

Network Scan Report

Target IP Address: 192.168.1.101 (Metasploitable)

1. TCP SYN Scan:

Command: `nmap -sS 192.168.1.101`

: This command performs a TCP SYN scan on the target IP address to identify open ports.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-04 01:19 PDT
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00062s latency).

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  cproxy-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: 7A:DD:4F:0C:8C:EB (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
[+] Internet Protocol Version 4 (ip), 20 byte(s)
  Source Port: 6000
  Destination Port: 62429
  [Stream index: 696]
  > [Conversation completeness: Incomplete (35)]
    [TCP Segment Len: 0]
    Sequence Number: 0      (relative sequence number)
    Sequence Number (raw): 2571495019
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1  (relative ack number)
    Acknowledgment number (raw): 1644659311
    0110 .... = Header Length: 24 bytes (6)
  > Flags: 0x012 (SYN, ACK)
  Window: 5849
  Calculated Window Size: 58401
```

2. Full Scan with Version Detection:

Command: `nmap -sV 192.168.1.101`

This command conducts a full scan on the target IP address, including version detection to identify services running on open ports.

```
root@kali:/home/kali
# nmap -sV 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-04 01:28 PDT
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00062s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 7.9p1 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_494-Not Found (text/html)
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)
135/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  exec?       512/tcp   open  login
513/tcp   open  login
514/tcp   open  tcptrawpped
109/tcp   open  java-rmi   GNU Classpath grmiregistry
2049/tcp  open  bindshell   Metasploitable root shell
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
MAC Address: 7A:DD:4F:0C:8C:EB (Unknown)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.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 65.20 seconds

