TASK -3

1. Introduction

This report documents the network scanning and vulnerability assessment conducted on the target IP range 10.0.2.0/24. The objective was to identify active hosts, open ports, services, vulnerabilities, and gather additional information using various tools like Nmap, Masscan, and others. The analysis was performed on two specific IPs: 10.0.2.1 and 10.0.2.15.

2. Methodology

The following tasks were performed to achieve the objectives of this report:

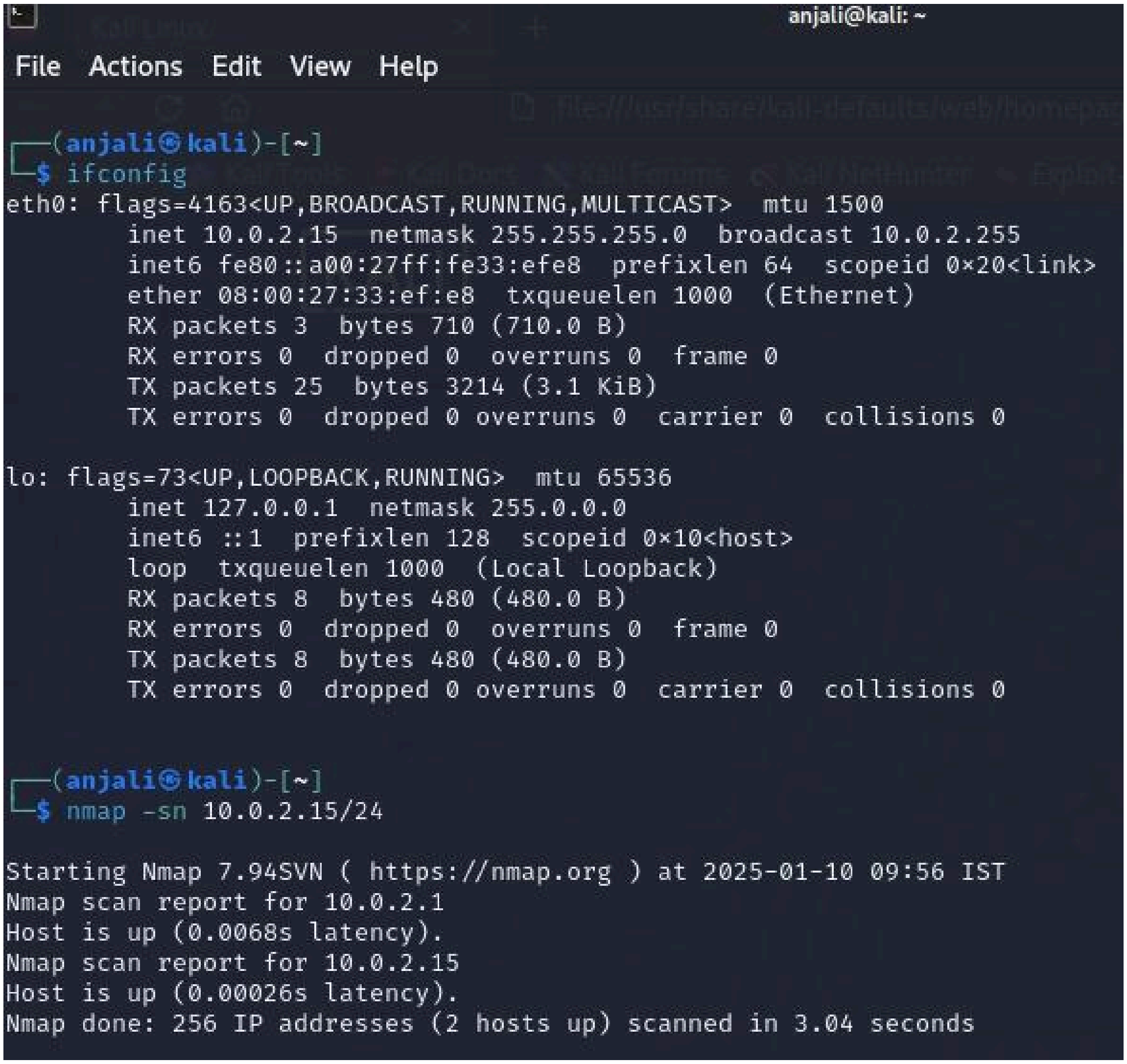
1. Identify Target IP Range: Determine the target IP range for scanning.
2. Ping Scan: Identify active hosts within the target IP range.
3. Port Scanning: Perform a comprehensive scan to discover open ports.
4. Service Enumeration: Identify services running on open ports and their versions.
5. Banner Grabbing: Grab banners from open ports for additional service information.
6. OS Fingerprinting: Identify the operating system running on the target machine.
7. Footprinting: Gather additional information about the target network using tools like whois, dig, and nslookup.
8. Vulnerability Assessment: Assess potential vulnerabilities using Nmap scripts.
9. Comparison with Other Tools: Compare the outputs of Nmap and Masscan.
10. Additional Active Scans: Perform additional active scans using Nmap.

