Scanning Networks

Lab Manual

Hacking with

RANJITH ADLAKADI

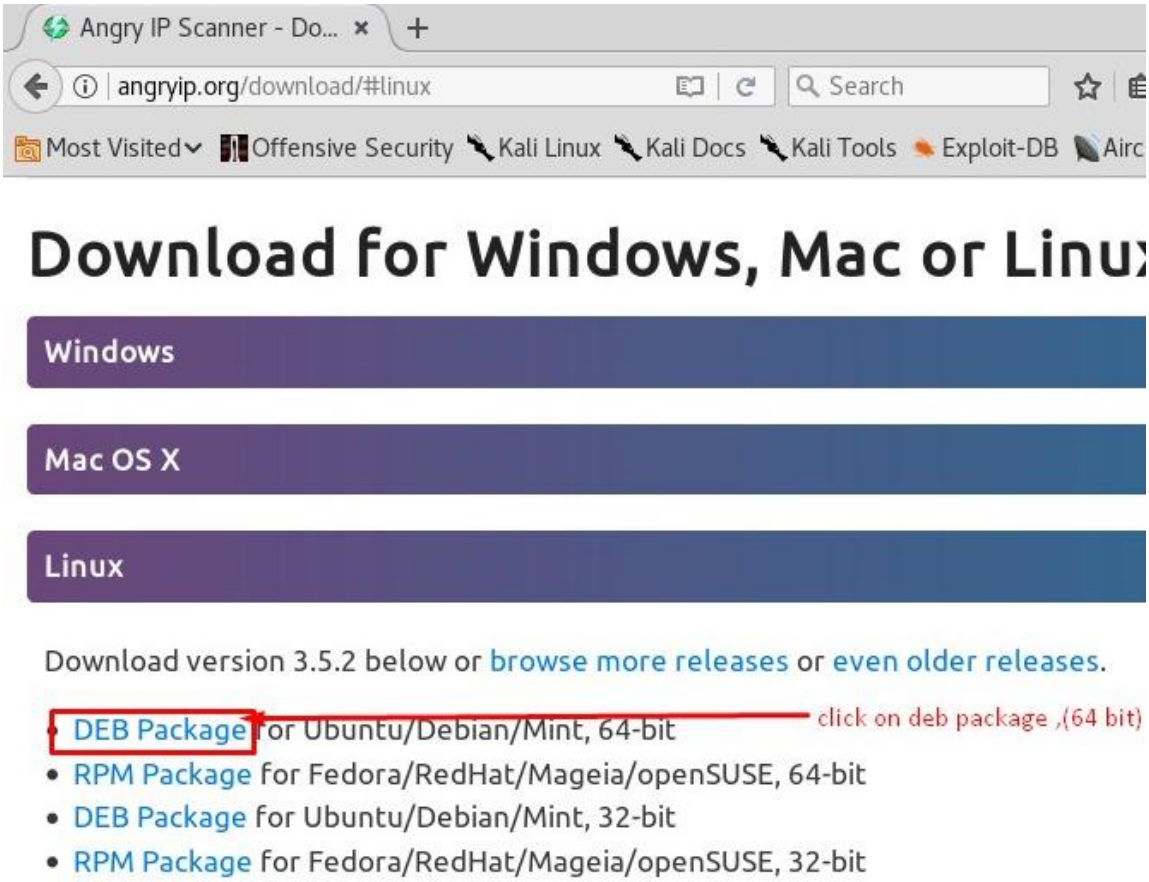
THE DOCUMENT INCLUDES ADDITIONAL PRACTICALS WHICH MAY OR MAY NOT BE COVERED IN THE COURSE

INDEX

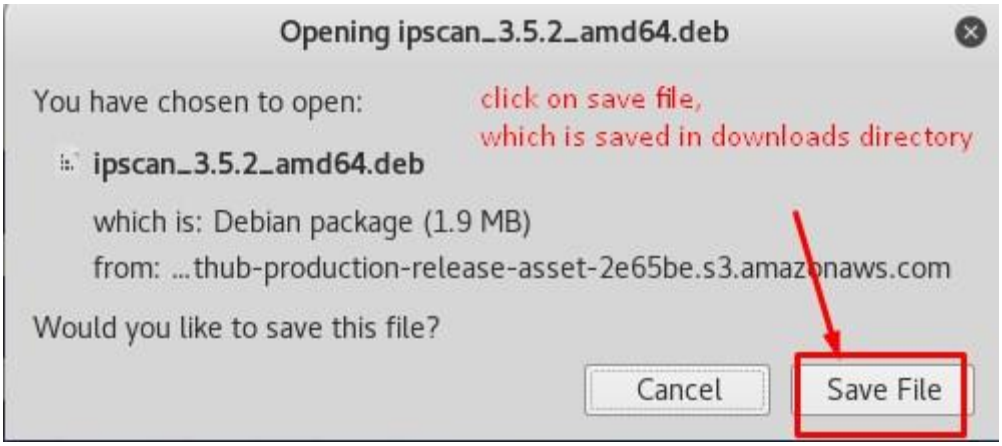
Practical 1: Network Scanning with Angry IP Scanner

To download Angry IP scanner, visit following link https://angryip.org/download/

And download a suitable package, for Kali Linux download ***.deb*** package (based on your installation 32 bit or 64bit)

