WEEK-1

AIM:-

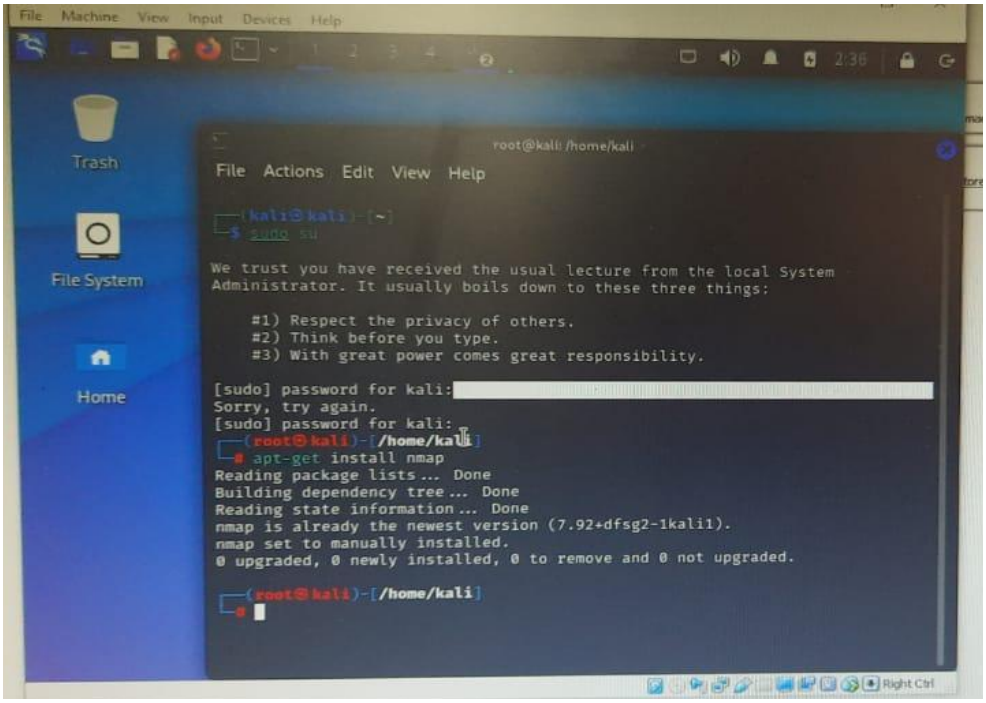
About nmap and tools introduction

PROGARM:-

Nmap is a network scanning tool that uses IP packets to identify all the devices connected to a network and to provide information on the services and operating systems they are running.

cmd: sudo su

apt-get install nmap



Scanning networks that you do not have permission to scan can get you in

trouble with your internet service provider, the police, and possibly even the

government. Don’t go off scanning the FBI or Secret Service websites unless you

i want to get in trouble.

Aggressively scanning some systems may cause them to crash which can

lead to undesirable results like system downtime and data loss. Always scan

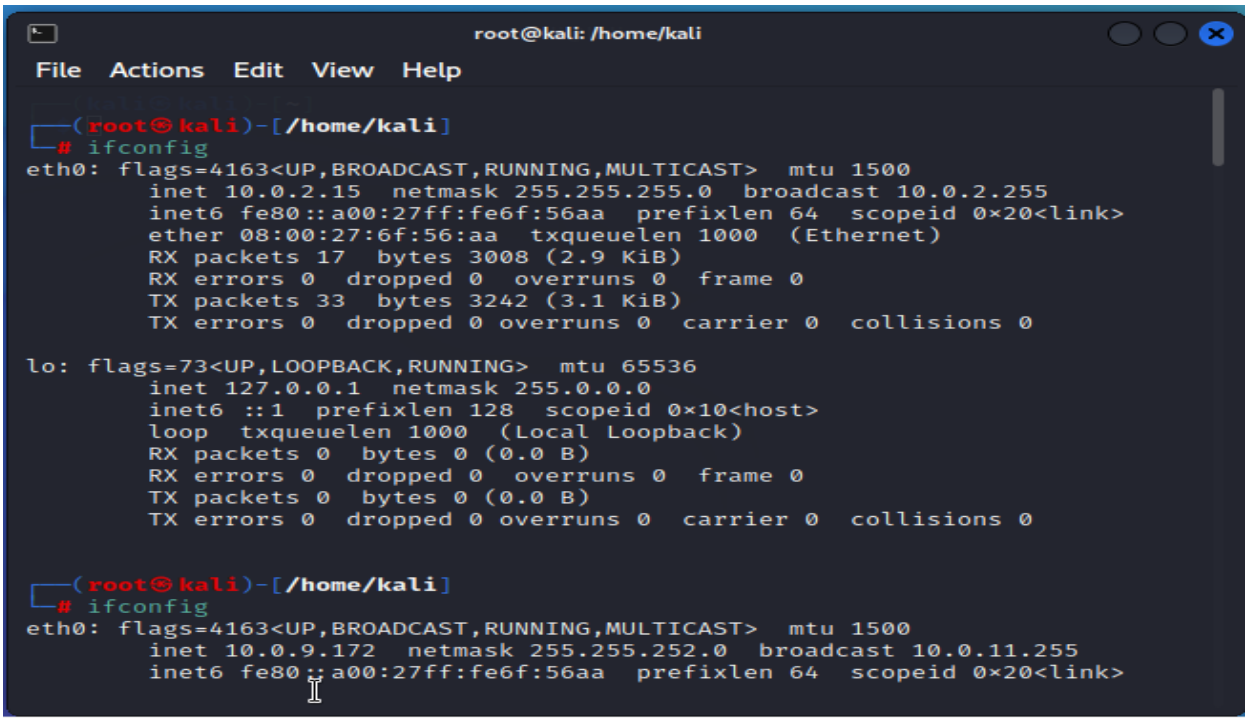
mission critical systems with caution.