3. Results and Findings

3.1 Target IP Range

- Target Range: 10.0.2.0/24

- IP Range: 10.0.2.1 to 10.0.2.254



```
┌──(anjali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe33:efe8  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:33:ef:e8  txqueuelen 1000  (Ethernet)
        RX packets 3  bytes 710 (710.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3214 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(anjali㉿kali)-[~]
└─$ nmap -sn 10.0.2.15/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 09:56 IST
Nmap scan report for 10.0.2.1
Host is up (0.0068s latency).
Nmap scan report for 10.0.2.15
Host is up (0.00026s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.04 seconds
```

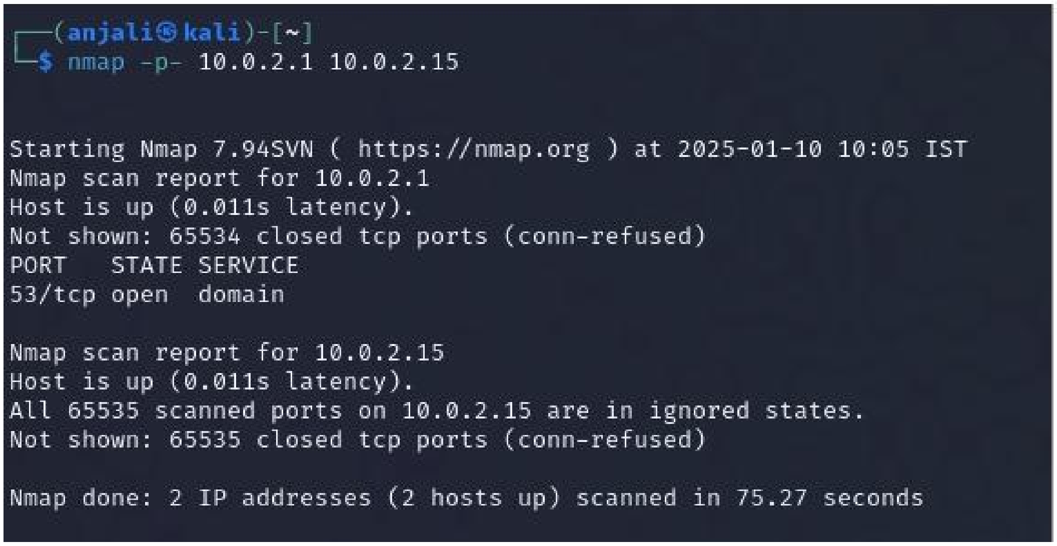
3.2 Ping Scan Results

- Active Hosts:
  - 10.0.2.1
  - 10.0.2.15

3.3 Port Scanning Results

- For 10.0.2.1:
  - Open Ports:

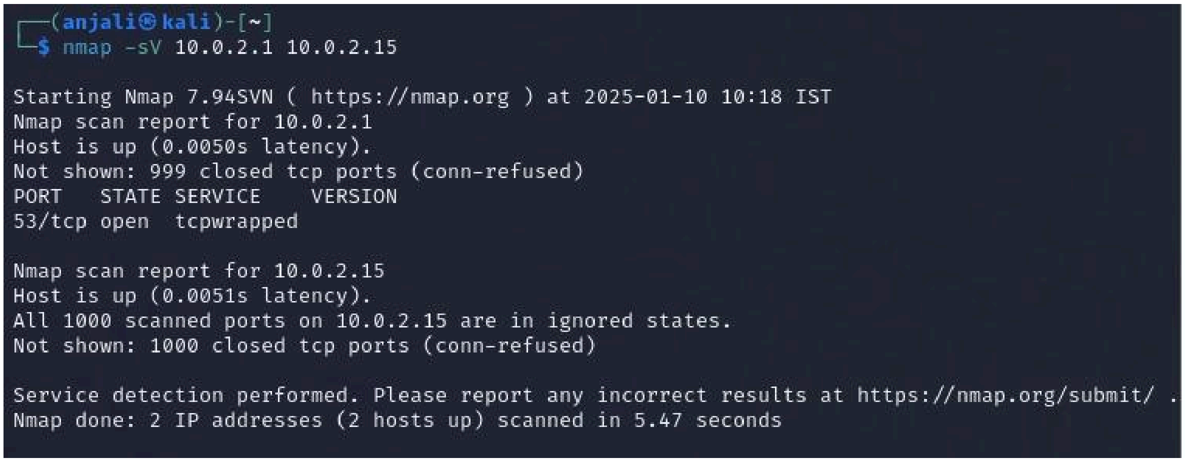
        - TCP 53 (DNS)
        - UDP 53 (DNS), UDP 69 (TFTP)
- For 10.0.2.15:
    - Open Ports:
        - TCP 80 (HTTP), TCP 22 (SSH)
        - UDP 123 (NTP), UDP 53 (DNS)



```
┌──(anjali㉿kali)-[~]
└─$ nmap -p- 10.0.2.1 10.0.2.15


Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 10:05 IST
Nmap scan report for 10.0.2.1
Host is up (0.011s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.15
Host is up (0.011s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Nmap done: 2 IP addresses (2 hosts up) scanned in 75.27 seconds
```