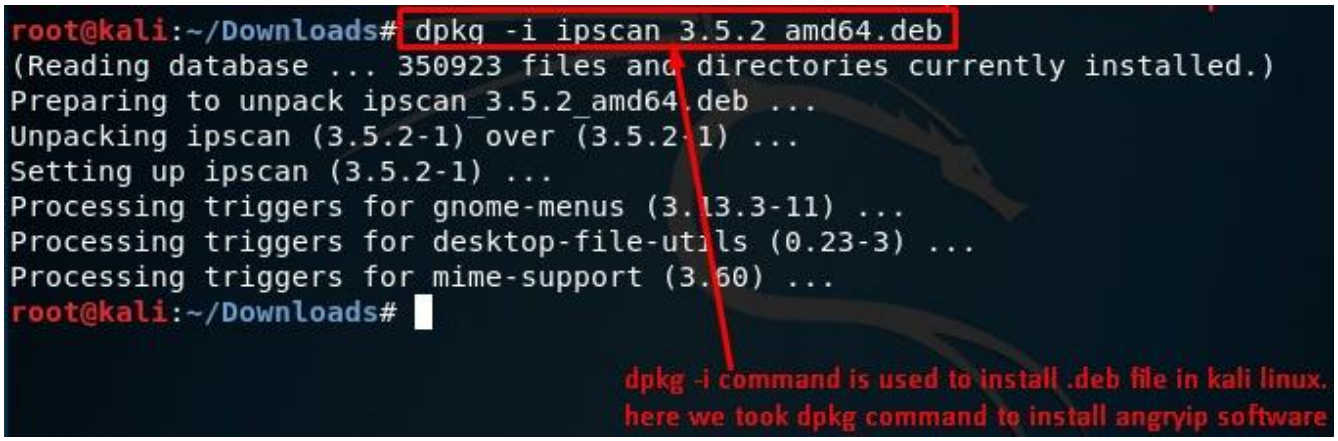


Save the file if it is asking



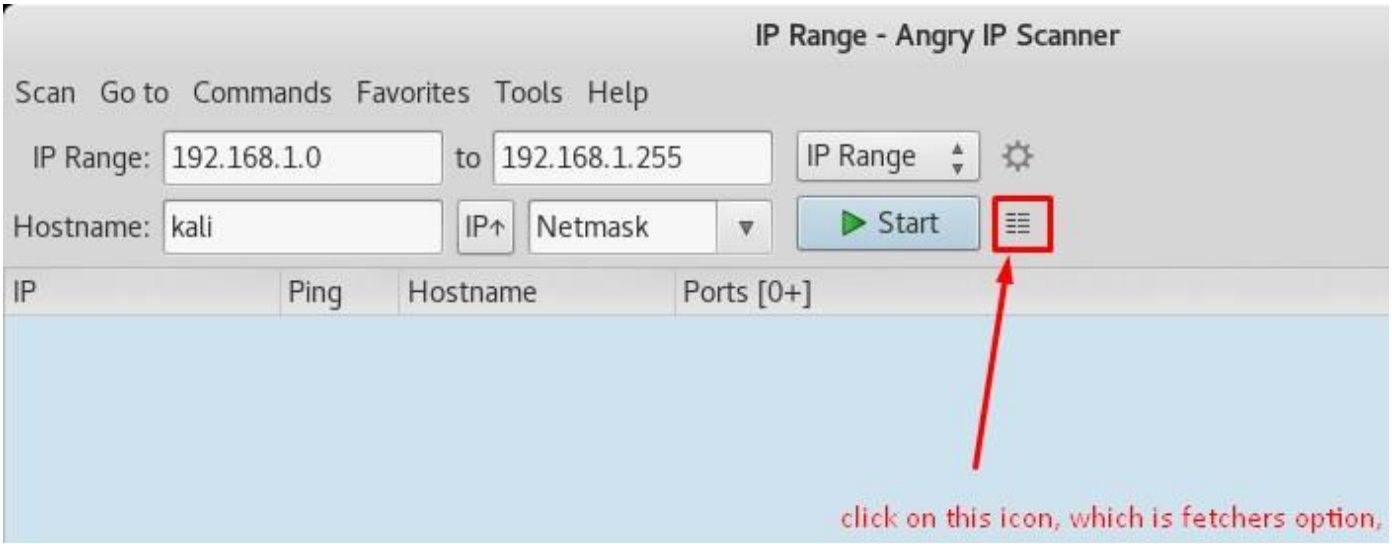
Then open a terminal and go to ***Downloads*** location (/root/Downloads/)

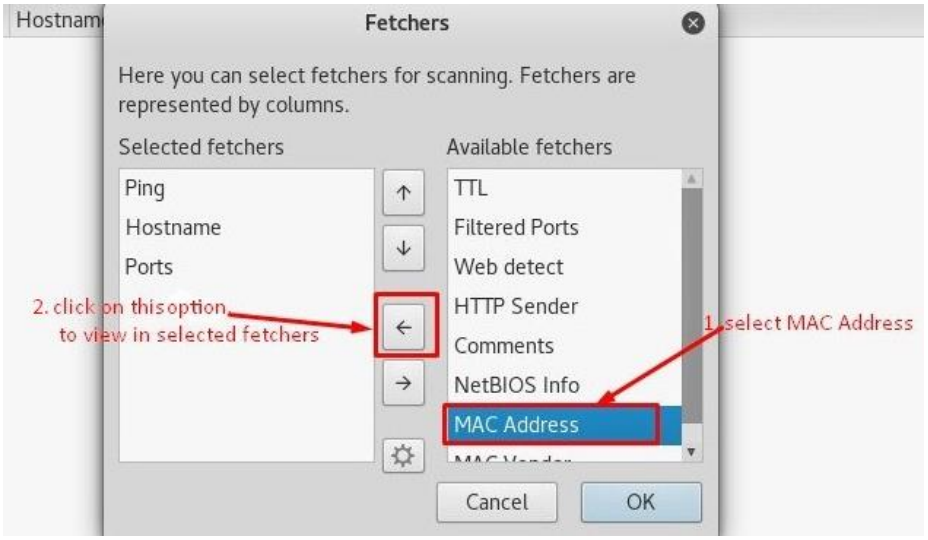
we can see the downloaded file in the ***Downloads*** directory; we can install it by executing the following command