Packets: 601 - Displayed: 601 (100.0%) - Dropped: 0 (0.0%) | Profile: Default
```

3. Output to File:

Command: `nmap -sV -oN file.txt 192.168.1.101`

This command performs a full scan with version detection on the target IP address and saves the output to a file named "file.txt".

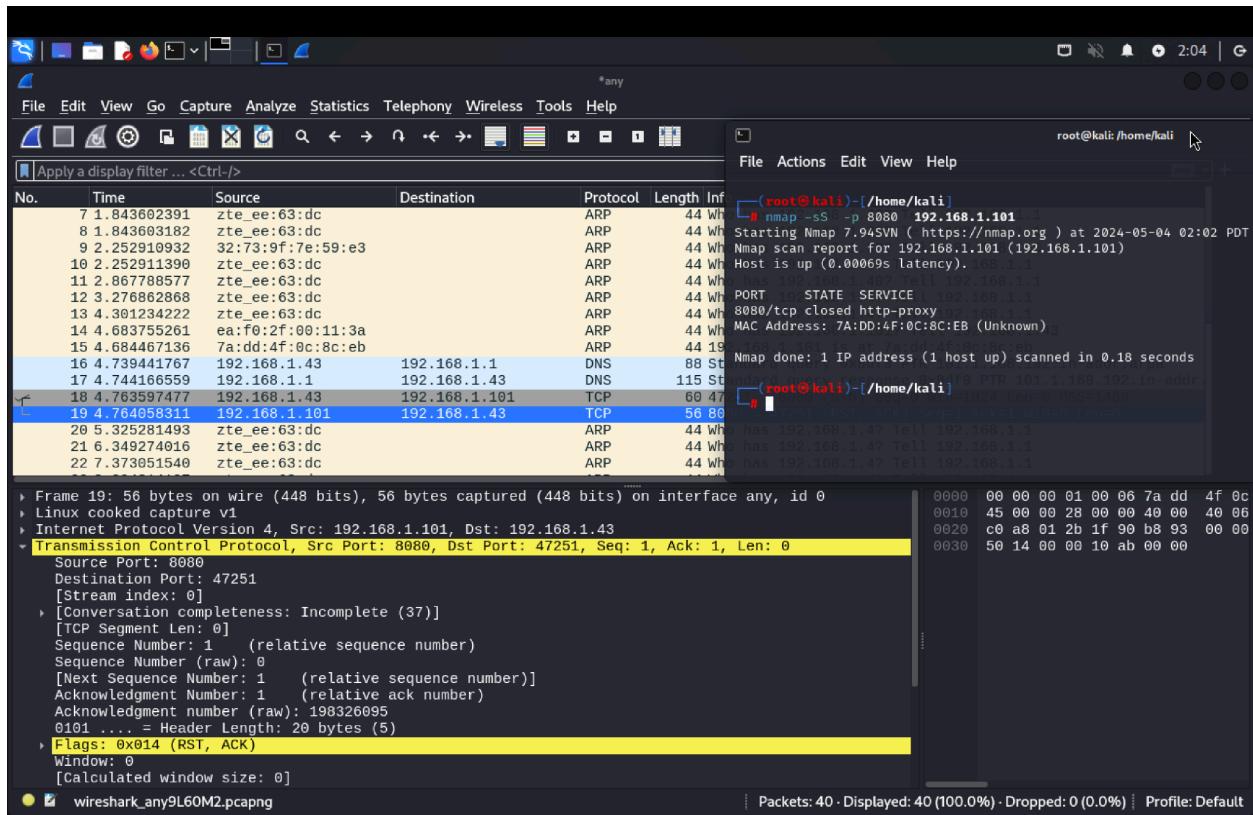
The screenshot shows the Wireshark interface with the following details:

- File Menu:** File, Actions, Edit, View, Help.
- Toolbar:** Apply a display filter ... <Ctrl-/>, Packet list, Narrow & Wide, Case sensitive.
- Table Headers:** No., Time, Source, Destination.
- Table Data:** A list of network packets captured by Nmap. Many ports are shown as open, including ssh (22/tcp), http (80/tcp), and various services like vsftpd, Postfix, Samba, and MySQL.
- Selected Port:** Port 80 (HTTP) is selected, showing the following details:
 - HTTP Headers:** Server: Apache-Coyote/1.1, Content-Type: text/html; charset=ISO-8859-1, Date: Fri, 03 May 2024 21:34:18 GMT, Connection: close.
