.85/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 07:31 EDT
Nmap scan report for 10.255.64.48
Host is up (0.00065s latency).
All 1000 scanned ports on 10.255.64.48 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F8:54:F6:B8:2F:07 (AzureWave Technology)

Nmap scan report for 10.255.64.211
Host is up (0.0081s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
```



```
       valid_lft 3564sec preferred_lft 3564sec
    inet6 2401:4900:627f:47a4:852d:cbba:59de:f2f7/64 scope global dynamic noprefixroute
       valid_lft 7165sec preferred_lft 7165sec
    inet6 fe80::d7fe:9c3e:ecba:2b13/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.255.64.85/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 07:31 EDT
Nmap scan report for 10.255.64.48
Host is up (0.00065s latency).
All 1000 scanned ports on 10.255.64.48 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F8:54:F6:B8:2F:07 (AzureWave Technology)

Nmap scan report for 10.255.64.211
Host is up (0.0081s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
MAC Address: 76:80:44:C2:3D:F1 (Unknown)

Nmap scan report for 10.255.64.85
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.255.64.85 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/subm
Nmap done: 256 IP addresses (3 hosts up) scanned in 12.96 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -A 10.255.64.48
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.255.64.48
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 07:32 EDT
Nmap scan report for 10.255.64.48
Host is up (0.00034s latency).
All 1000 scanned ports on 10.255.64.48 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F8:54:F6:B8:2F:07 (AzureWave Technology)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.34 ms 10.255.64.48

OS and Service detection performed. Please report any incorrect results at https://nmap.o
Nmap done: 1 IP address (1 host up) scanned in 29.32 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.255.64.211
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 07:34 EDT
Nmap scan report for 10.255.64.211
Host is up (0.0068s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
| dns-nsid:
|_  bind.version: dnsmasq-2.51
MAC Address: 76:80:44:C2:3D:F1 (Unknown)
Device type: phone
Running: Google Android 10.X, Linux 4.X
OS CPE: cpe:/o:google:android:10 cpe:/o:linux:linux_kernel:4
OS details: Android 9 - 10 (Linux 4.9 - 4.14)
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   6.79 ms 10.255.64.211

OS and Service detection performed. Please report any incorrect results at https://nmap.o
Nmap done: 1 IP address (1 host up) scanned in 16.15 seconds
```