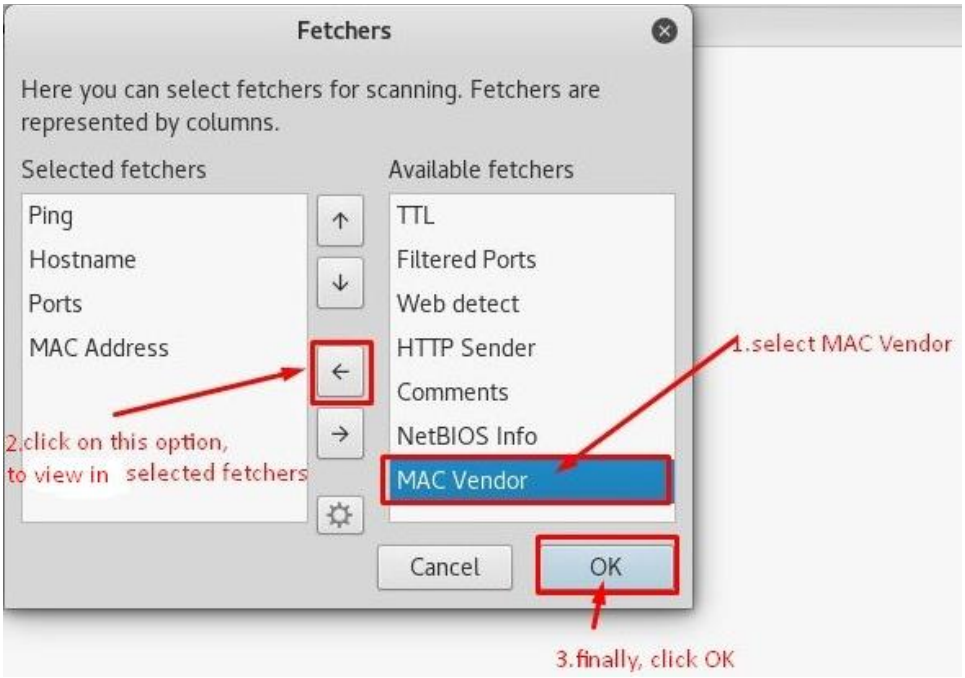


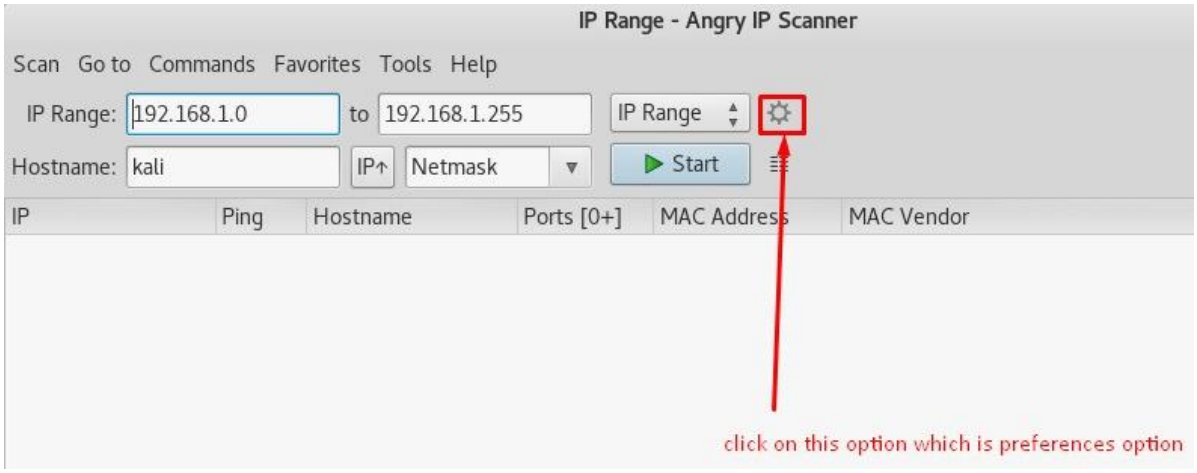
After installation, search for ***Angry IP scanner*** in installed applications and start Angry IP scanner.

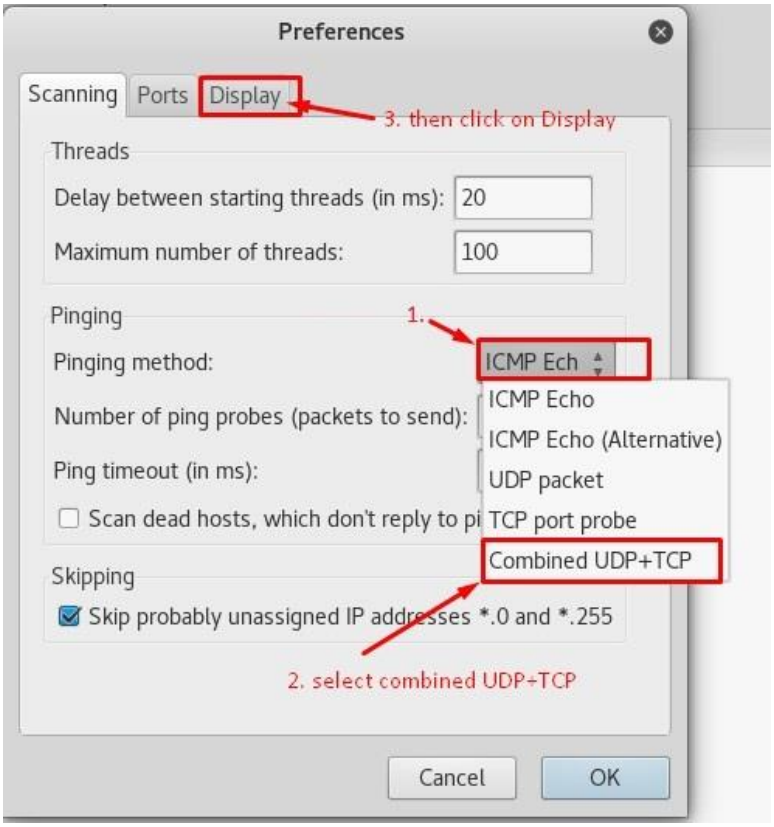
The application looks as shown below. Follow the steps to perform scanning and discover devices.