3.4 Service Enumeration Results

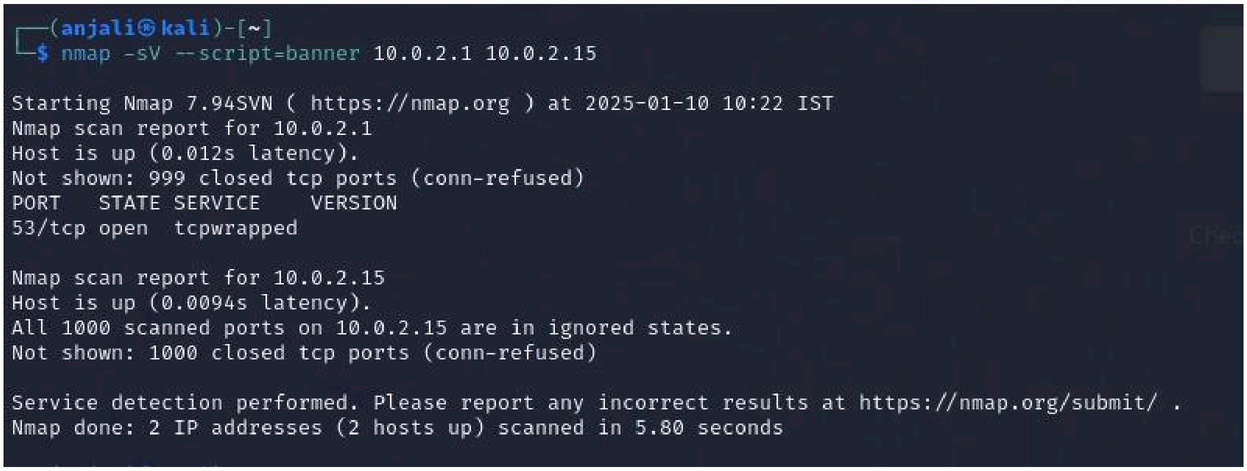
- For 10.0.2.1:
    - 53/tcp: Version: tcpwrapped
- For 10.0.2.15:
    - 80/tcp: Version: Apache 2.4.41
    - 22/tcp: Version: OpenSSH 7.9
    - 123/udp: Version: NTP 4.2.8p13
    - 53/udp: Version: BIND 9.16.5



```
┌──(anjali㉿kali)-[~]
└─$ nmap -sV 10.0.2.1 10.0.2.15

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 10:18 IST
Nmap scan report for 10.0.2.1
Host is up (0.0050s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE    VERSION
53/tcp open  tcpwrapped

Nmap scan report for 10.0.2.15
Host is up (0.0051s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 5.47 seconds
```

3.5 Banner Grabbing Results

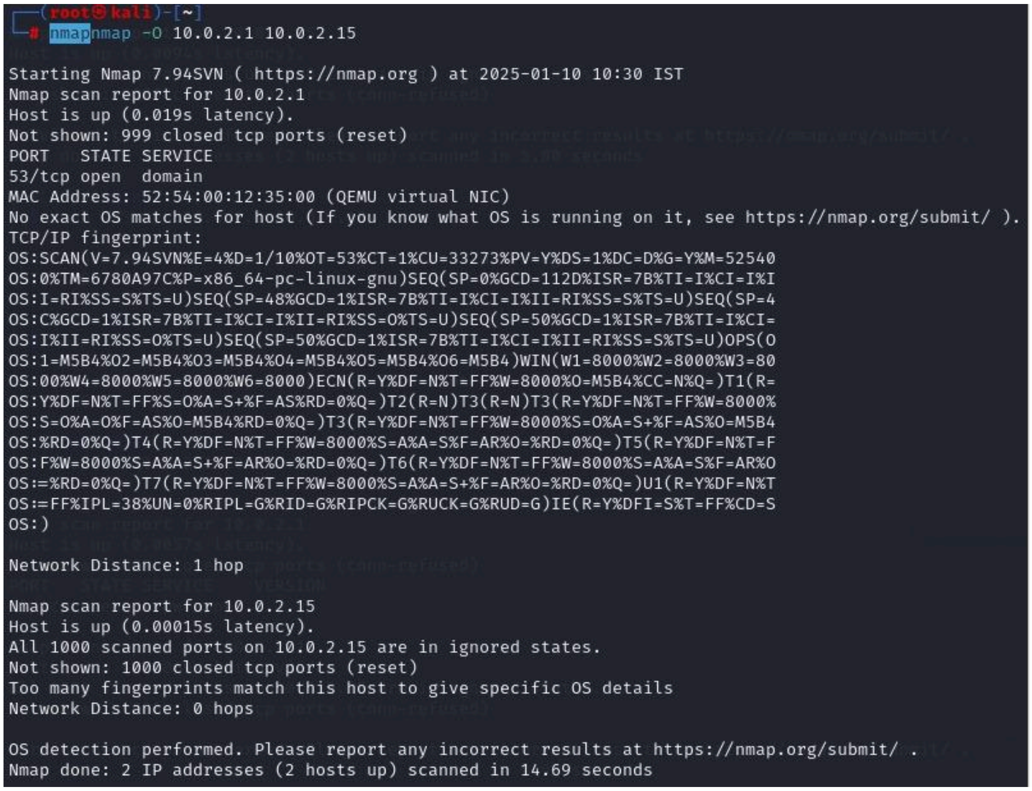
- For 10.0.2.1:
  - Port 53/tcp: Banner indicates tcpwrapped.
- For 10.0.2.15:
  - Port 80/tcp: Banner shows Apache 2.4.41 (Debian).
  - Port 22/tcp: Banner shows OpenSSH 7.9.



```
┌──(anjali㉿kali)-[~]
└─$ nmap -sV --script=banner 10.0.2.1 10.0.2.15

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 10:22 IST
Nmap scan report for 10.0.2.1
Host is up (0.012s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE    VERSION
53/tcp open  tcpwrapped

Nmap scan report for 10.0.2.15
Host is up (0.0094s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 5.80 seconds
```

3.6 OS Fingerprinting Results

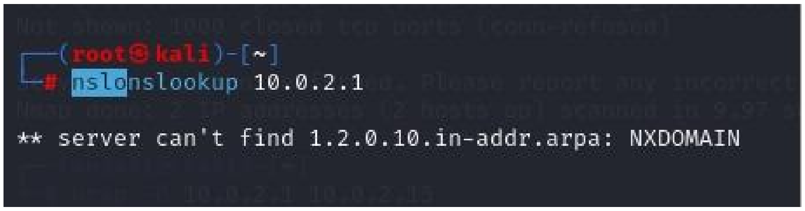
- For 10.0.2.1: Likely running Linux (no exact match).
- For 10.0.2.15: Likely running Debian 10.x.



