



Chapter 3

Scanning Networks

Lab Manual



**THIS DOCUMENT INCLUDES ADDITIONAL PRACTICALS WHICH
MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING.
FOR MORE DETAILS APPROACH LAB COORDINATORS**

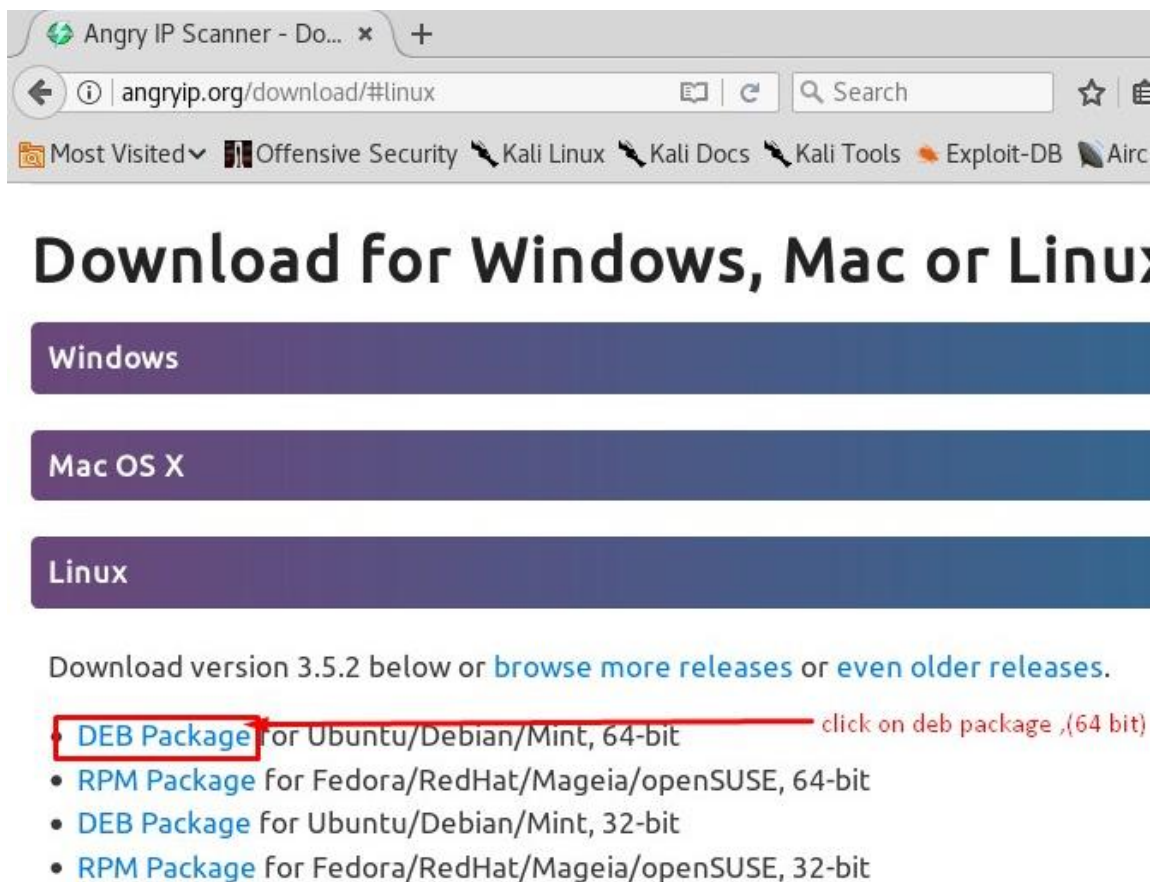
INDEX

S. No.	Practical Name	Page No.
1	Network Scanning with Angry IP Scanner	1
2	Network Scanning with fping	6
3	Network Scanning With netdiscover	7
4	Ping Sweeping with nmap	8
5	Port Scanning with nmap	9