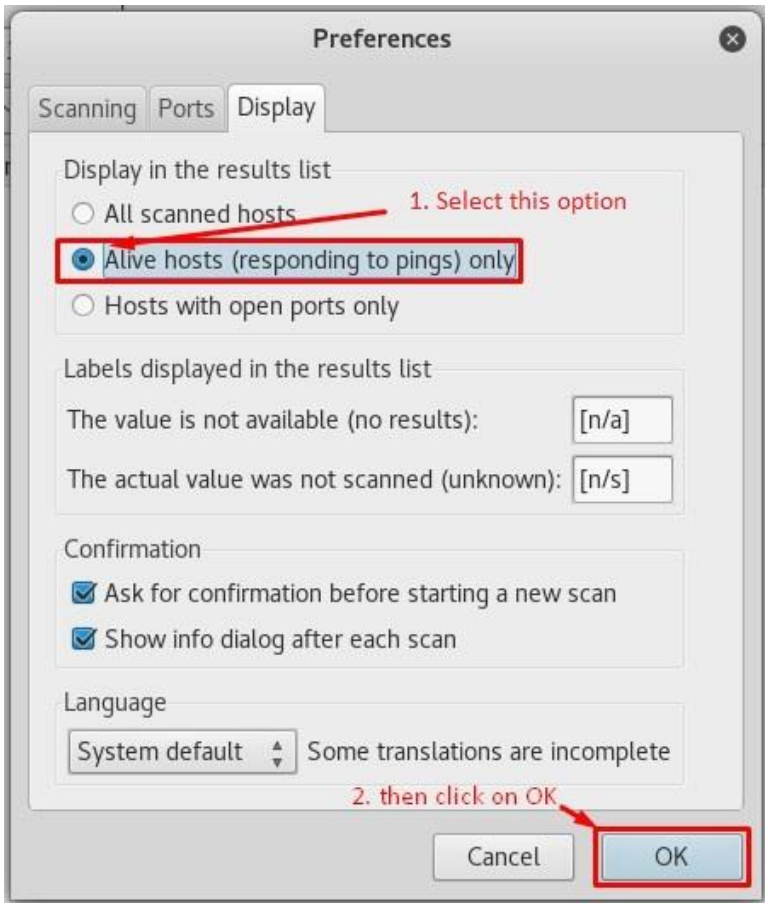


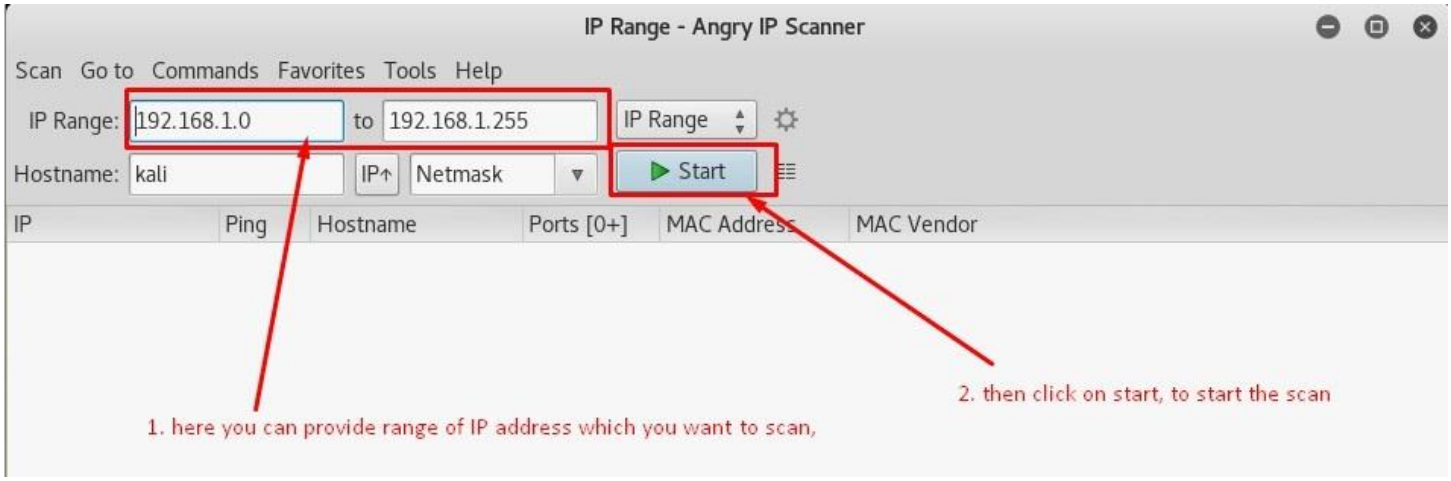

Fetchers
Here you can select fetchers for scanning. Fetchers are represented by columns.
Selected fetchers
Available fetchers
Ping
Hostname
Ports
TTL
Filtered Ports
Web detect
HTTP Sender
Comments
NetBIOS Info
MAC Address
2. click on this option, to view in selected fetchers
1.select MAC Address
Cancel
OK


Fetchers
Here you can select fetchers for scanning. Fetchers are represented by columns.
Selected fetchers
Available fetchers
Ping
Hostname
Ports
MAC Address
TTL
Filtered Ports
Web detect
HTTP Sender
Comments
NetBIOS Info
MAC Vendor
2.click on this option, to view in selected fetchers
1.select MAC Vendor
Cancel
OK
3.finally, click OK

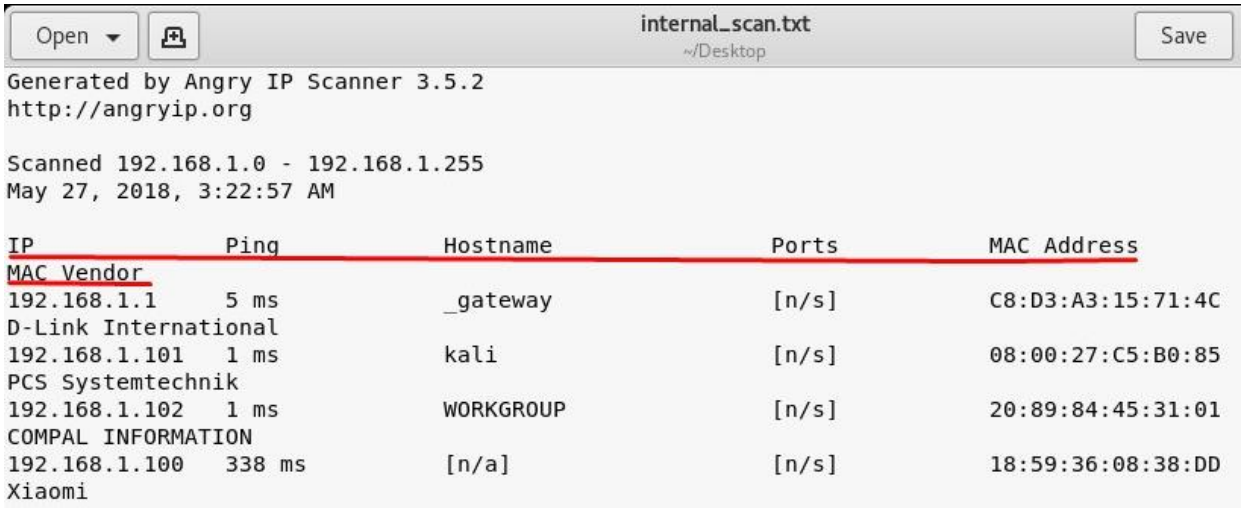

IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 192.168.1.0 to 192.168.1.255 IP Range
Hostname: kali IP↑ Netmask Start
IP Ping Hostname Ports [0+] MAC Address MAC Vendor
click on this option which is preferences option


Preferences
Scanning
Ports
Display
3. then click on Display
Threads
Delay between starting threads (in ms):
20
Maximum number of threads:
100
Pinging
1.
Pinging method:
ICMP Ech
Number of ping probes (packets to send):
Ping timeout (in ms):
Scan dead hosts, which don't reply to pi
ICMP Echo
ICMP Echo (Alternative)
UDP packet
TCP port probe
Combined UDP+TCP
Skipping
Skip probably unassigned IP addresses *.0 and *.255
2. select combined UDP+TCP
Cancel
OK


Preferences
Scanning
Ports
Display
Display in the results list
1. Select this option
All scanned hosts
Alive hosts (responding to pings) only
Hosts with open ports only
Labels displayed in the results list
The value is not available (no results):
[n/a]
The actual value was not scanned (unknown):
[n/s]
Confirmation
Ask for confirmation before starting a new scan
Show info dialog after each scan
Language
System default
Some translations are incomplete
2. then click on OK
Cancel
OK



Export the scan results to a text file. We can use this output file to feed it to another VA tools or port scanner tools.