 - HTTP Response:** [HTTP response 1/1], [Time since request: 0.058663797 seconds], [Request in Frame: 2609], [Request URI: /], File Data: 8692 bytes.
- Bottom Status Bar:** Line-based text data: text/html (234 lines), 68 bytes | Reassembled TCP(8838 bytes), Packets: 2839 - Displayed: 2839 (100.0%) - Dropped: 0 (0.0%) | Profile: Default.

4. Port Scan (Port 8080):

Command: `nmap -sS -p 8080 192.168.1.101

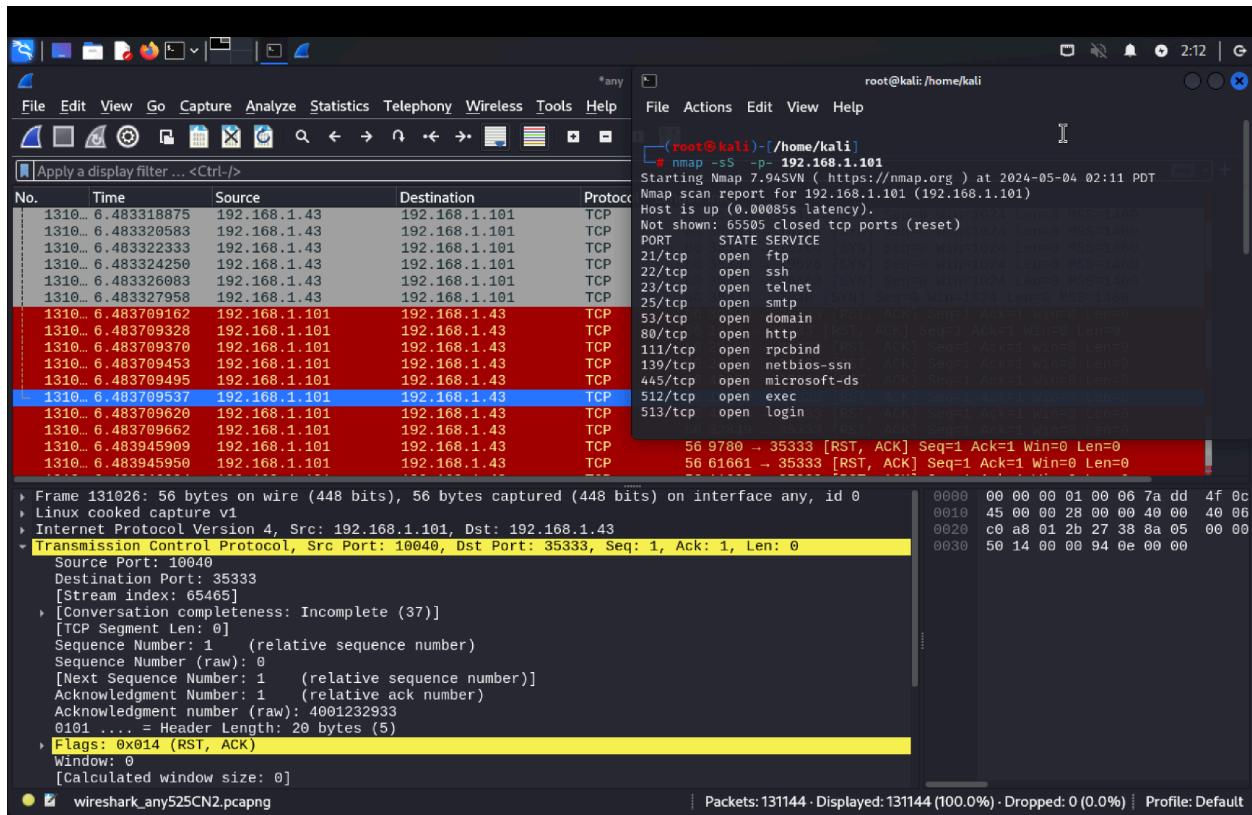
This command scans port 8080 on the target IP address using TCP SYN scan.



5. Full Port Scan:

Command: `nmap -sS -p- 192.168.1.101`

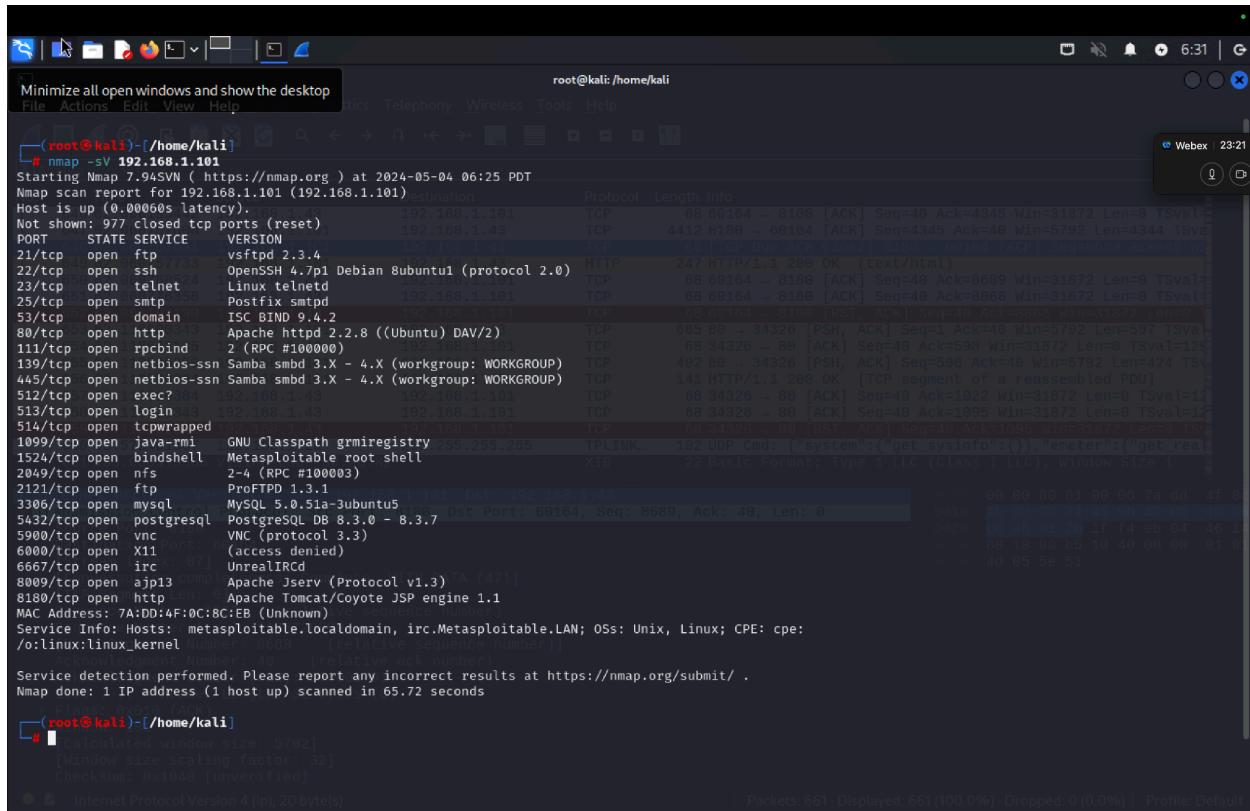
This command performs a full port scan on the target IP address to identify all open ports.



7. Operating System Scan:

Command: `nmap -O 192.168.1.101`

This command performs an operating system scan on the target IP address to identify the operating system running on the host.



The screenshot shows a terminal window titled "root@kali:/home/kali". The command entered is "nmap -O 192.168.1.101". The output is a detailed Nmap scan report for the host 192.168.1.101, which is identified as running Ubuntu 18.04 LTS (64-bit). The report lists numerous open ports and their corresponding services, including Apache, MySQL, PostgreSQL, and various SSH and Telnet ports. The "-O" option indicates an OS detection attempt, which is successful in identifying the host's operating system as Ubuntu 18.04 LTS (64-bit).

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-04 06:25 PDT
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.0060s latency).
Not shown: 977 closed tcp ports (reset)
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 2.0.0
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?    192.168.1.101
513/tcp   open  login    192.168.1.101
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry 259.255.255
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
MAC Address: 7A:D0:4F:0C:8C:EB (Unknown)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.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 65.72 seconds
```