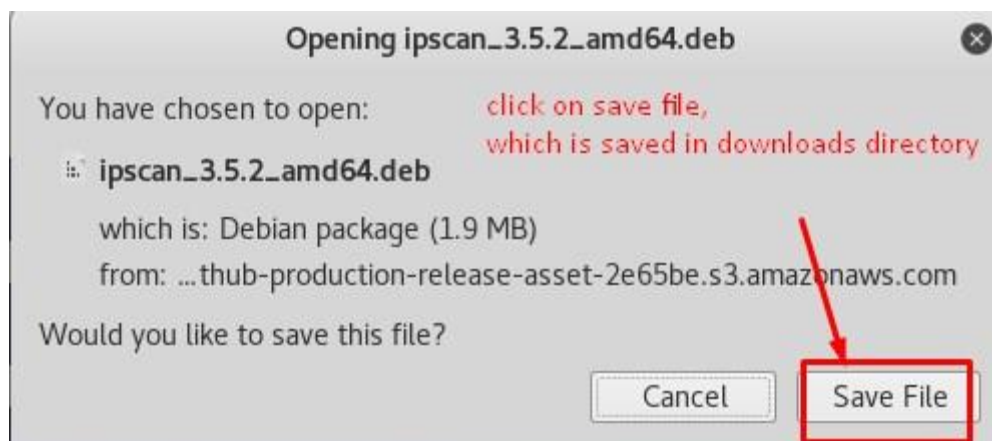
Practical 1: Network Scanning with Angry IP Scanner

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/)

```
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
ipscan_3.5.2_amd64.deb      Untitled.txt
tor-browser_en-US          vpn
tor-browser-linux64-7.5.4_en-US.tar.xz  VPNBook.com-OpenVPN-Euro1.zip
root@kali:~/Downloads#
```

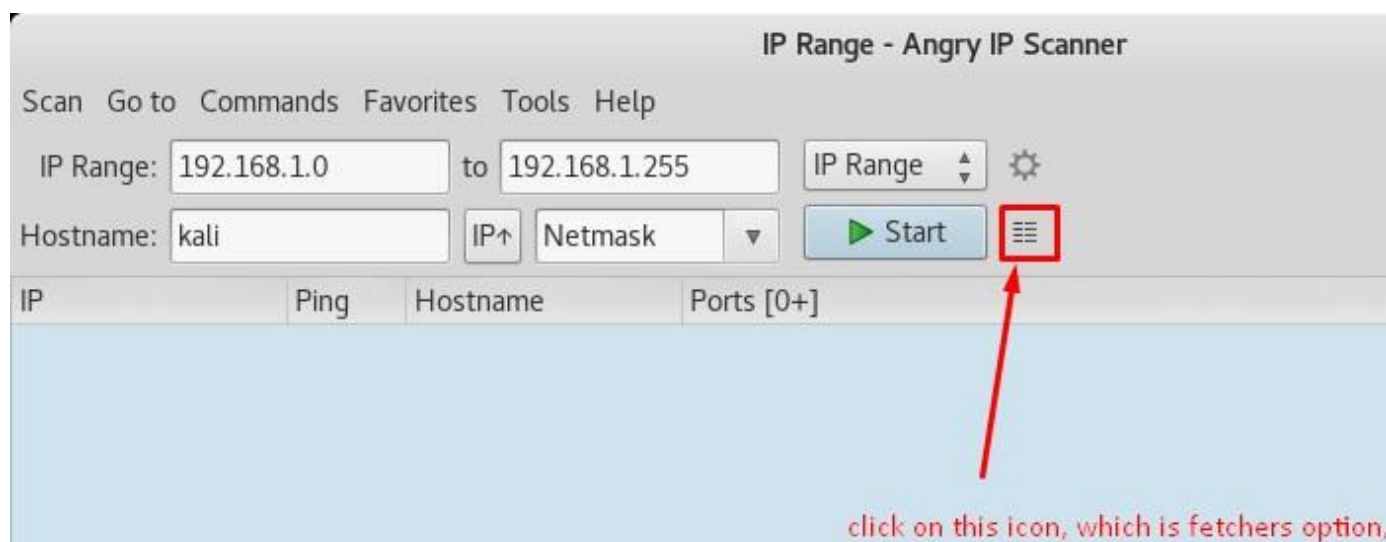
to checkout the list of available items in downloads Directory

