

Operating system used :
Kali Linux

Tools Used : NMAP,
Wireshark

Performed by Shourya
Sharma

1. Installation of NMAP

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali) ~ - /home/kali
$ apt install nmap
The following packages were automatically installed and are no longer required:
binutils-mingw-w64-i686 libblosc2-4 python3-aiococonsole python3-neobolt python3-qrcode
binutils-mingw-w64-x86_64 libgssrpc4t64 python3-aiosmb python3-neotime python3-serial-asyncio
bloodhound.py libkadm5srv-mit12 python3-aiowinreg python3-nfsclient python3-smmap
comerr-dev libkadm5srv-mit12 python3-arc4 python3-asciitree python3-numexpr python3-tables
dnsmap libkrb5-dev python3-asn1tools python3-odf python3-numexpr python3-tables-lib
dsniiff liblua5.1-2 python3-asynctools python3-odf python3-odf python3-tld
ettercap-common liblua5.1-2 python3-asynctools python3-odf python3-odf python3-tomlkit
ettercap-graphical liblua5.1-2 python3-asynctools python3-odf python3-odf python3-winactl
figlet liblua5.1-2 python3-asynctools python3-odf python3-odf python3-xmldict
finger medusa python3-bitstruct python3-odf python3-odf python3-yaswfp
gcc-mingw-w64-base mingw-w64-common python3-bitstruct python3-odf python3-odf rsh-redone-client
gcc-mingw-w64-i686-win32 mingw-w64-i686-dev python3-bitstruct python3-odf python3-odf smtp-user-enum
gcc-mingw-w64-i686-win32-runtime mingw-w64-x86_64-dev python3-bitstruct python3-odf python3-odf sparta-scripts
gcc-mingw-w64-x86_64-win32 oracle-instantclient-basic python3-bitstruct python3-odf python3-odf sphinx-rtd-theme-common
gcc-mingw-w64-x86_64-win32-runtime python-odf-doc python3-bitstruct python3-odf python3-odf toilet-fonts
imagemagick python-odf-tools python3-bitstruct python3-odf python3-odf unicornscan
imagemagick-7.q16 python-tables-data python3-bitstruct python3-odf python3-odf urlscan
krb5-multidev python3-aardwolf python3-bitstruct python3-odf python3-odf wapiti
libalio1t64 python3-aesedb python3-bitstruct python3-odf python3-odf
libapache2-mod-php python3-aiohttp python3-bitstruct python3-odf python3-odf
Use 'sudo apt autoremove' to remove them.

Installing:
nmap

Suggested packages:
ncat zenmap

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 724
Download size: 1,938 kB
Space needed: 4,690 kB / 63.2 GB available

Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.95+dfsg-1kali1 [1,938 kB]
Fetched 1,938 kB in 1s (1,733 kB/s)
Selecting previously unselected package nmap.
(Reading database ... 382783 files and directories currently installed.)
Preparing to unpack .../nmap_7.95+dfsg-1kali1_amd64.deb ...
Unpacking nmap (7.95+dfsg-1kali1) ...
```

```
root@kali: /home/kali
File Actions Edit View Help

CPU usage: 3.0%

comerr-dev libkadm5srv-mit12 python3-arc4 python3-nfsclient python3-tables
dnsmap libkdb5-10t64 python3-asciitree python3-numexpr python3-tables-lib
dsniiff libkrb5-dev python3-asn1tools python3-odf python3-tld
ettercap-common liblua5.1-2 python3-asynctools python3-odf python3-tomlkit
ettercap-graphical liblua5.1-2 python3-asynctools python3-odf python3-winactl
figlet liblua5.1-2 python3-asynctools python3-odf python3-xmldict
finger medusa python3-bitstruct python3-odf python3-yaswfp
gcc-mingw-w64-base mingw-w64-common python3-bitstruct python3-odf rsh-redone-client
gcc-mingw-w64-i686-win32 mingw-w64-i686-dev python3-bitstruct python3-odf smtp-user-enum
gcc-mingw-w64-i686-win32-runtime mingw-w64-x86_64-dev python3-bitstruct python3-odf sparta-scripts
gcc-mingw-w64-x86_64-win32 oracle-instantclient-basic python3-bitstruct python3-odf sphinx-rtd-theme-common
gcc-mingw-w64-x86_64-win32-runtime python-odf-doc python3-bitstruct python3-odf toilet-fonts
imagemagick python-odf-tools python3-bitstruct python3-odf urlscan
imagemagick-7.q16 python-tables-data python3-bitstruct python3-odf wapiti
krb5-multidev python3-aardwolf python3-bitstruct python3-odf
libalio1t64 python3-aesedb python3-bitstruct python3-odf
libapache2-mod-php python3-aiohttp python3-bitstruct python3-odf
Use 'sudo apt autoremove' to remove them.