Host Scanning

Host scanning returns more detailed information on a particular host or a range of IP addresses. As mentioned above, you can perform a host scan using the following command:

nmap -sp <target IP range>

cmd: if config



You can use the **ifconfig** command to assign an address to a network interface and to

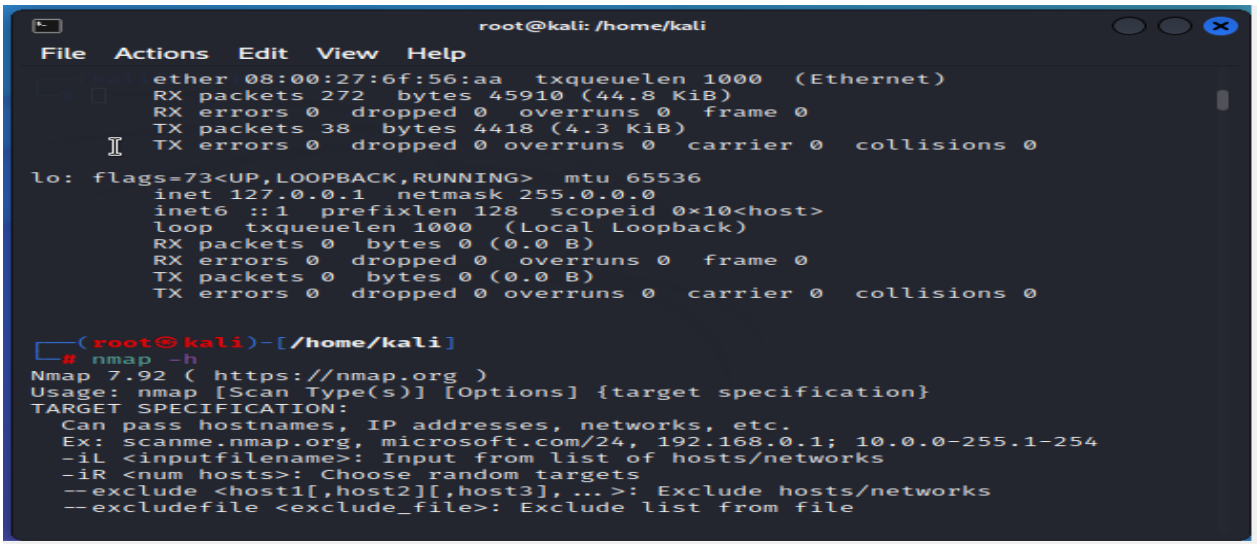
configure or display the current network interface configuration information. The

ifconfig command must be used at system startup to define the network address of

each interface present on a system. After system startup, it can also be used to

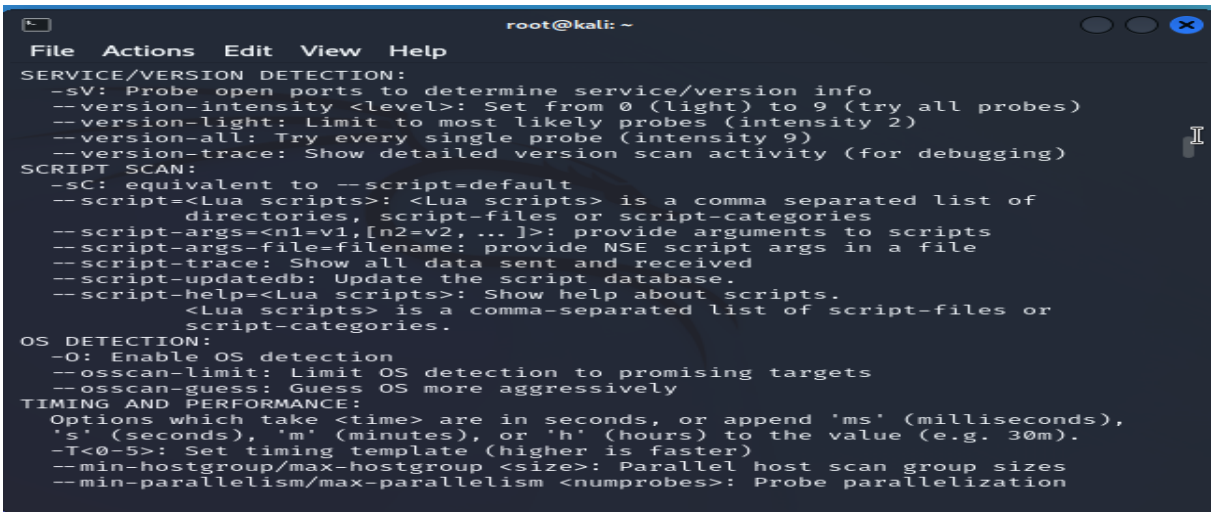
redefine an interfaces address and its other operating parameters.

cmd: nmap -h



The **ifconfig** function displays the current configuration for a network interface when no optional parameters are supplied.

If a protocol family is specified, **ifconfig** reports only the details specific to that protocol family.