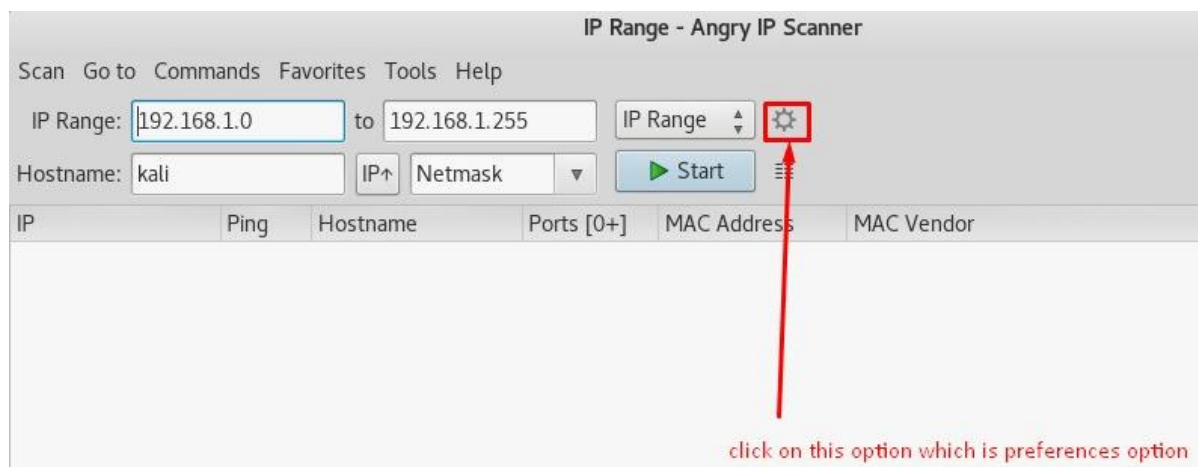
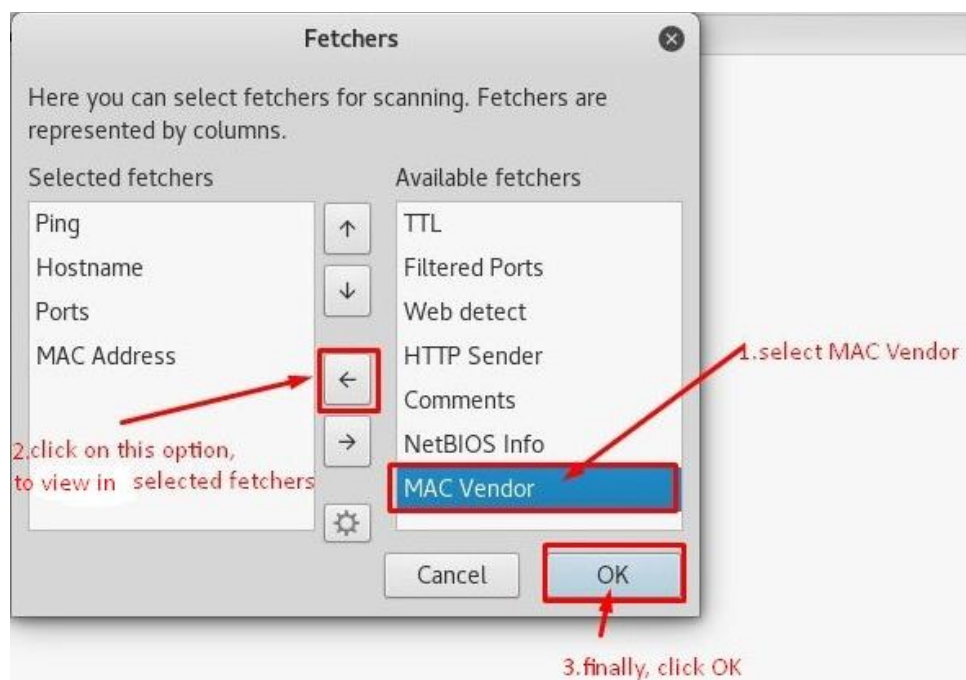
we can see the downloaded file in the **Downloads** directory; we can install it by executing the following command