Installing:
nmap

Suggested packages:
ncat zenmap

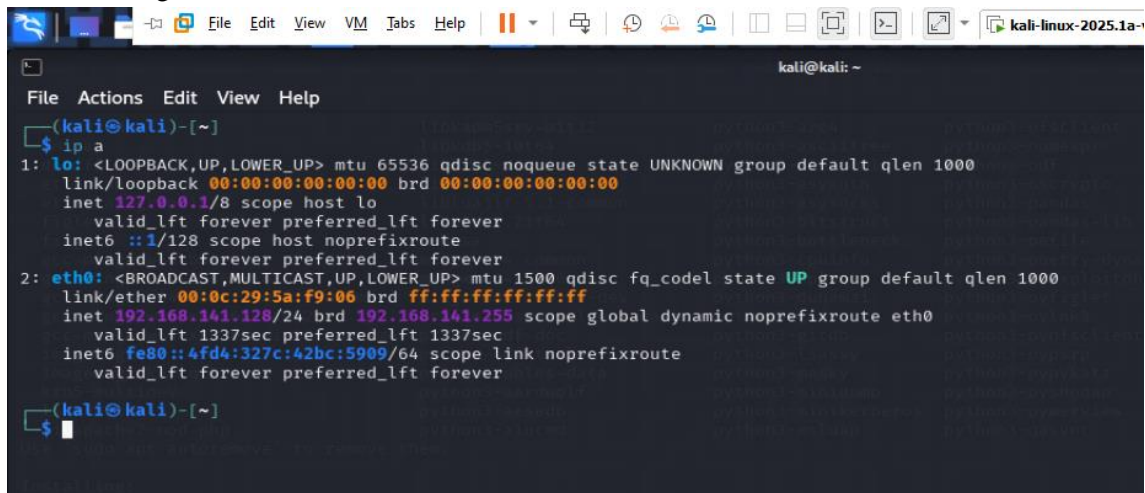
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 724
Download size: 1,938 kB
Space needed: 4,690 kB / 63.2 GB available

Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.95+dfsg-1kali1 [1,938 kB]
Fetched 1,938 kB in 1s (1,733 kB/s)
Selecting previously unselected package nmap.
(Reading database ... 382783 files and directories currently installed.)
Preparing to unpack .../nmap_7.95+dfsg-1kali1_amd64.deb ...
Unpacking nmap (7.95+dfsg-1kali1) ...
Setting up nmap (7.95+dfsg-1kali1) ...
Setcap worked! Adding configuration to environment
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...

(root@kali) ~ - /home/kali
```

2. Identification of Local IP Range

2.1. Checking IP Address

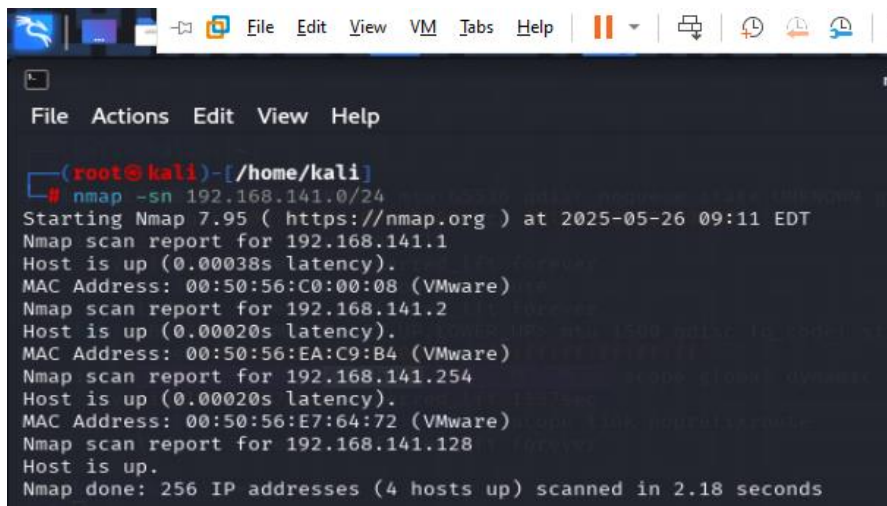