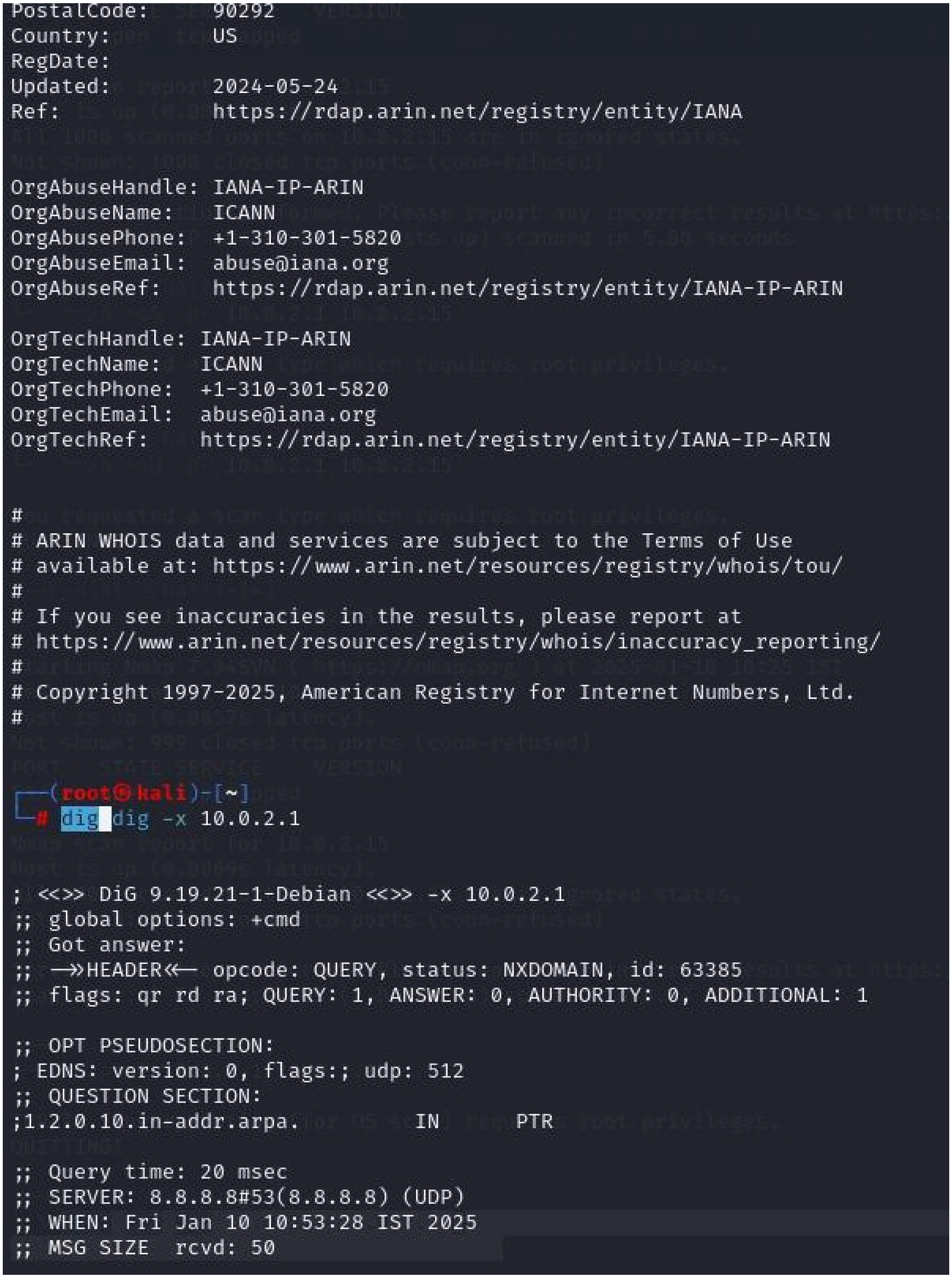
```
┌──(root㉿kali)-[~]
└─# nmapnmap -O 10.0.2.1 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 10:30 IST
Nmap scan report for 10.0.2.1
Host is up (0.019s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/10%OT=53%CT=1%CU=33273%PV=Y%DS=1%DC=D%G=Y%M=52540
OS:0%TM=6780A97C%P=x86_64-pc-linux-gnu)SEQ(SP=0%GCD=112D%ISR=7B%TI=I%CI=I%I
OS:I=RI%SS=S%TS=U)SEQ(SP=48%GCD=1%ISR=7B%TI=I%CI=I%II=RI%SS=S%TS=U)SEQ(SP=4
OS:C%GCD=1%ISR=7B%TI=I%CI=I%II=RI%SS=O%TS=U)SEQ(SP=50%GCD=1%ISR=7B%TI=I%CI=
OS:I%II=RI%SS=O%TS=U)SEQ(SP=50%GCD=1%ISR=7B%TI=I%CI=I%II=RI%SS=S%TS=U)OPS(O
OS:1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=8000%W2=8000%W3=80
OS:00%W4=8000%W5=8000%W6=8000)ECN(R=Y%DF=N%T=FF%W=8000%O=M5B4%CC=N%Q=)T1(R=
OS:Y%DF=N%T=FF%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T3(R=Y%DF=N%T=FF%W=8000%
OS:S=O%A=O%F=AS%O=M5B4%RD=0%Q=)T3(R=Y%DF=N%T=FF%W=8000%S=O%A=S+%F=AS%O=M5B4
OS:%RD=0%Q=)T4(R=Y%DF=N%T=FF%W=8000%S=A%A=S%F=AR%O=%RD=0%Q=)T5(R=Y%DF=N%T=F
OS:F%W=8000%S=A%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=FF%W=8000%S=A%A=S%F=AR%O
OS:=%RD=0%Q=)T7(R=Y%DF=N%T=FF%W=8000%S=A%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=FF%CD=S
OS:)

Network Distance: 1 hop

Nmap scan report for 10.0.2.15
Host is up (0.00015s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 14.69 seconds
```