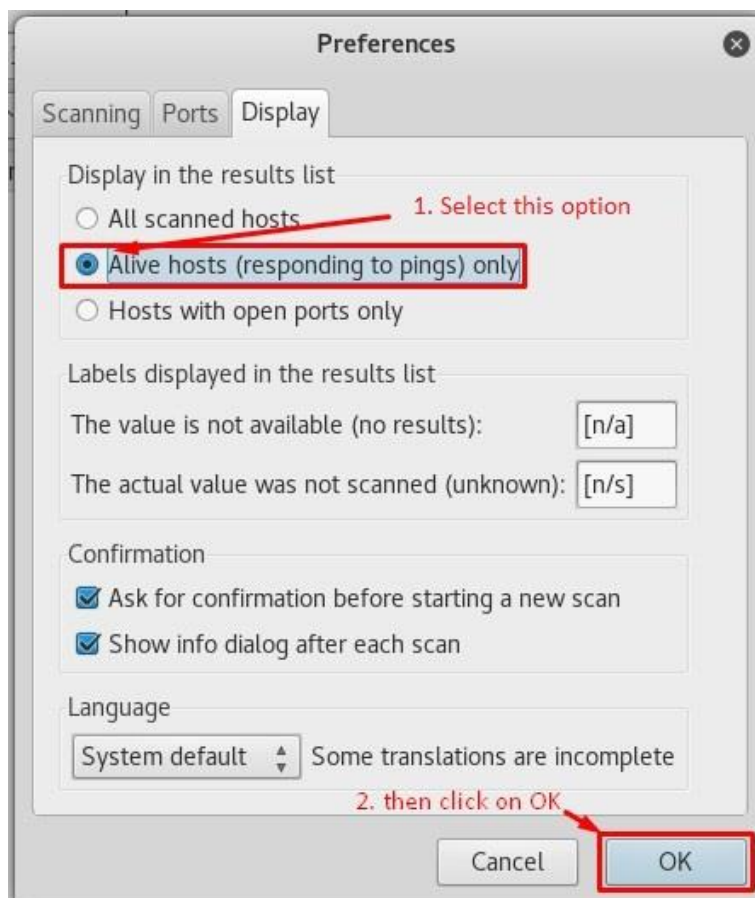
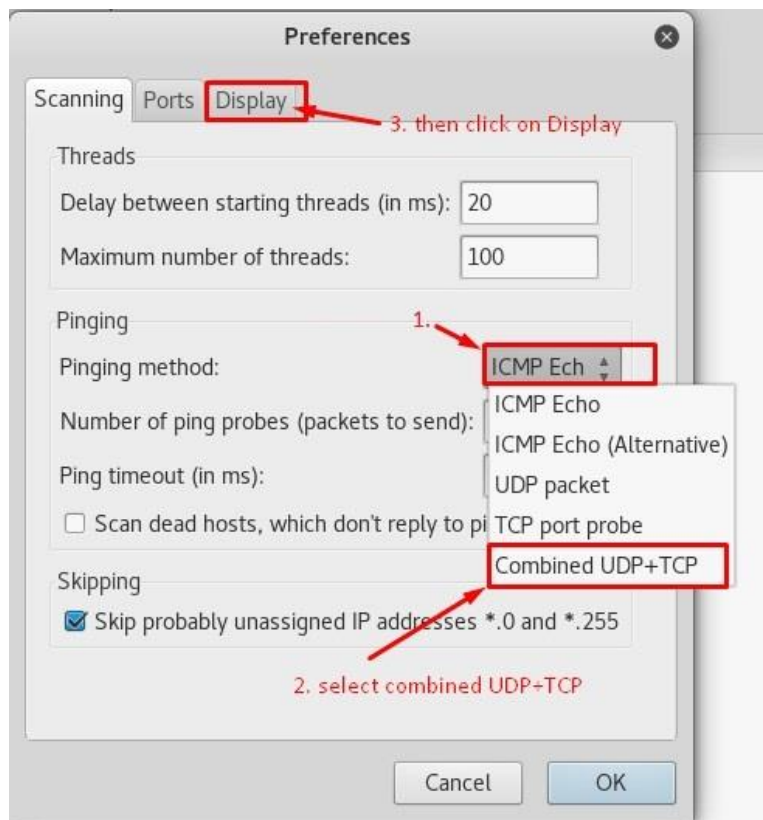
```
root@kali:~/Downloads# dpkg -i ipscan 3.5.2 amd64.deb
(Reading database ... 350923 files and directories currently installed.)
Preparing to unpack ipscan_3.5.2_amd64.deb ...
Unpacking ipscan (3.5.2-1) over (3.5.2-1) ...
Setting up ipscan (3.5.2-1) ...
Processing triggers for gnome-menus (3.13.3-11) ...
Processing triggers for desktop-file-utils (0.23-3) ...
Processing triggers for mime-support (3.60) ...
root@kali:~/Downloads#
```