Syntaxes

ifconfig *interface* [*addressfamily* [*address* [*destinationaddress*]] [*parameters*...]]

ifconfig *interface* [*protocolfamily*] *interface protocolfamily*

ifconfig -a [**-l**] [**-d**] [**-u**] [*protocolfamily*]

ifconfig *interface* [**tcp_low_rto** *rto* | **-tcp_low_rto**]

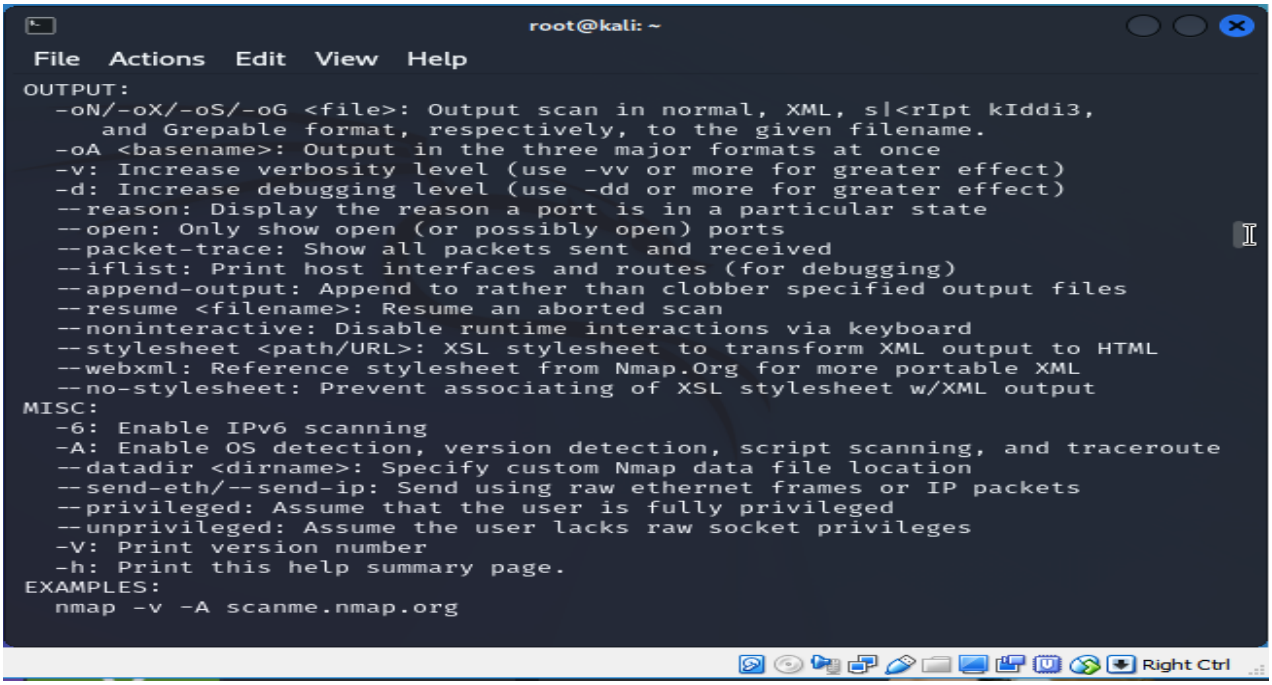
Configures or displays network interface parameters for a network by using TCP/IP.

Ping Scanning

Ping scan returns information on every active IP on your network. You can execute a

ping scan using this command:

nmap -sp 192.100.1.1/24



Scan an Entire Subnet

Nmap can be used to scan an entire subnet using CIDR (Classless Inter-Domain Routing) notation.

cmd: nmap 10.0.9.1/24

nmap --top-ports 20 192.168.1.106

Replace the “20” with the number of ports to scan, and Nmap quickly scans that many ports. It returns a concise output that details the status of the most common ports, and this lets you quickly see whether you have any unnecessarily open ports.

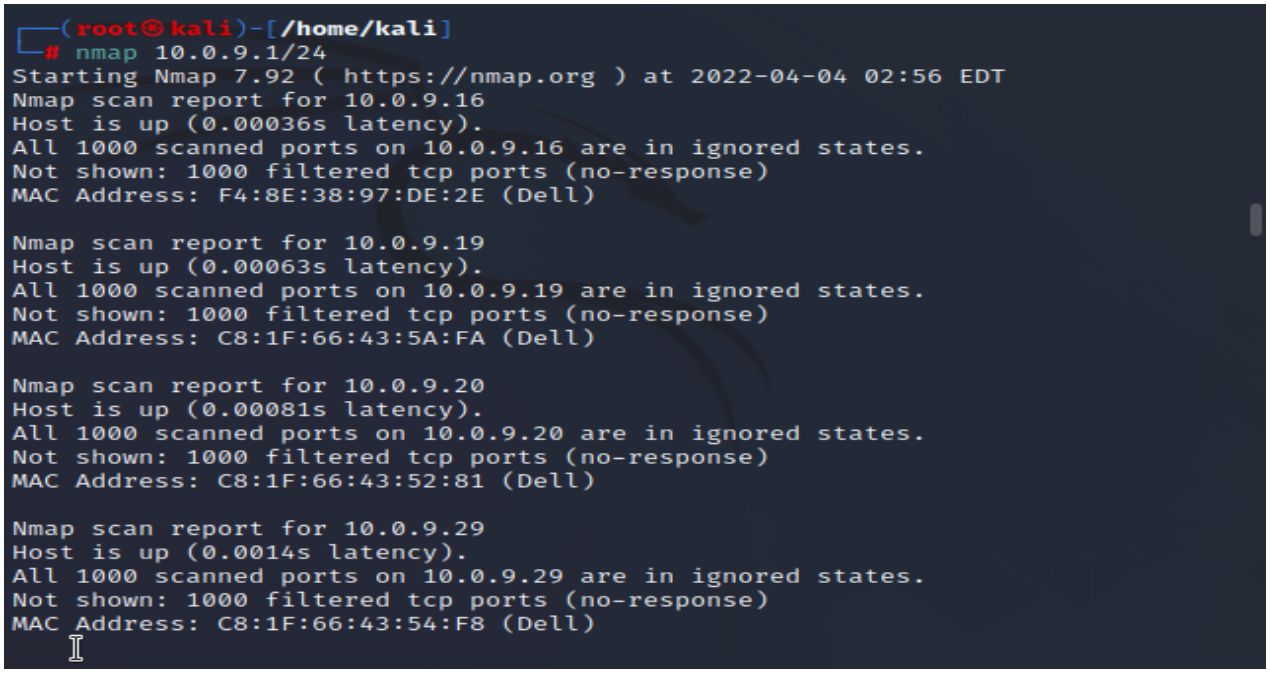
OS scanning is one of the most powerful features of Nmap. When using this type of scan, Nmap sends TCP and UDP packets to a particular port, and then analyze its response. It compares this response to a database of 2600 operating