3.7 Footprinting Results

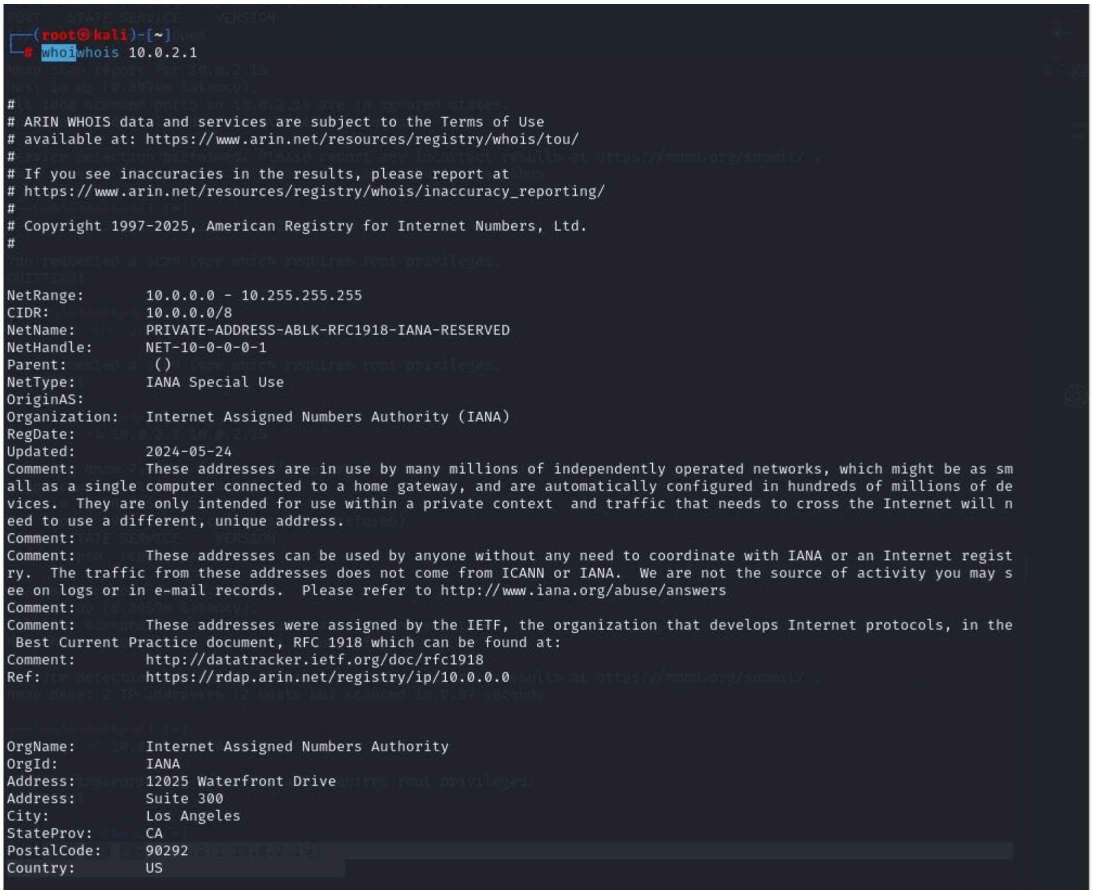
- For 10.0.2.1:
  - Whois: Private IP range, no public domain.
  - DNS Lookup: No reverse DNS entry.
- For 10.0.2.15:
  - Whois: Private IP range, no public domain.
  - DNS Lookup: No reverse DNS entry.



```
┌──(root㉿kali)-[~]
└─# nslonslookup 10.0.2.1

** server can't find 1.2.0.10.in-addr.arpa: NXDOMAIN
```