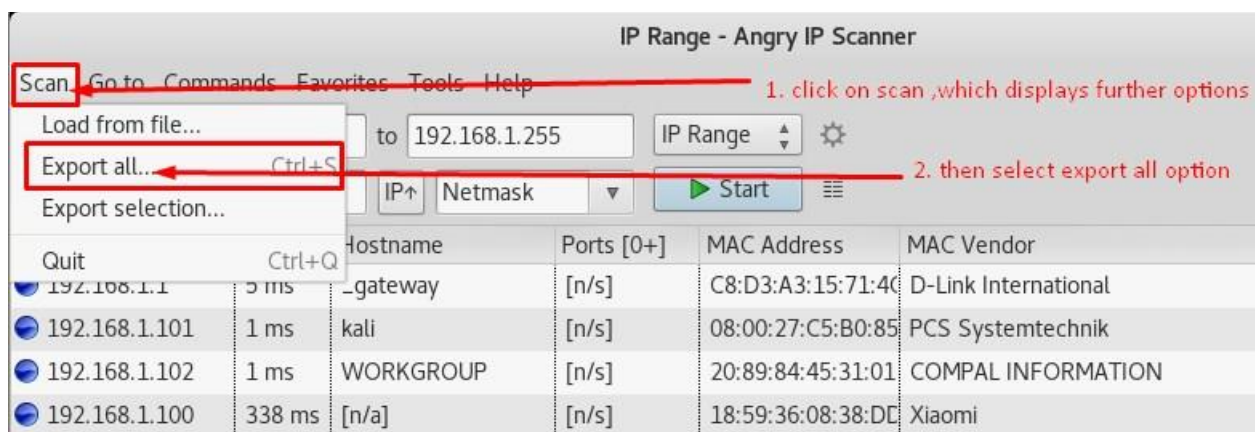
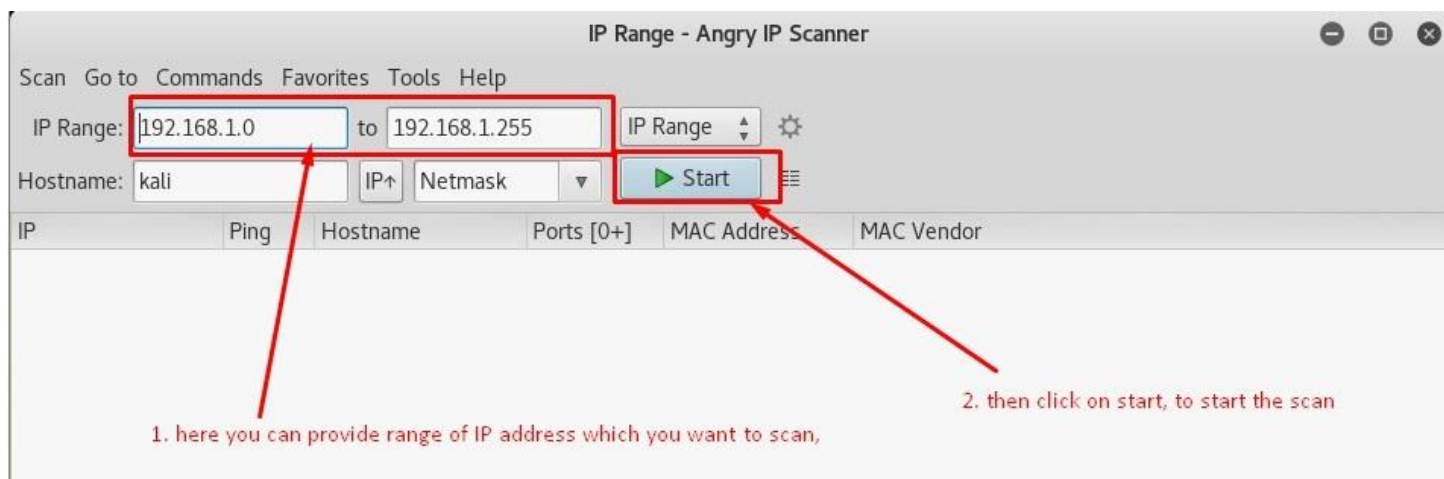
dpkg -i command is used to install .deb file in kali linux. here we took dpkg command to install angryip software