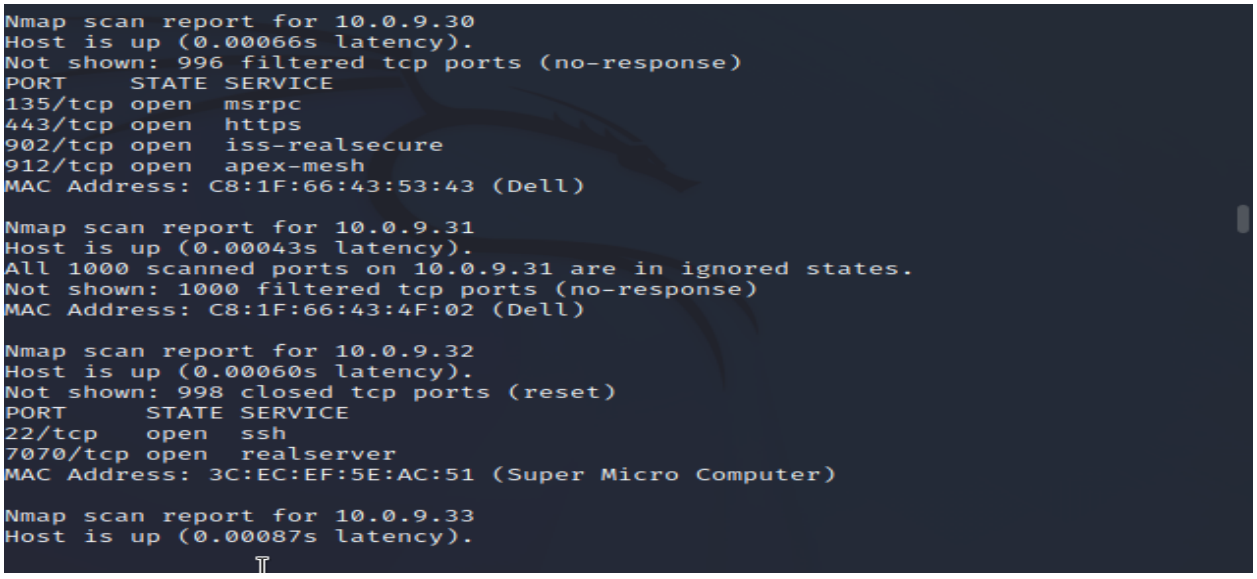
systems, and return information on the OS (and version) of a host.

To run an OS scan, use the following command:

nmap -O <target IP>

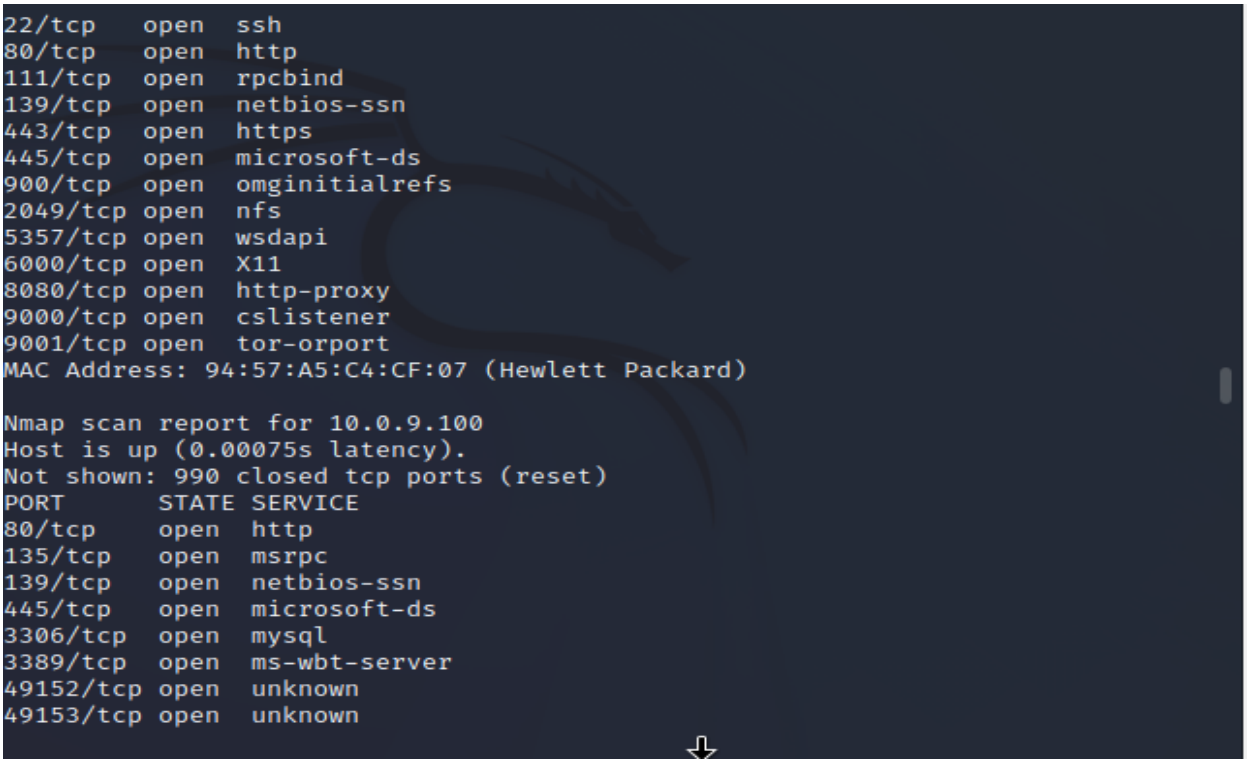
cmd: nmap 10.0.9.1/24

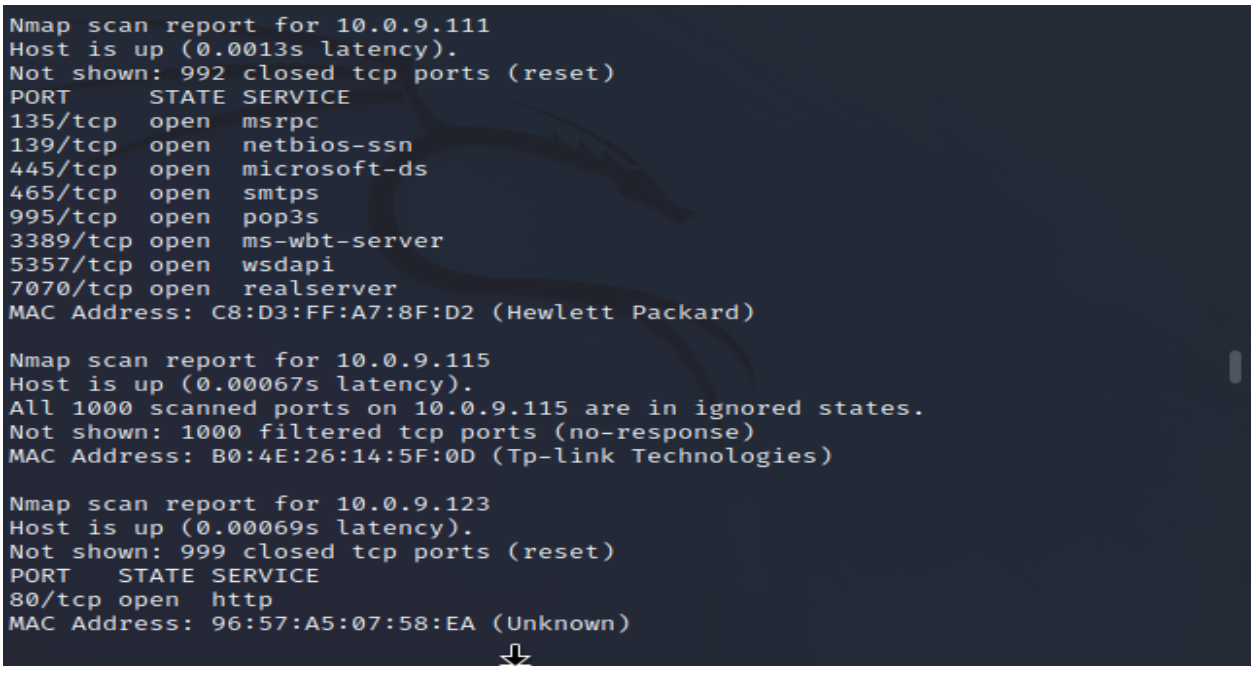




Nmap has the capability of scanning multiple hosts simultaneously. This feature comes in real handy when you are managing vast network infrastructure.

cmd: nmap 10.0.9.1/24





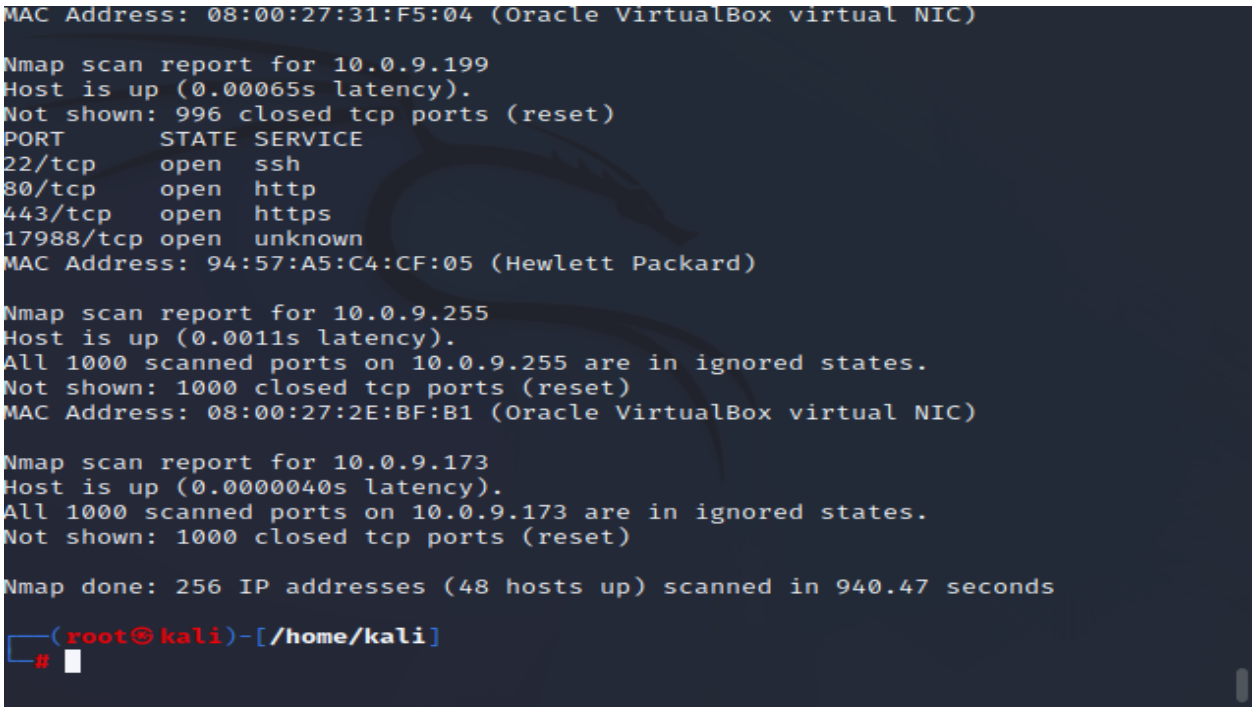
Write all the IP addresses in a single row to scan all of the hosts at the same time.> nmap 192.164.1.1 192.164.0.2 192.164.0.2

```
Host is up (0.0014s latency).
All 1000 scanned ports on 10.0.9.163 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:1F:DF:E1 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.9.164
Host is up (0.0010s latency).
All 1000 scanned ports on 10.0.9.164 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:1B:32:47 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.9.165
Host is up (0.00095s latency).
All 1000 scanned ports on 10.0.9.165 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:12:CF:B1 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.9.166
Host is up (0.0011s latency).
All 1000 scanned ports on 10.0.9.166 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:7E:4D:E9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.9.167
Host is up (0.00089s latency).
All 1000 scanned ports on 10.0.9.167 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