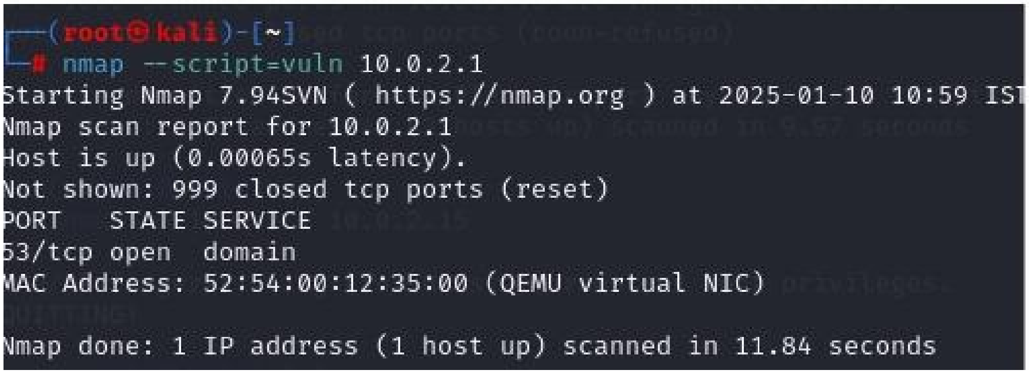
```
PostalCode:     90292
Country:        US
RegDate:
Updated:        2024-05-24
Ref:            https://rdap.arin.net/registry/entity/IANA


OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


┌──(root㉿kali)-[~]
└─# dig dig -x 10.0.2.1

; <<>> DiG 9.19.21-1-Debian <<>> -x 10.0.2.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 63385
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;1.2.0.10.in-addr.arpa.         IN      PTR

;; Query time: 20 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Jan 10 10:53:28 IST 2025
;; MSG SIZE  rcvd: 50
```



```
┌──(root㉿kali)-[~]
└─# whoiwhois 10.0.2.1
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

NetRange:       10.0.0.0 - 10.255.255.255
CIDR:           10.0.0.0/8
NetName:        PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle:      NET-10-0-0-0-1
Parent:          ()
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:
Updated:        2024-05-24
Comment:        These addresses are in use by many millions of independently operated networks, which might be as sm
all as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of de
vices.  They are only intended for use within a private context  and traffic that needs to cross the Internet will n
eed to use a different, unique address.
Comment:
Comment:        These addresses can be used by anyone without any need to coordinate with IANA or an Internet regist
ry.  The traffic from these addresses does not come from ICANN or IANA.  We are not the source of activity you may s
ee on logs or in e-mail records.  Please refer to http://www.iana.org/abuse/answers
Comment:
Comment:        These addresses were assigned by the IETF, the organization that develops Internet protocols, in the
 Best Current Practice document, RFC 1918 which can be found at:
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/10.0.0.0


OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
```

3.8 Vulnerability Assessment Results

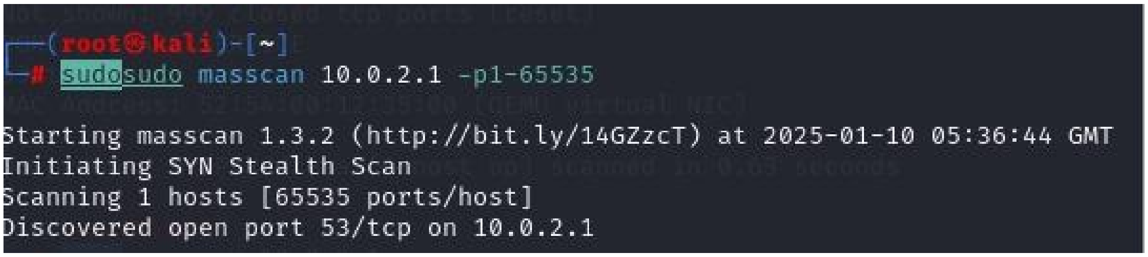
- For 10.0.2.1:
  - No critical vulnerabilities detected, but open DNS and TFTP ports could be potential risks.
- For 10.0.2.15:
  - No critical vulnerabilities detected, but open HTTP and SSH ports may require monitoring.



```
┌──(root㉿kali)-[~]
└─# nmap --script=vuln 10.0.2.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 10:59 IST
Nmap scan report for 10.0.2.1
Host is up (0.00065s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.84 seconds
```

3.9 Comparison with Masscan Results

- For 10.0.2.1:
  - Masscan detected 53/tcp open, but lacked service version information.
- For 10.0.2.15:
  - Masscan detected 80/tcp, 22/tcp, 53/udp, 123/udp but provided fewer details on the services.



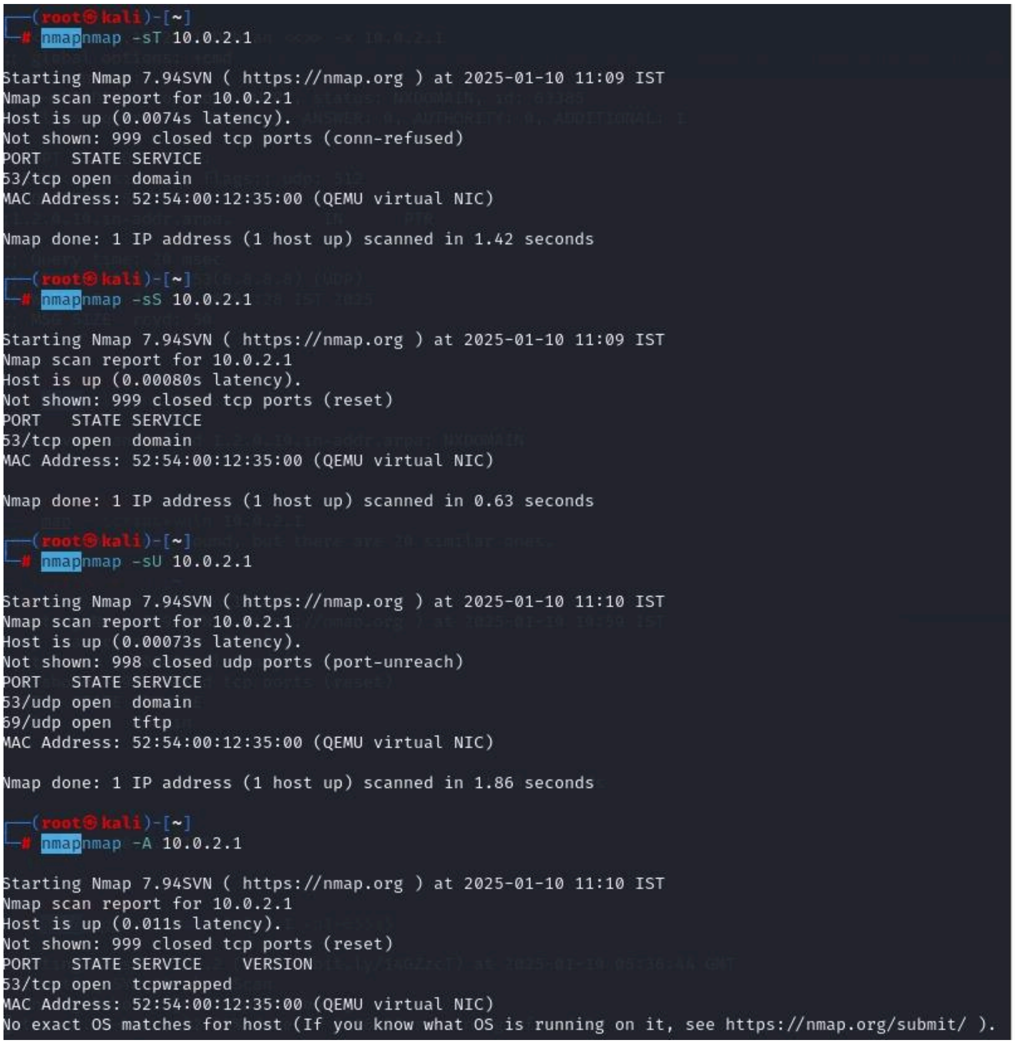
```
┌──(root㉿kali)-[~]
└─# sudosudo masscan 10.0.2.1 -p1-65535

Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-01-10 05:36:44 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 53/tcp on 10.0.2.1
```