Practical 2: Network Scanning with fping

Fping is a tool that can scan a range of IP addresses and identify some hosts that are up and running in the given range.

```
root@kali:~# fping -c 1 -g 192.168.0.1/24
```

```
192.168.0.92  : xmt/rcv/%loss = 1/0/100%
192.168.0.93  : xmt/rcv/%loss = 1/0/100%
192.168.0.94  : xmt/rcv/%loss = 1/0/100%
192.168.0.95  : xmt/rcv/%loss = 1/0/100%
192.168.0.96  : xmt/rcv/%loss = 1/0/100%
192.168.0.97  : xmt/rcv/%loss = 1/0/100%
192.168.0.98  : xmt/rcv/%loss = 1/0/100%
192.168.0.99  : xmt/rcv/%loss = 1/0/100%
192.168.0.100 : xmt/rcv/%loss = 1/0/100%
192.168.0.101 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 1.91/1.91/1.91
192.168.0.102 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 1.98/1.98/1.98
192.168.0.103 : xmt/rcv/%loss = 1/0/100%
192.168.0.104 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 1.44/1.44/1.44
192.168.0.105 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 6.54/6.54/6.54
192.168.0.106 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 21.4/21.4/21.4
192.168.0.107 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 2.68/2.68/2.68
192.168.0.108 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 0.45/0.45/0.45
192.168.0.109 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 0.80/0.80/0.80
192.168.0.110 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 0.04/0.04/0.04
192.168.0.111 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 2.68/2.68/2.68
192.168.0.112 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 1.01/1.01/1.01
192.168.0.113 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 4.35/4.35/4.35
192.168.0.114 : xmt/rcv/%loss = 1/0/100%
192.168.0.115 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 1.50/1.50/1.50
192.168.0.116 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 3.79/3.79/3.79
192.168.0.117 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 1.02/1.02/1.02
192.168.0.118 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 1.49/1.49/1.49
192.168.0.119 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 5.52/5.52/5.52
192.168.0.120 : xmt/rcv/%loss = 1/0/100%
192.168.0.121 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 1.91/1.91/1.91
192.168.0.122 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 1.02/1.02/1.02
```

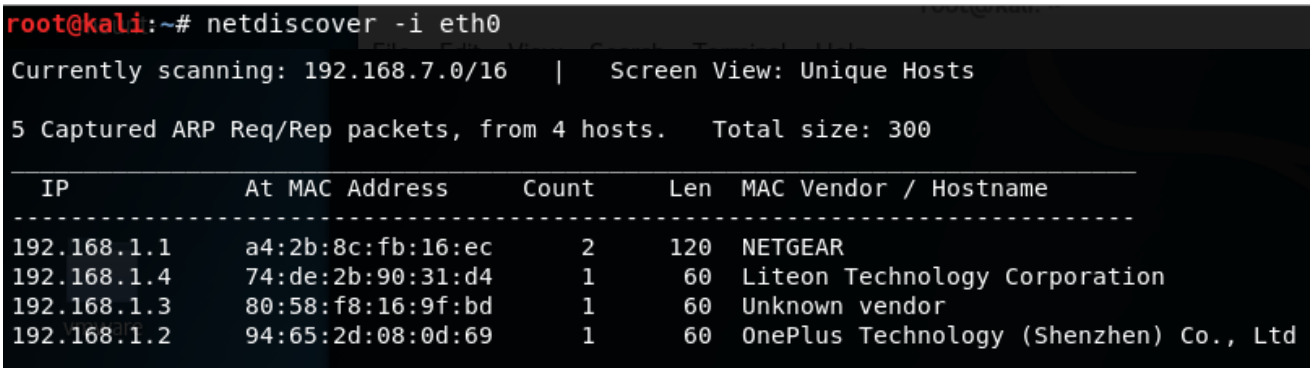
ip is not active,

ip adress is active

Practical 3: Network Scanning With netdiscover

In kali linux terminal type the following command ***netdiscover –i <interface name>***

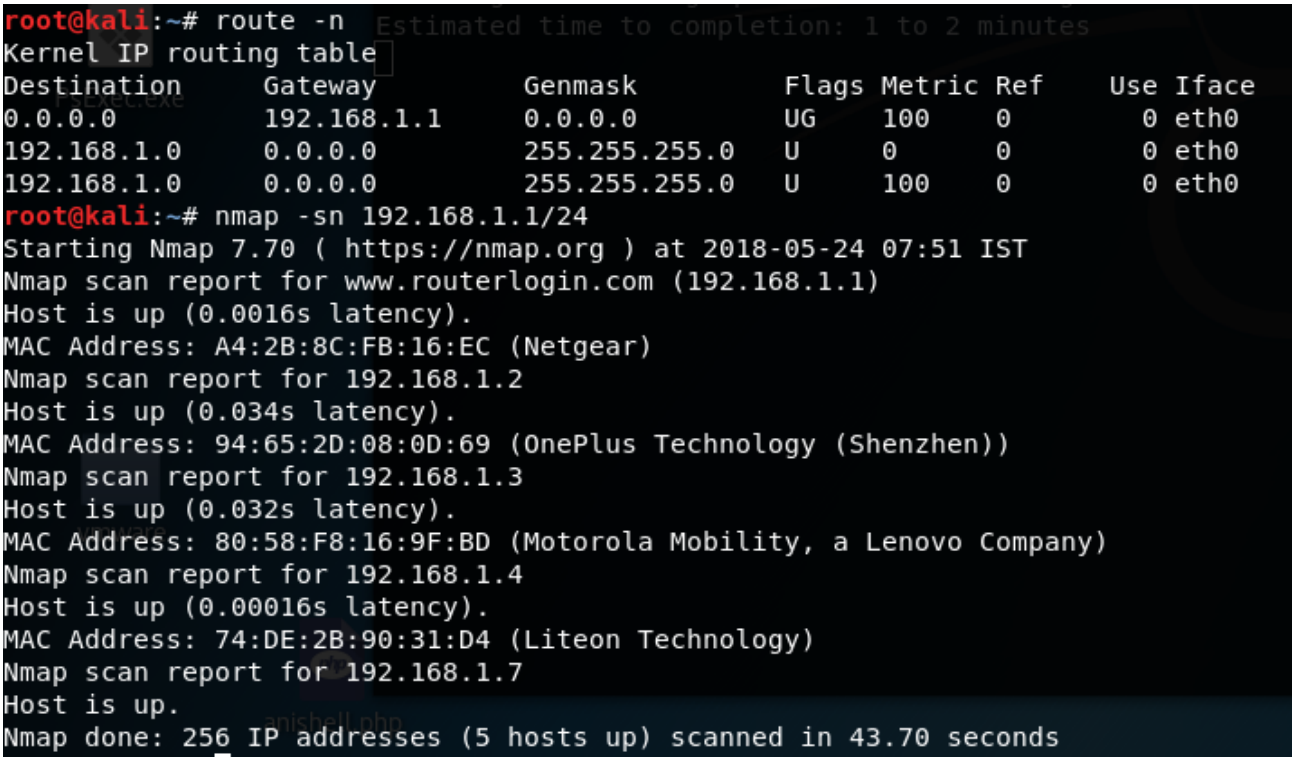
for example: ***netdiscover –i eth0***



Practical 4: Ping Sweeping with nmap

In Kali Linux terminal type the following command

nmap –sn 192.168.1.1/24



Practical 5: Port Scanning with nmap

1.Regular Scan (SYN stealth scan or half open scan):

nmap <target IP or domain>

Ex: ***nmap 192.168.0.137***

nmap –sS example.com

nmap –sS 192.168.0.137

nmap –sS example.com

```
root@kali:~# nmap -sS 192.168.0.137
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-27 05:53 EDT
Nmap scan report for 192.168.0.137
Host is up (0.031s latency).
Not shown: 977 closed ports
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: 02:25:98:60:ED:4F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds
```

NOTE: out of 1000 ports, 977 ports are closed and remaining 23 ports are open.