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.

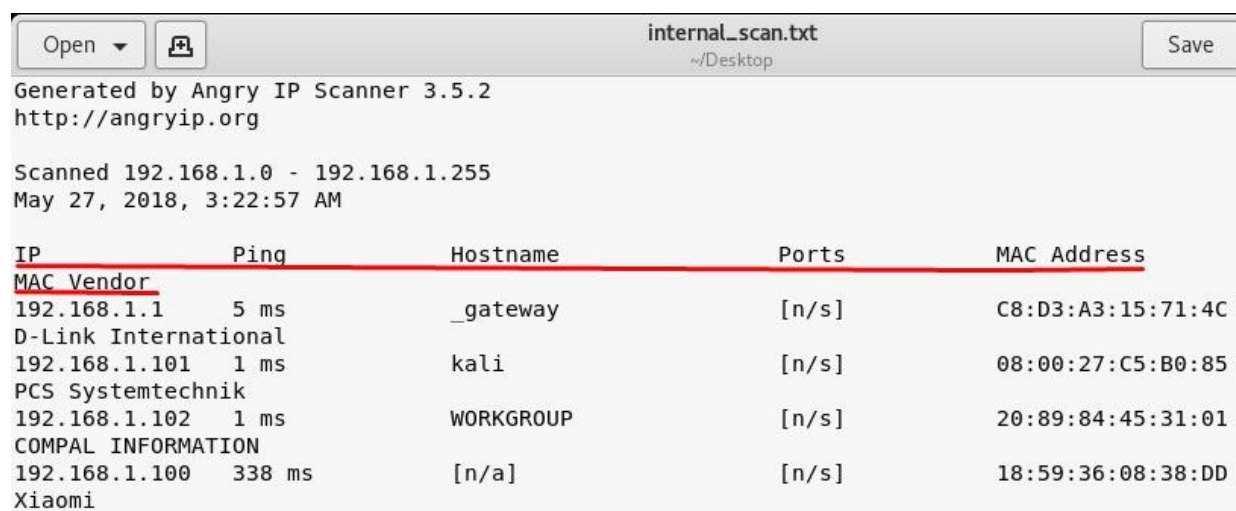








Export the scan results to a text file. We can use this output file to feed it to another VA tools or port scanner tools.