```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:5a:f9:06 brd ff:ff:ff:ff:ff:ff
    inet 192.168.141.128/24 brd 192.168.141.255 scope global dynamic noprefixroute eth0
        valid_lft 1337sec preferred_lft 1337sec
    inet6 fe80::4fd4:327c:42bc:5909/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali@kali)-[~]
$
```

2.2. Scanning and Identifying Ports

2.2.1 Scanning Local Subnet

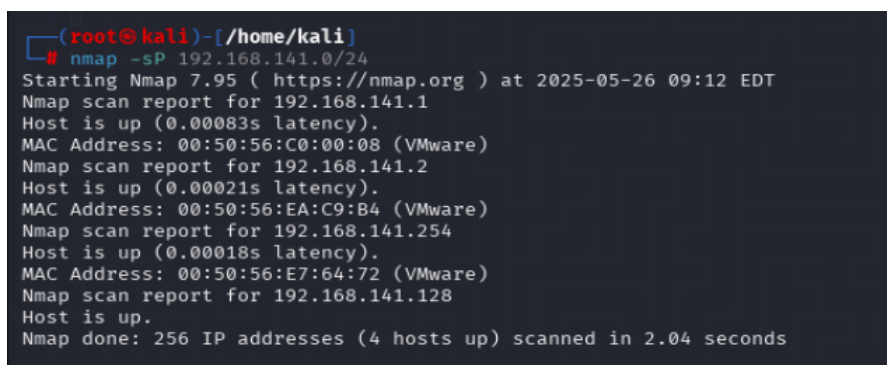
Code used : `nmap -sn 192.168.141.0/24`



```
(root@kali)-[/home/kali]
# nmap -sn 192.168.141.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 09:11 EDT
Nmap scan report for 192.168.141.1
Host is up (0.00038s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.141.2
Host is up (0.00020s latency).
MAC Address: 00:50:56:EA:C9:B4 (VMware)
Nmap scan report for 192.168.141.254
Host is up (0.00020s latency).
MAC Address: 00:50:56:E7:64:72 (VMware)
Nmap scan report for 192.168.141.128
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.18 seconds
```

2.2.2 Port Scanning.

Code Used : `nmap -sP 192.168.141.0/24`



```
(root@kali)-[/home/kali]
# nmap -sP 192.168.141.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 09:12 EDT
Nmap scan report for 192.168.141.1
Host is up (0.00083s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.141.2
Host is up (0.00021s latency).
MAC Address: 00:50:56:EA:C9:B4 (VMware)
Nmap scan report for 192.168.141.254
Host is up (0.00018s latency).
MAC Address: 00:50:56:E7:64:72 (VMware)
Nmap scan report for 192.168.141.128
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.04 seconds
```

3. Performing TCP-SYN Scan

3.1. OS (Operating System) Identification with Stealth Scan

```
root@kali: /home/kali
File Actions Edit View Help
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.04 seconds