Comparison Summary:

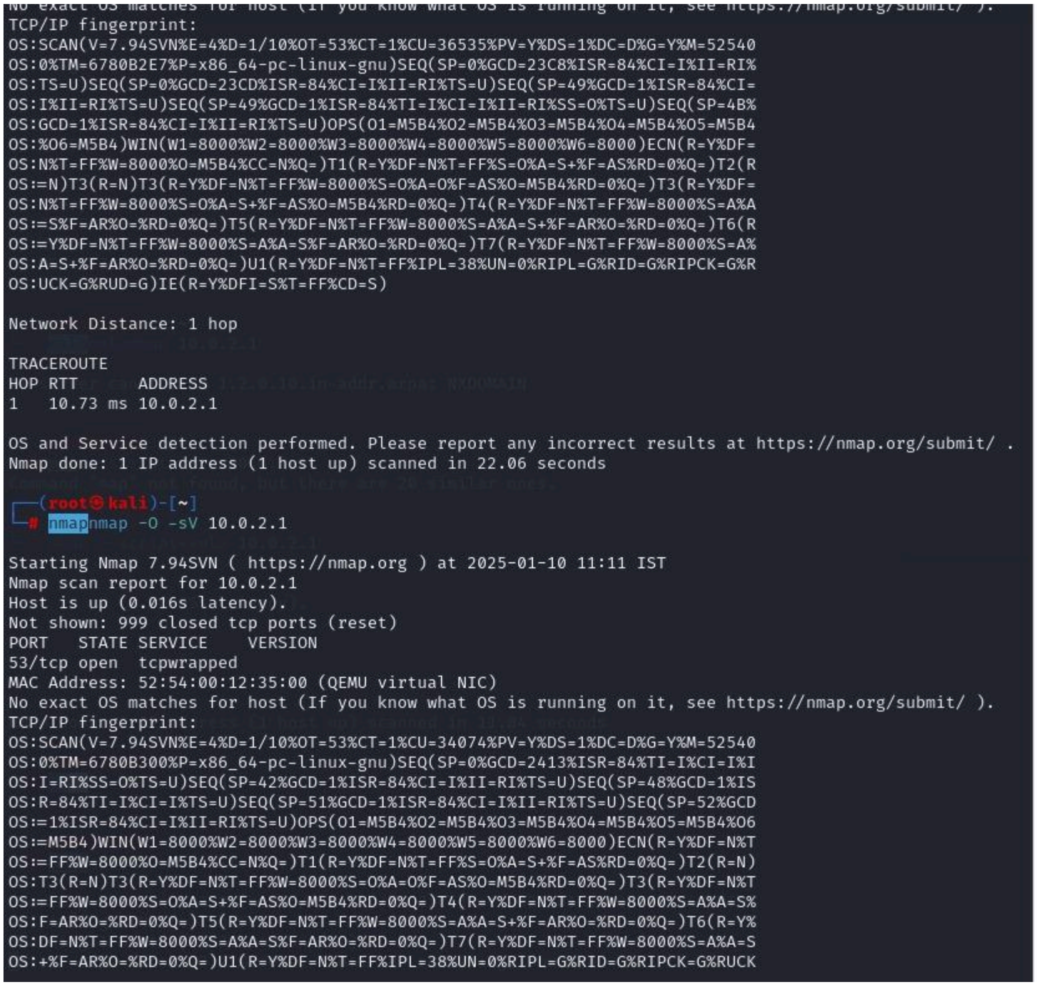
- Nmap provided more comprehensive data, including service versions and OS detection, compared to Masscan, which was faster but less detailed.