Note: Even if we take a domain name, nmap will not scan the website, it will scan the computer (server) hosting that website.

2. TCP connect scan (Full Connect Scan):

nmap –sT <target IP or domain>

Example: ***nmap –sT example.com***

nmap –sT 192.168.0.137

```
root@kali:~# nmap -sT todaypk.com

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:06 IST
Stats: 0:02:39 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 65.85% done; ETC: 17:10 (0:01:22 remaining)
Nmap scan report for todaypk.com (192.124.249.3)
Host is up (0.074s latency).
rDNS record for 192.124.249.3: cloudproxy10003.sucuri.net
Not shown: 997 filtered ports
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 526.36 seconds
```

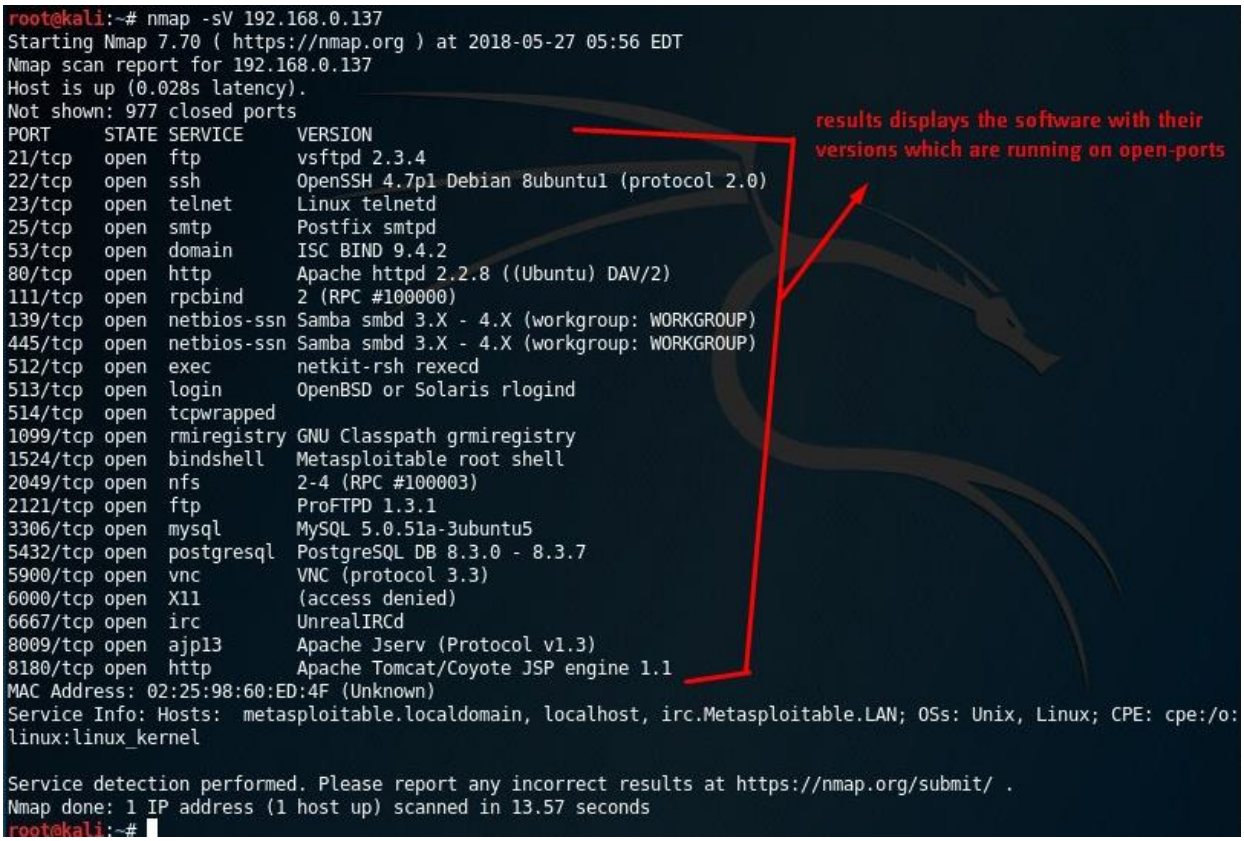
If you get any error saying host may be down or disabled ICMP try adding –Pn to the command