(root@kali)-[/home/kali]
$ nmap -sS -O 192.168.141.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 09:12 EDT
Nmap scan report for 192.168.141.1
Host is up (0.00026s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
7070/tcp  open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|11|2019 (92%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2019
Aggressive OS guesses: Microsoft Windows 10 1803 (92%), Microsoft Windows 10 1903 - 21H1 (92%), Microsoft Windows 11 (89%), Microsoft Windows 10 1809 (87%),
Microsoft Windows 10 1909 (85%), Microsoft Windows 10 1909 - 2004 (85%), Windows Server 2019 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.141.2
Host is up (0.0014s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:EA:C9:B4 (VMware)
Aggressive OS guesses: VMware Player virtual NAT device (99%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), Microsoft Windows XP SP3
(91%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Actiontec MI424WR-GEN3I WAP (91%), DVTel DVT-9540DW network camera (89%), Linux 3.2 (89%), Linux 4.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.141.254
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.141.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E7:64:72 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.141.128
Host is up (0.000041s latency).
All 1000 scanned ports on 192.168.141.128 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: 256 IP addresses (4 hosts up) scanned in 14.47 seconds
```

4. Finding & Observations

4.1. It is observed that 4 IP Addresses were found, those being

- 192.168.141.1
- 192.168.141.2
- 192.168.141.254
- 192.168.141.128

Out of those 4 IP Addresses only 2 were found to be functional, other 2 were in ignored state

4.2. IP Address with open ports are:-

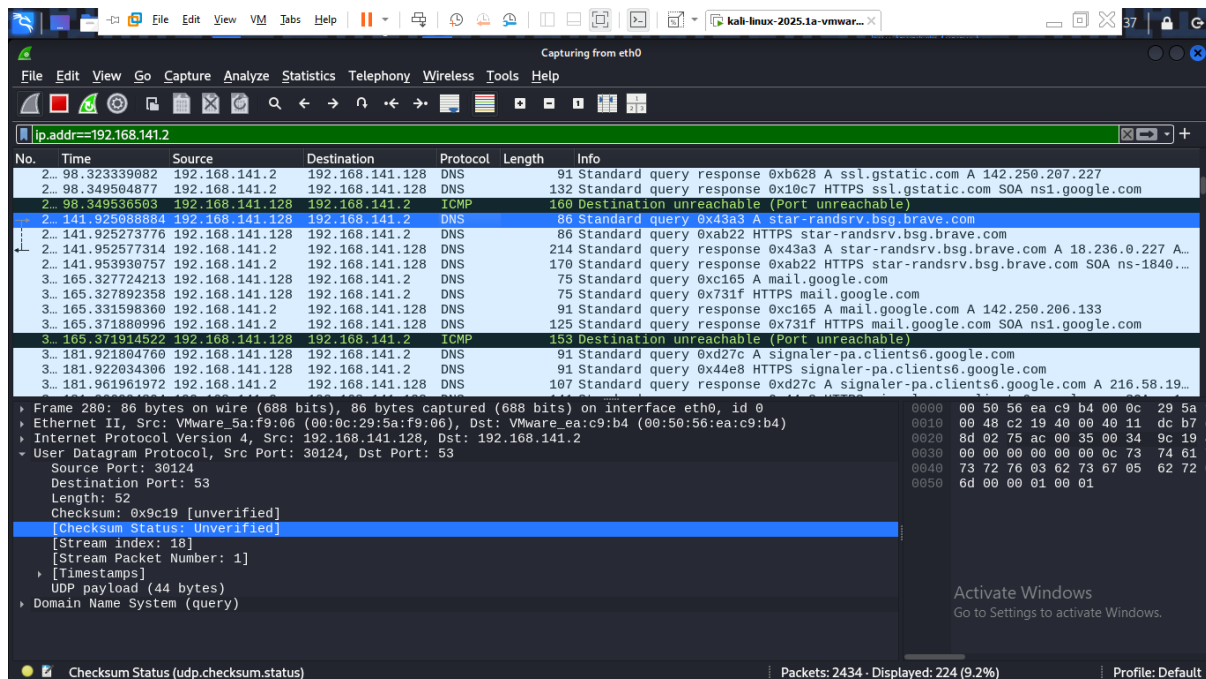
1. 192.168.141.1 – 7070
 - 7070 – Commonly used for Media streaming, it is now is used for RealPlayer streaming (RTSP – Real-Time Streaming Protocol)
2. 192.168.141.2 – 53
 - 53 – It is the default port used by the DNS (Domain Name System) to establish and communicate between the Client & the Server.

4.3 Operating System

- According to the scanning it is found that the OS maybe Windows 10/11

5. Wireshark Analysis

1. Traffic travelling to and from the IP Address 192.168.141.2



2. Behind the scenes when a user tries to access a website (in this case google is the example)

857	8.213296450	142.251.132.67	192.168.141.128	TCP	60	443	→	44464	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460
858	8.213360159	192.168.141.128	142.251.132.67	TCP	54	44464	→	443	[ACK]	Seq=1	Ack=1	Win=64240	Len=0	
859	8.213373733	192.168.141.128	142.251.132.67	TLSv1.3	1841	Client Hello	(SNI=www.google.com)							
860	8.214438521	142.251.132.67	192.168.141.128	TCP	60	443	→	44464	[ACK]	Seq=1	Ack=1461	Win=64240	Len=0	
861	8.214438793	142.251.132.67	192.168.141.128	TCP	60	443	→	44464	[ACK]	Seq=1	Ack=1788	Win=64240	Len=0	

Here the user sends an request to the internet to access google.com

- Client → Server SYN Request to connect
- Server → Client SYN, ACK Accept & respond
- Client → Server ACK Final confirmation

In this manner the connection between the client and the server is established and the user is able to connect to the internet.

6. Commonly run services on Port 53 & 7070

- 53 – It is the default port used by the DNS (Domain Name System) to establish and communicate between the Client & the Server.
- 7070 – Commonly used for Media streaming, it is now is used for RealPlayer streaming (RTSP – Real-Time Streaming Protocol)

7. Risks on Open port

While useful to communicate some common risks that run on open ports are

- Unauthorized access - Open ports can highlight services that can exploit to get admission in the attacker system.
- Religion exploitation - Weaknesses (eg, old software) can be targeted in listening services on open ports, which can be targeted.
- Information leakage - Misconfed services can reveal sensitive information like system banners, user names or internal IP. Ports such as
- Brute-Force attack-22 (SSH) or 3389 (RDP) can be targeted for password-hired attacks.
- Malware communication-open port can be used by malware for command-end-control (C2) or data exfoliation.

8. Saving the File

- Command used : `nmap -sS -O 192.168.141.0/21 -oN Scan-Results.txt`
 - This saves the file in normal TXT Format