[root@kali ~]# [root@kali ~]# calculated window size: 5792 [root@kali ~]# [root@kali ~]# window size scaling factor: 32 [root@kali ~]# [root@kali ~]# Checksum: 0x1040 [unverified] [root@kali ~]# [root@kali ~]# Internet Protocol Version 4 (IP): 20 byte(s)

8. Version Detection Scan:

Command: `nmap -sV 192.168.1.101`

This command performs a version detection scan on the target IP address to identify services and their versions running on open ports.

The screenshot shows a Wireshark interface capturing traffic from any interface. The packet list pane displays several TCP connections between the local host (192.168.1.101) and a target host (192.168.1.43). The details and bytes panes show the raw hex and ASCII data for each packet. A selected packet (Frame 202) is highlighted in blue, showing its details as an Internet Protocol Version 4 (IP) packet with source port 2121 and destination port 59690, with flags indicating SYN and ACK.

The bottom right of the screen shows the terminal window output of the nmap command. It starts with the command "nmap -F 192.168.1.101". The output shows the host is up with 0 latency. It lists various open ports and their services, including:

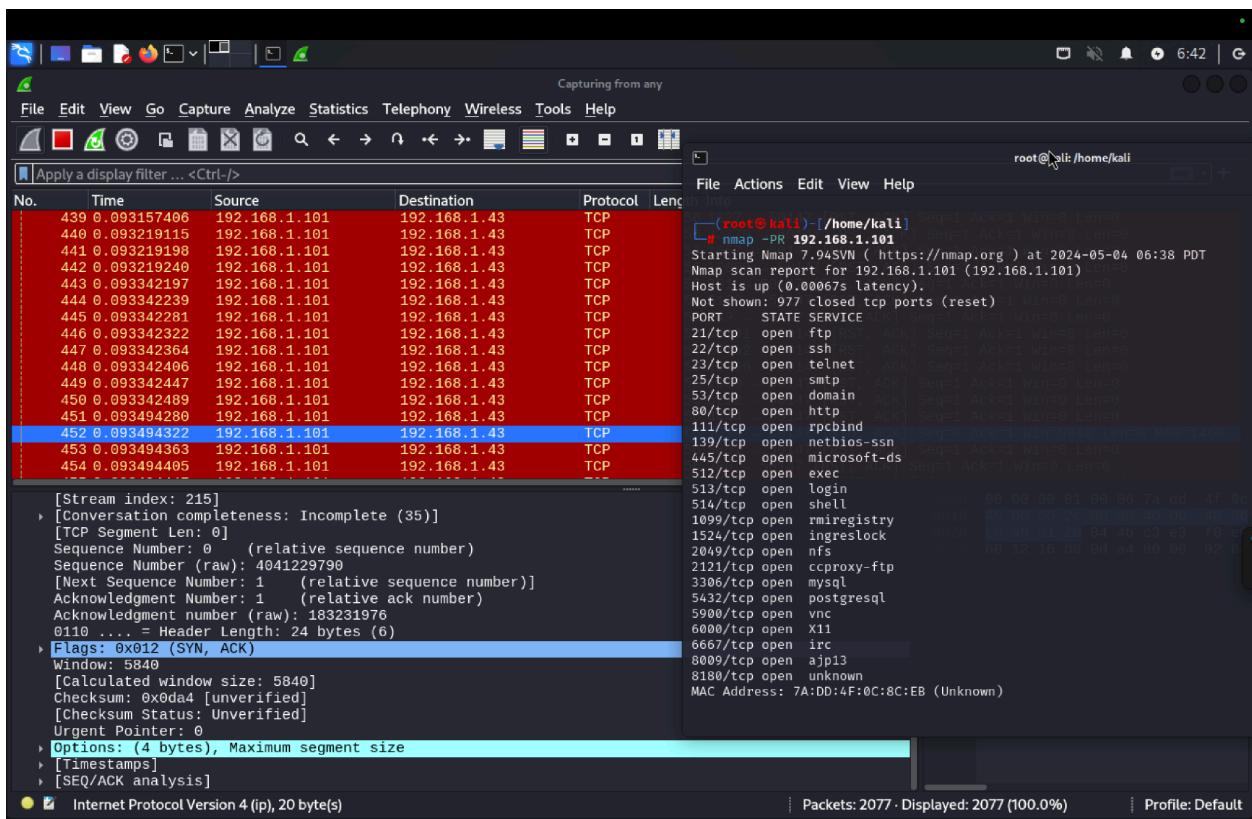
- PORT STATE SERVICE
- 21/tcp open ftp
- 22/tcp open ssh
- 23/tcp open telnet
- 25/tcp open smtp
- 53/tcp open domain
- 80/tcp open http
- 111/tcp open rpcbind
- 139/tcp open netbios-ssn
- 445/tcp open microsoft-ds
- 513/tcp open login
- 514/tcp open shell
- 2049/tcp open nfs
- 2121/tcp open ccproxy-ftp
- 3306/tcp open mysql
- 5432/tcp open postgresql
- 5900/tcp open vnc
- 6000/tcp open X11
- 8009/tcp open ajp13

The output concludes with "Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds".