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% → ip is not active,
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 → ip address is active
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
```


Practical 3: Network Scanning With netdiscover

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

for example: ***netdiscover -i eth0***

```
root@kali:~# netdiscover -i eth0
Currently scanning: 192.168.7.0/16 | Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 4 hosts. Total size: 300

-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.1.1   a4:2b:8c:fb:16:ec    2     120  NETGEAR
192.168.1.4   74:de:2b:90:31:d4    1      60  Liteon Technology Corporation
192.168.1.3   80:58:f8:16:9f:bd    1      60  Unknown vendor
192.168.1.2   94:65:2d:08:0d:69    1      60  OnePlus Technology (Shenzhen) Co., Ltd
```

Practical 4: Ping Sweeping with nmap

In Kali Linux terminal type the following command

nmap -sn 192.168.1.1/24

```
root@kali:~# route -n Estimated time to completion: 1 to 2 minutes
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.1.1    0.0.0.0         UG      100    0      0 eth0
192.168.1.0      0.0.0.0        255.255.255.0   U       0      0      0 eth0
192.168.1.0      0.0.0.0        255.255.255.0   U      100    0      0 eth0
root@kali:~# nmap -sn 192.168.1.1/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-24 07:51 IST
Nmap scan report for www.routerlogin.com (192.168.1.1)
Host is up (0.0016s latency).
MAC Address: A4:2B:8C:FB:16:EC (Netgear)
Nmap scan report for 192.168.1.2
Host is up (0.034s latency).
MAC Address: 94:65:2D:08:0D:69 (OnePlus Technology (Shenzhen))
Nmap scan report for 192.168.1.3
Host is up (0.032s latency).
MAC Address: 80:58:F8:16:9F:BD (Motorola Mobility, a Lenovo Company)
Nmap scan report for 192.168.1.4
Host is up (0.00016s latency).
MAC Address: 74:DE:2B:90:31:D4 (Liteon Technology)
Nmap scan report for 192.168.1.7
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 43.70 seconds
```

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)

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

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

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`

```
root@kali:~# nmap -sV 192.168.0.137
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-27 05:56 EDT
Nmap scan report for 192.168.0.137
Host is up (0.028s latency).
Not shown: 977 closed ports
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
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         netkit-rsh rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
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: 02:25:98:60:ED:4F (Unknown)
Service Info: Hosts: metasploitable.localdomain, localhost, 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 13.57 seconds
root@kali:~#
```

results displays the software with their versions which are running on open-ports

4. OS Detection Scan:

`nmap -O <target IP or domain>`

Example: `nmap -O example.com`

`nmap -O 192.168.0.137`

```
root@kali:~# nmap -O 192.168.0.137
```

```
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)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
```

Based on open and closed ports, this scan finds out the OS running on target ip.

NOTE: this scan needs atleast 2 open and 2 closed ports to identify OS.

5. FIN scan (FIN Flag):

`nmap -sF <target IP or domain>`

Example: `nmap -sF example.com`

`nmap -sF 192.168.0.137 -v`

```
root@kali:~# nmap -sF 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 (0.00028s 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 1.86 seconds
root@kali:~# nmap -sF 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 (0.016s 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 1.49 seconds
```

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

```
root@kali:~# nmap -A 192.168.1.9
Starting Nmap 7.70 ( https://nmap.org ) at 2018-07-08 17:34 IST
Nmap scan report for 192.168.1.9
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey:
|   1024 50:ca:0d:3f:43:28:f7:fe:51:27:68:df:11:df:1f:8e (DSA)
|   2048 a5:ee:aa:1c:da:34:67:fd:87:08:dc:bb:a6:34:58:e8 (RSA)
23/tcp    open  telnet   VyOS telnetd
MAC Address: 00:0C:29:21:AE:8C (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   1.21 ms  192.168.1.9
```

9. UDP port scan:

`nmap -sU <target IP or domain>`

Example: `nmap -sU example.com`

`nmap -sU 192.168.0.137`

```
root@kali:~# nmap -sU 192.168.1.9
Starting Nmap 7.70 ( https://nmap.org ) at 2018-07-08 17:19 IST
Nmap scan report for 192.168.1.9
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
68/udp    open|filtered dhcpc
123/udp   open      ntp
161/udp   open      snmp
MAC Address: 00:0C:29:21:AE:8C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1091.64 seconds
```


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).
Estimated time to completion: 1 to 2 minutes

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
```