Example: nmap –sT –Pn example.com

3. Service Detection scan or Version Detection scan:

Example: ***nmap –sV example.com***

nmap –sV 192.168.0.137

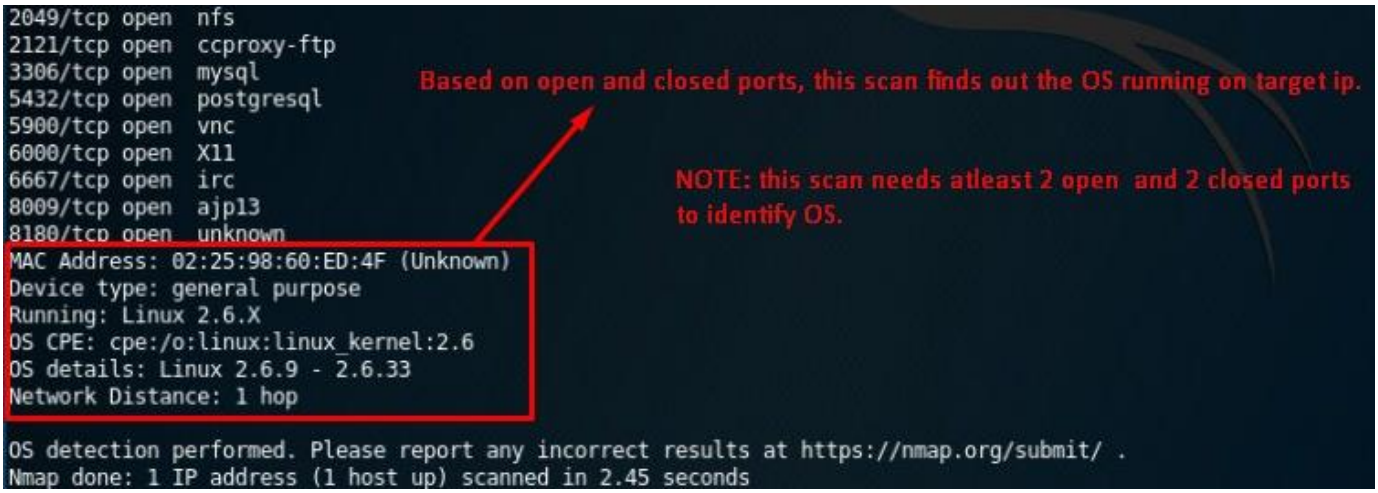


4. OS Detection Scan:

nmap –O <target IP or domain>

Example: ***nmap –O example.com***

nmap –O 192.168.0.137

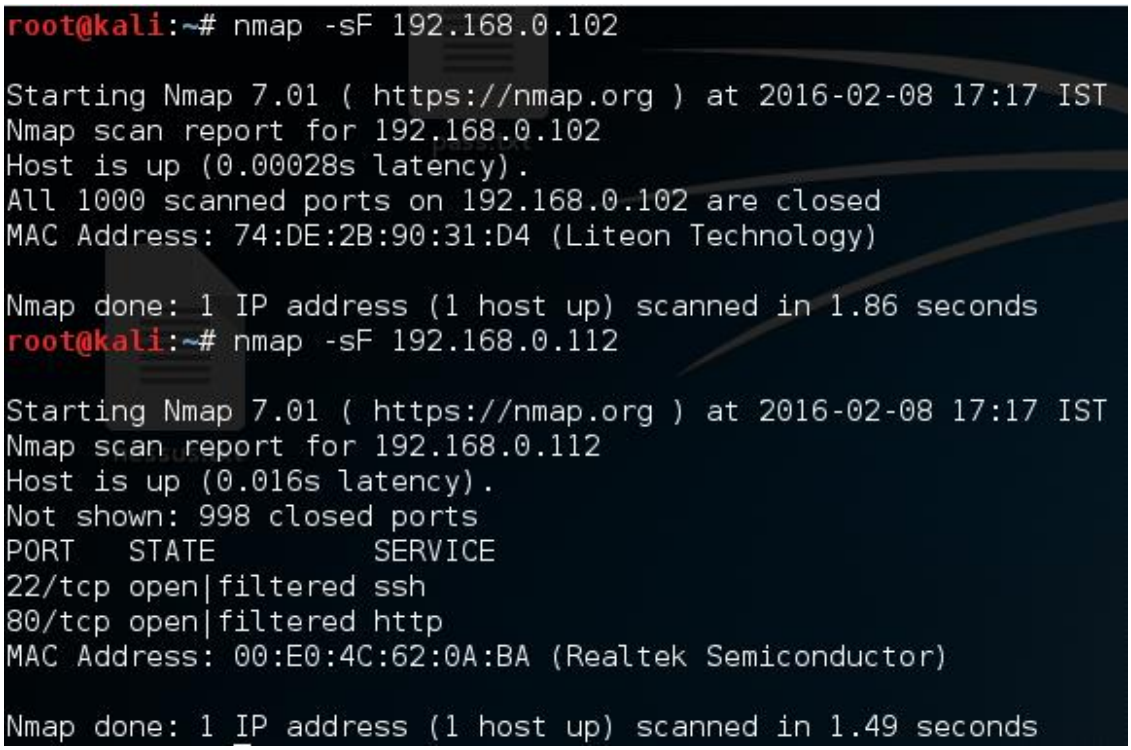


5. FIN scan (FIN Flag):

nmap –sF <target IP or domain>

Example: ***nmap –sF example.com***

nmap –sF 192.168.0.137 –v



6. XMAS scan (FIN, PSH, URG Flags):

nmap –sX <target IP or domain>

Ex: ***nmap –sX example.com***

nmap –sX 192.168.0.137 –v

```
root@kali:~# nmap -sX 192.168.0.112

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:17 IST
Nmap scan report for 192.168.0.112
Host is up (0.018s latency).
Not shown: 998 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh
80/tcp open|filtered http
MAC Address: 00:E0:4C:62:0A:BA (Realtek Semiconductor)

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
root@kali:~# nmap -sX 192.168.0.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:17 IST
Nmap scan report for 192.168.0.102
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.0.102 are closed
MAC Address: 74:DE:2B:90:31:D4 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
```

7. NULL scan (No Flags)

nmap –sN <target IP or domain>

Ex: ***nmap –sN example.com***

nmap –sN 192.168.0.137 –v

```
root@kali:~# nmap -sN 192.168.0.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:17 IST
Nmap scan report for 192.168.0.102
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.0.102 are closed
MAC Address: 74:DE:2B:90:31:D4 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds
root@kali:~# nmap -sN 192.168.0.112

Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-08 17:18 IST
Nmap scan report for 192.168.0.112
Host is up (0.018s latency).
Not shown: 998 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh
80/tcp open|filtered http
MAC Address: 00:E0:4C:62:0A:BA (Realtek Semiconductor)

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
```

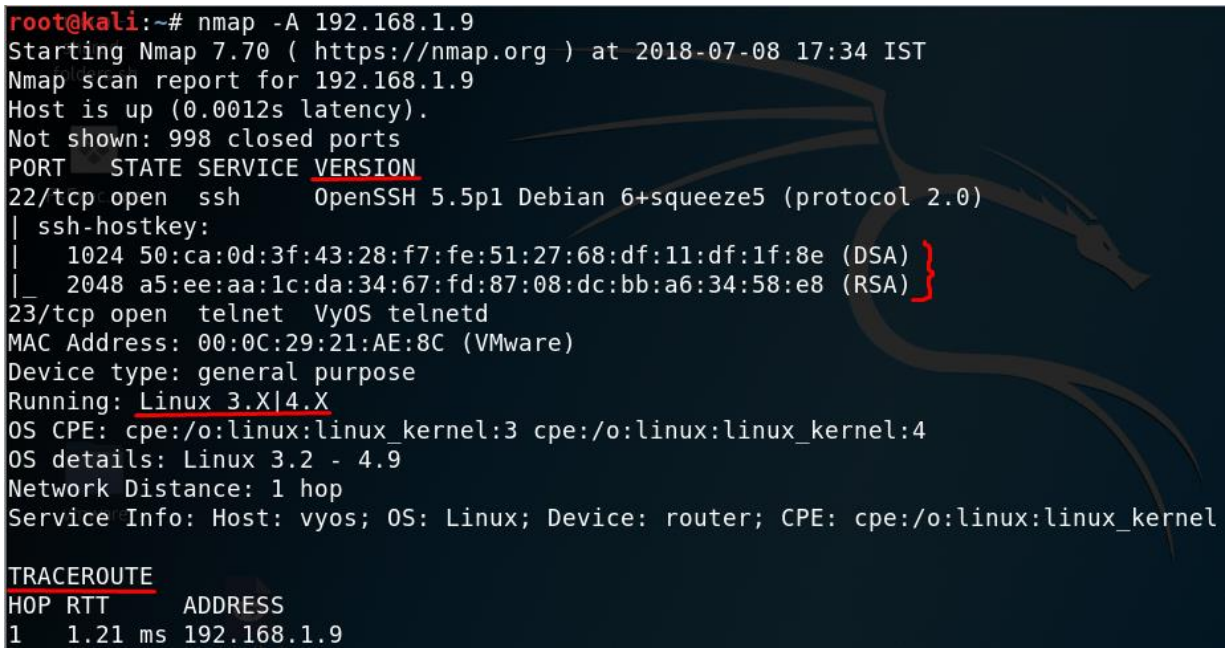
8. Aggressive scan:

nmap –A <target IP of domain>

Ex: ***nmap –A example.com***

nmap –A 192.168.0.137 –v

You can add –v at the end of any command to see the verbose (in detailed) information

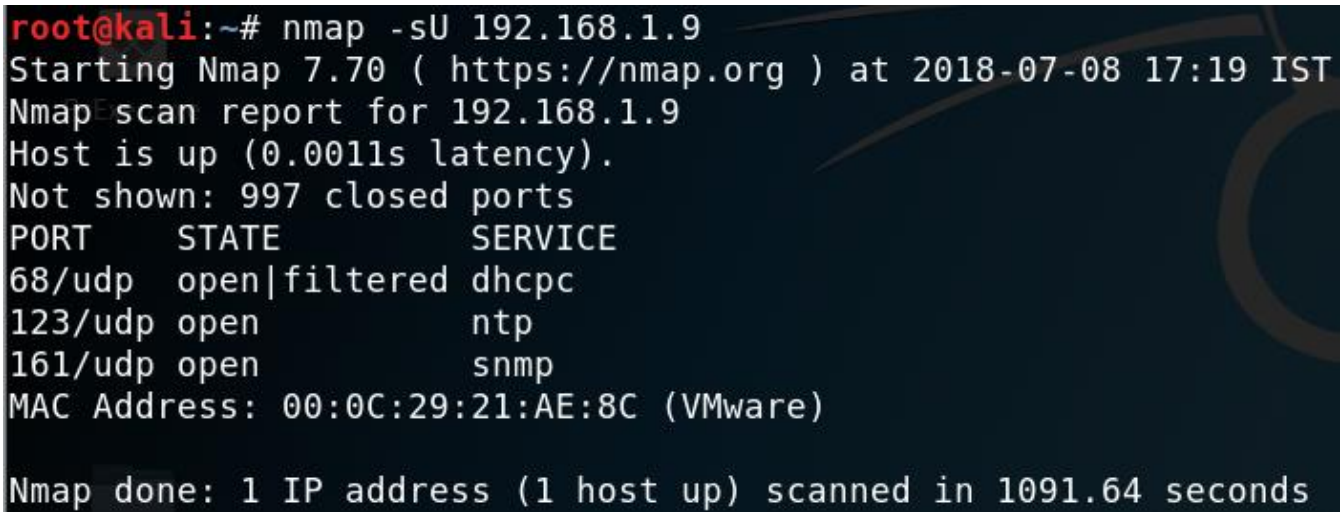


9. UDP port scan:

nmap –sU <target IP or domain>

Example: ***nmap –sU example.com***

nmap –sU 192.168.0.137



10. Custom port scanning:

nmap –p <port range> <target IP or domain>

Ex: ***nmap –p 80 example.com***

nmap 192.168.0.137 –p 80-85

nmap 49.204.90.43 –p 80,81,85,21,443

```
root@kali:~# nmap -p 80,21 192.168.1.1
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-24 07:57 IST
Nmap scan report for www.routerlogin.com (192.168.1.1)
Host is up (0.0015s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
80/tcp open   http
MAC Address: A4:2B:8C:FB:16:EC (Netgear)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@kali:~# nmap -p 80 192.168.1.1
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-24 07:57 IST
Nmap scan report for www.routerlogin.com (192.168.1.1)
Host is up (0.0023s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: A4:2B:8C:FB:16:EC (Netgear)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

```
root@kali:~# nmap -p 20-80 192.168.1.1
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-24 07:57 IST
Nmap scan report for www.routerlogin.com (192.168.1.1)
Host is up (0.0042s latency).
Not shown: 58 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
53/tcp open  domain
80/tcp open  http
MAC Address: A4:2B:8C:FB:16:EC (Netgear)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

11. traceroute scan with nmap

nmap --traceroute <target IP or domain>

Ex: ***nmap --traceroute example.com***

nmap --traceroute 192.168.0.137 –v

```
root@kali:~# nmap --traceroute example.com
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-07 16:28 IST
Nmap scan report for example.com (93.184.216.34)
Host is up (0.17s latency).
Other addresses for example.com (not scanned): 2606:2800:220:1:248:1893:25c8:1946
Not shown: 995 filtered ports
PORT     STATE  SERVICE
25/tcp   open   smtp
80/tcp   open   http
443/tcp  open   https
1119/tcp closed bnetgame
1935/tcp closed rtmp

TRACEROUTE (using port 1935/tcp)
HOP RTT       ADDRESS
1   3.95 ms   192.168.1.1
2   4.32 ms   dlinkrouter (192.168.0.1)
3   14.20 ms  14.141.24.177.static-hyderabad.tcl.net.in (14.141.24.177)
4   ...
5   19.90 ms  ix-ae-0-4.tcore1.mlv-mumbai.as6453.net (180.87.38.5)
6   143.47 ms if-ae-5-2.tcore1.wyn-marseille.as6453.net (80.231.217.29)
7   129.30 ms if-ae-8-1600.tcore1.pye-paris.as6453.net (80.231.217.6)
8   143.63 ms if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)
9   134.04 ms ae-7.r04.parsfr01.fr.bb.gin.ntt.net (129.250.8.1)
10  131.77 ms ae-2.r25.londen12.uk.bb.gin.ntt.net (129.250.6.13)
11  146.69 ms ae-1.r24.londen12.uk.bb.gin.ntt.net (129.250.2.26)
12  204.91 ms ae-5.r24.nycmny01.us.bb.gin.ntt.net (129.250.2.18)
13  205.92 ms ae-1.r08.nycmny01.us.bb.gin.ntt.net (129.250.5.62)
14  204.60 ms ce-0-19-0-1.r07.nycmny01.us.ce.gin.ntt.net (128.241.1.14)
15  194.21 ms 152.195.68.135
16  193.79 ms 93.184.216.34
```