```
Host is up (0.00098s latency).
All 1000 scanned ports on 10.0.9.168 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:E6:A0:53 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.9.169
Host is up (0.00086s latency).
All 1000 scanned ports on 10.0.9.169 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:96:54:53 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.9.170
Host is up (0.00080s latency).
All 1000 scanned ports on 10.0.9.170 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:E1:0B:40 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.9.171
Host is up (0.00088s latency).
All 1000 scanned ports on 10.0.9.171 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:BE:18:F9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.9.172
Host is up (0.00076s latency).
All 1000 scanned ports on 10.0.9.172 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

Use the asterisk (*) to scan all of the subnets at once.> nmap 192.164.1.*

cmd: nmap 10.0.9.1/24



AIM:-

About nmap tools commands

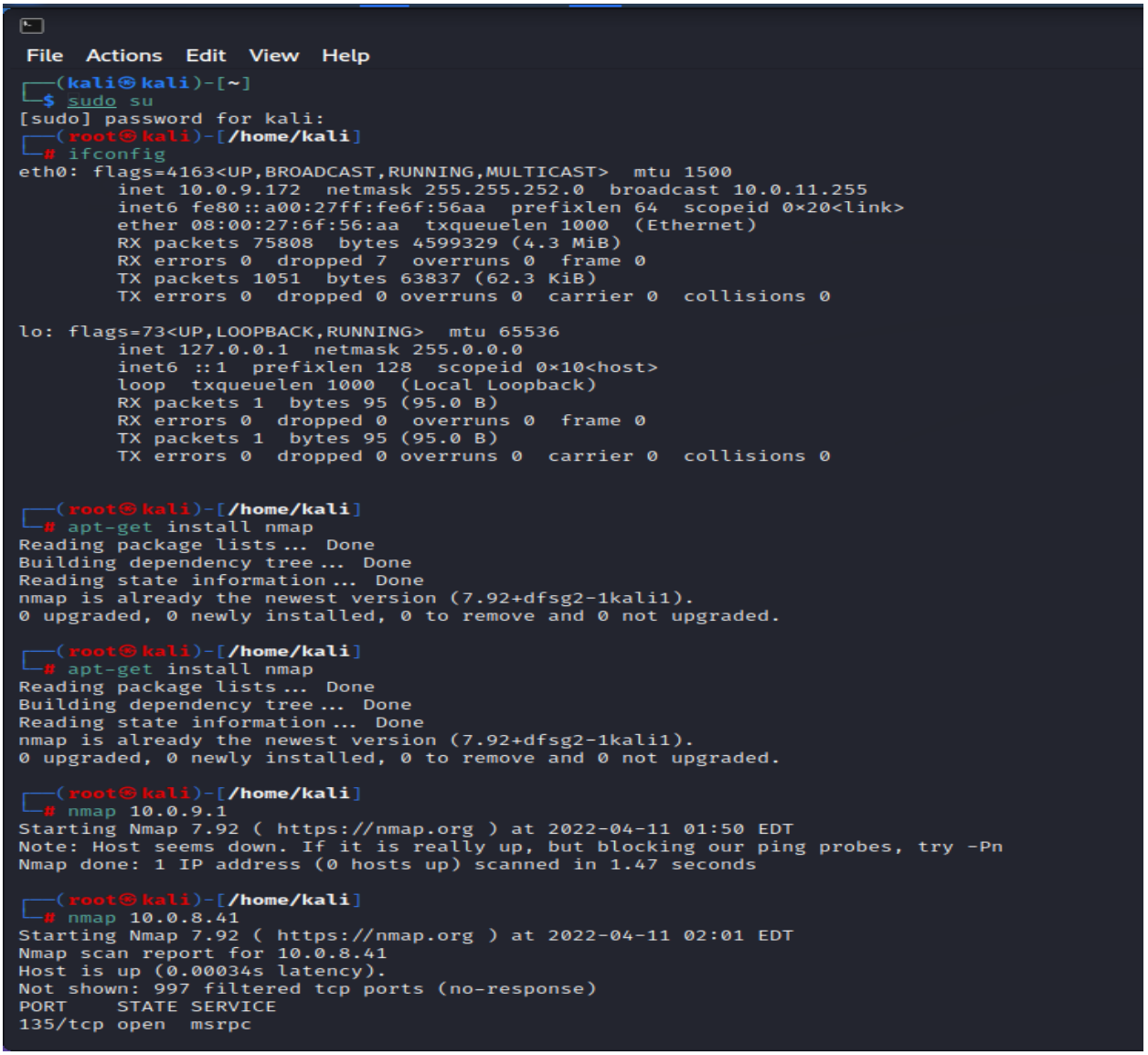
cmd: sudo su

ifconfig

apt-get install nmap

nmap 10.0.9.1

nmap 10..8.41



Don’t Ping

By default, before Nmap attempts to scan a system for open ports it will first ping the target to see if it is online. This feature helps save time when scanning as it causes targets that do not respond to be skipped.