9. Common Ports Scan (Top 100):

Command: `nmap -F 192.168.1.101`

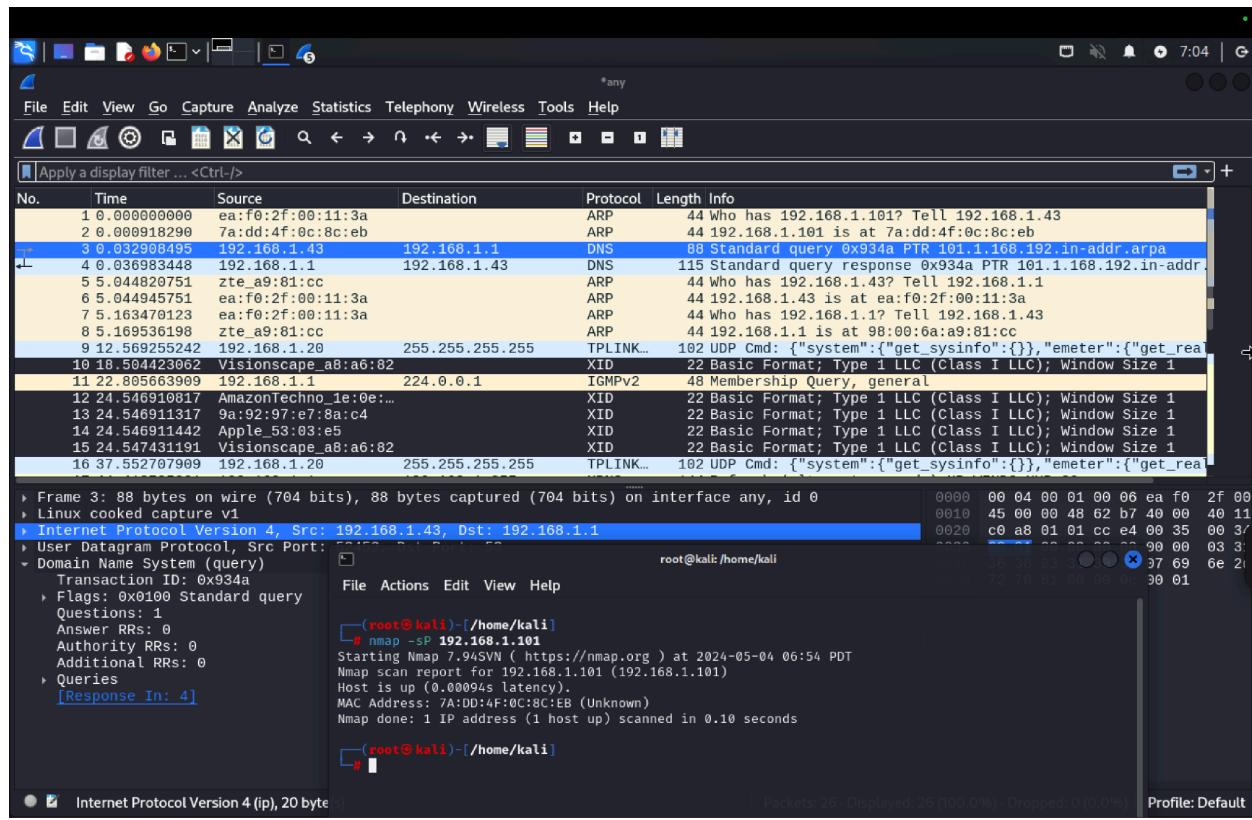
This command conducts a scan on the top 100 common ports on the target



10. ARP Scan:

Command: `nmap -PR 192.168.1.101`

This command performs an ARP scan on the target IP address to discover hosts within the local network.