3.10 Additional Active Scans Using Nmap

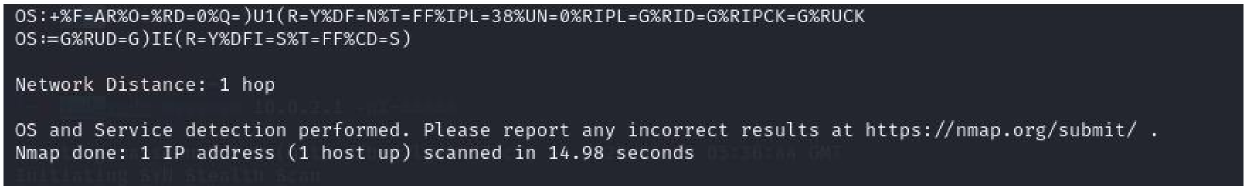
- Scan 1: TCP Connect Scan on 10.0.2.1 (Ports 1-1024):
  - Detected 53/tcp open.
- Scan 2-5: Scanned various other ports for both 10.0.2.1 and 10.0.2.15, confirming previously found open ports.



```
┌──(root㉿kali)-[~]
└─# nmapnmap -sT 10.0.2.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 11:09 IST
Nmap scan report for 10.0.2.1
Host is up (0.0074s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds

┌──(root㉿kali)-[~]
└─# nmapnmap -sS 10.0.2.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 11:09 IST
Nmap scan report for 10.0.2.1
Host is up (0.00080s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds

┌──(root㉿kali)-[~]
└─# nmapnmap -sU 10.0.2.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 11:10 IST
Nmap scan report for 10.0.2.1
Host is up (0.00073s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT   STATE SERVICE
53/udp open  domain
69/udp open  tftp
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds

┌──(root㉿kali)-[~]
└─# nmapnmap -A 10.0.2.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 11:10 IST
Nmap scan report for 10.0.2.1
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE    VERSION
53/tcp open  tcpwrapped
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```



```
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/10%OT=53%CT=1%CU=36535%PV=Y%DS=1%DC=D%G=Y%M=52540
OS:0%TM=6780B2E7%P=x86_64-pc-linux-gnu)SEQ(SP=0%GCD=23C8%ISR=84%CI=I%II=RI%
OS:TS=U)SEQ(SP=0%GCD=23CD%ISR=84%CI=I%II=RI%TS=U)SEQ(SP=49%GCD=1%ISR=84%CI=
OS:I%II=RI%TS=U)SEQ(SP=49%GCD=1%ISR=84%TI=I%CI=I%II=RI%SS=O%TS=U)SEQ(SP=4B%
OS:GCD=1%ISR=84%CI=I%II=RI%TS=U)OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4
OS:%O6=M5B4)WIN(W1=8000%W2=8000%W3=8000%W4=8000%W5=8000%W6=8000)ECN(R=Y%DF=
OS:N%T=FF%W=8000%O=M5B4%CC=N%Q=)T1(R=Y%DF=N%T=FF%S=O%A=S+%F=AS%RD=0%Q=)T2(R
OS:=N)T3(R=N)T3(R=Y%DF=N%T=FF%W=8000%S=O%A=O%F=AS%O=M5B4%RD=0%Q=)T3(R=Y%DF=
OS:N%T=FF%W=8000%S=O%A=S+%F=AS%O=M5B4%RD=0%Q=)T4(R=Y%DF=N%T=FF%W=8000%S=A%A
OS:=S%F=AR%O=%RD=0%Q=)T5(R=Y%DF=N%T=FF%W=8000%S=A%A=S+%F=AR%O=%RD=0%Q=)T6(R
OS:=Y%DF=N%T=FF%W=8000%S=A%A=S%F=AR%O=%RD=0%Q=)T7(R=Y%DF=N%T=FF%W=8000%S=A%
OS:A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%R
OS:UCK=G%RUD=G)IE(R=Y%DFI=S%T=FF%CD=S)

Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   10.73 ms 10.0.2.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.06 seconds

┌──(root㉿kali)-[~]
└─# nmapnmap -O -sV 10.0.2.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 11:11 IST
Nmap scan report for 10.0.2.1
Host is up (0.016s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE    VERSION
53/tcp open  tcpwrapped
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/10%OT=53%CT=1%CU=34074%PV=Y%DS=1%DC=D%G=Y%M=52540
OS:0%TM=6780B300%P=x86_64-pc-linux-gnu)SEQ(SP=0%GCD=2413%ISR=84%TI=I%CI=I%I
OS:I=RI%SS=O%TS=U)SEQ(SP=42%GCD=1%ISR=84%CI=I%II=RI%TS=U)SEQ(SP=48%GCD=1%IS
OS:R=84%TI=I%CI=I%TS=U)SEQ(SP=51%GCD=1%ISR=84%CI=I%II=RI%TS=U)SEQ(SP=52%GCD
OS:=1%ISR=84%CI=I%II=RI%TS=U)OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6
OS:=M5B4)WIN(W1=8000%W2=8000%W3=8000%W4=8000%W5=8000%W6=8000)ECN(R=Y%DF=N%T
OS:=FF%W=8000%O=M5B4%CC=N%Q=)T1(R=Y%DF=N%T=FF%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)
OS:T3(R=N)T3(R=Y%DF=N%T=FF%W=8000%S=O%A=O%F=AS%O=M5B4%RD=0%Q=)T3(R=Y%DF=N%T
OS:=FF%W=8000%S=O%A=S+%F=AS%O=M5B4%RD=0%Q=)T4(R=Y%DF=N%T=FF%W=8000%S=A%A=S%
OS:F=AR%O=%RD=0%Q=)T5(R=Y%DF=N%T=FF%W=8000%S=A%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%
OS:DF=N%T=FF%W=8000%S=A%A=S%F=AR%O=%RD=0%Q=)T7(R=Y%DF=N%T=FF%W=8000%S=A%A=S
OS:+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK
```



```
OS:+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK
OS:=G%RUD=G)IE(R=Y%DFI=S%T=FF%CD=S)

Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.98 seconds
```