In the above example the specified target is not scanned as it does not respond to Nmap’s pings. The **-PN** option instructs Nmap to skip the default discovery check and perform a complete port scan on the target. This is useful when scanning hosts that are protected by a firewall that blocks ping probes.

Ping Only Scan

The **-sP** option is used to perform a simple ping of the specified host.

When scanning a local network, you can execute Nmap with root privileges for additional ping functionality. When doing this, the **-sP** option will perform an ARP ping and return the MAC addresses of the discovered system(s).

Nmap supports several ping scanning techniques using different protocols. For example, the default ping scan command with no arguments (nmap -sn <target>) as a privileged user internally executes the -PS443 -PA80 -PE -PP options corresponding to TCP SYN to port 443, TCP ACK to port 80, and ICMP echo and timestamps requests.

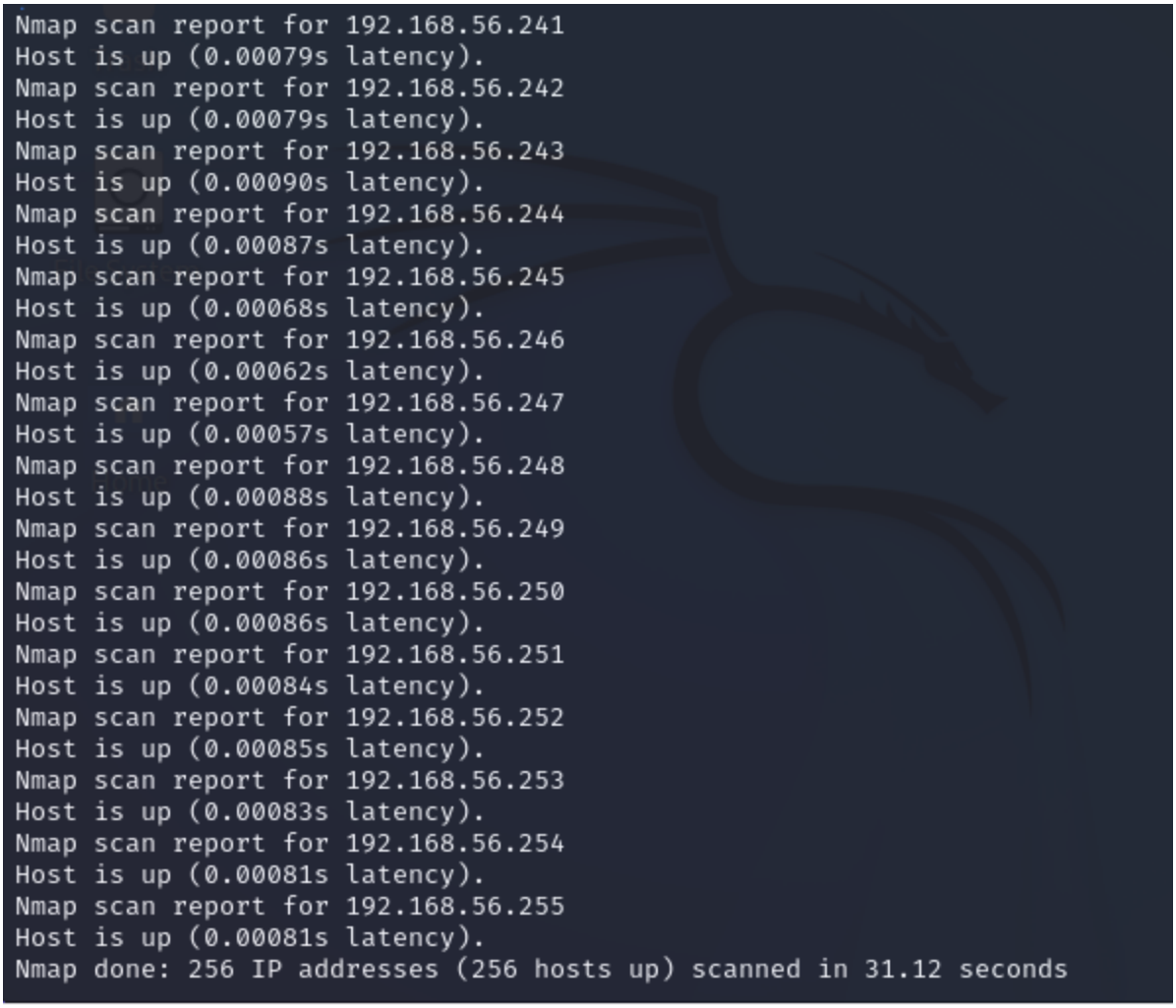
-sL (List Scan), -Pn (No ping), -PA <*port list*> (TCP ACK Ping)

-sn (No port scan), -PS <*port list*> (TCP SYN Ping), -PU <*port list*> (UDP Ping)

cmd: nmap -Pn 10.0.8.41

nmap -sP 192.168.56.1/24

```
File  Actions  Edit  View  Help
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 40:B0:34:F5:39:27 (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 11.56 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn 10.0.8.41
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-11 02:02 EDT
Nmap scan report for 10.0.8.41
Host is up (0.00036s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 40:B0:34:F5:39:27 (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sP 192.168.56.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-11 02:13 EDT
Nmap scan report for 192.168.56.0
Host is up (0.00044s latency).
Nmap scan report for 192.168.56.1
Host is up (0.00060s latency).
Nmap scan report for 192.168.56.2
Host is up (0.00062s latency).
Nmap scan report for 192.168.56.3
Host is up (0.00061s latency).
Nmap scan report for 192.168.56.4
Host is up (0.00059s latency).
Nmap scan report for 192.168.56.5
Host is up (0.00056s latency).
Nmap scan report for 192.168.56.6
Host is up (0.00054s latency).
Nmap scan report for 192.168.56.7
Host is up (0.00059s latency).
Nmap scan report for 192.168.56.8
Host is up (0.00059s latency).
Nmap scan report for 192.168.56.9
Host is up (0.00045s latency).
Nmap scan report for 192.168.56.10
Host is up (0.00041s latency).
Nmap scan report for 192.168.56.11
Host is up (0.00077s latency).
Nmap scan report for 192.168.56.12
Host is up (0.00078s latency).
Nmap scan report for 192.168.56.13
Host is up (0.00032s latency).
```



This option is useful when you want to perform a quick search of the target network

to see which hosts are online without actually scanning the target(s) for open ports.