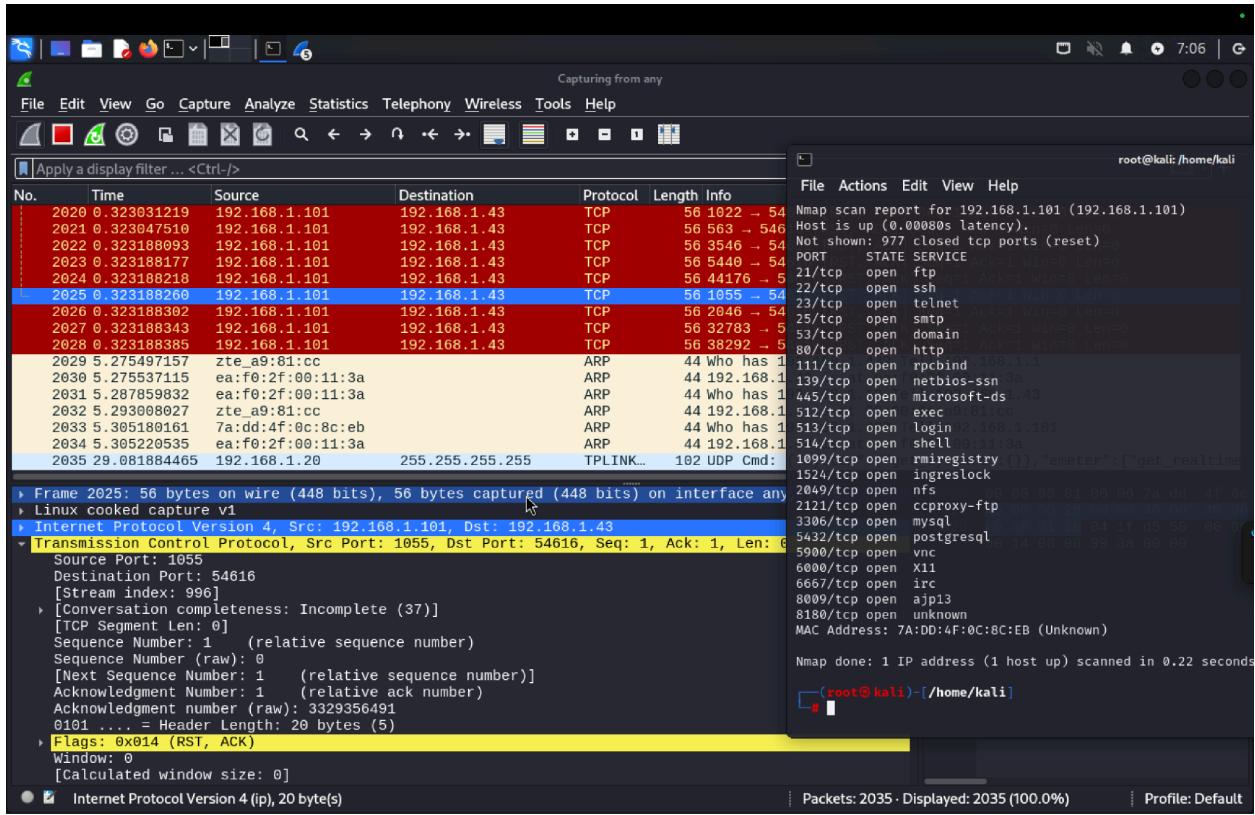
The screenshot shows a Wireshark capture window with the following details:

- File menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard icons for opening files, saving, zooming, and filtering.
- Display Filter:** *any
- List View:** Shows a list of captured frames. Frame 3 is highlighted, showing an ARP request from 192.168.1.43 to 192.168.1.1. Other frames include DNS queries and responses, and various TCP and UDP traffic.
- Details View:** Shows the raw hex and ASCII data for selected frames, including the ARP request for frame 3.
- Hex View:** Shows the raw hex data for selected frames.
- Source View:** Shows the source IP and MAC addresses for selected frames.
- Destination View:** Shows the destination IP and MAC addresses for selected frames.
- Protocols View:** Shows the protocols used in the selected frames.
- Length View:** Shows the length of the selected frames.
- Info View:** Shows additional information about the selected frames.
- Bottom Status Bar:** Displays "Packets: 26 Displayed: 26 (100.0%) Dropped: 0 (0.0%) Profile: Default".

11. Ping Scan:

Command: `nmap -sP 192.168.1.101`

This command conducts a ping scan on the target IP address to determine if the hosts are alive.



12. Scan without Ping:

Command: `nmap -PN 192.168.1.101`

This command performs a scan on the target IP address without sending ICMP echo requests.