In the above example, all 254 addresses in the 192.168.10.0 subnet are pinged and

results from live hosts are displayed.

A more powerful way to scan your networks is to use Nmap to perform a host scan.

Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts

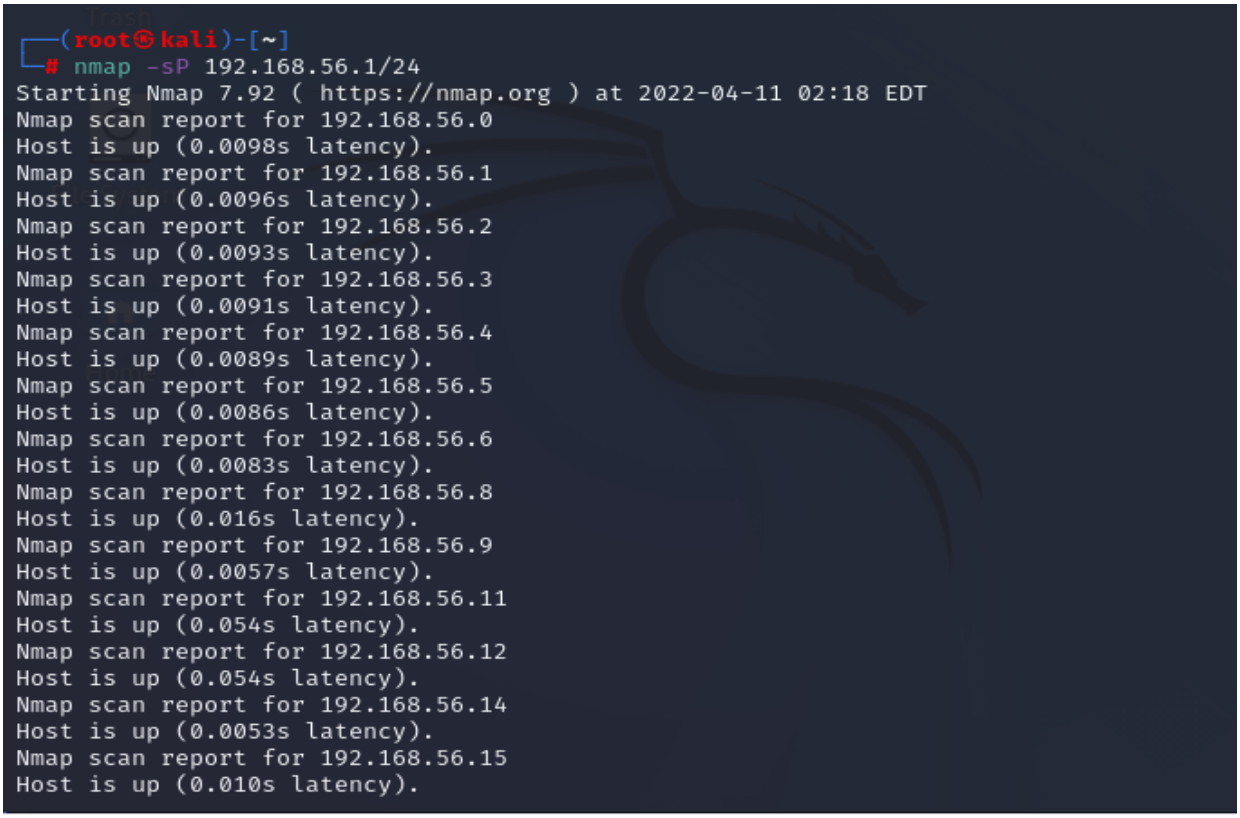
connected to your network. Each host then responds to this packet with another ARP

packet containing its status and MAC address.

To run a host scan, use the following command:

nmap -sp <target IP range>

cmd:nmap -sP 192.168.56.1/24



```
Host is up (0.010s latency).
Nmap scan report for 192.168.56.17
Host is up (0.0032s latency).
Nmap scan report for 192.168.56.18
Host is up (0.0030s latency).
Nmap scan report for 192.168.56.20
Host is up (0.028s latency).
Nmap scan report for 192.168.56.21
Host is up (0.032s latency).
Nmap scan report for 192.168.56.22
Host is up (1.1s latency).
Nmap scan report for 192.168.56.24
Host is up (0.021s latency).
Nmap scan report for 192.168.56.25
Host is up (0.032s latency).
Nmap scan report for 192.168.56.29
Host is up (0.015s latency).
Nmap scan report for 192.168.56.31
Host is up (0.019s latency).
Nmap scan report for 192.168.56.32
Host is up (0.019s latency).
Nmap scan report for 192.168.56.33
Host is up (0.018s latency).
Nmap scan report for 192.168.56.34
Host is up (0.018s latency).
Nmap scan report for 192.168.56.35
Host is up (0.018s latency).
Nmap scan report for 192.168.56.36
Host is up (0.017s latency).
Nmap scan report for 192.168.56.37
Host is up (0.017s latency).
```

```
Nmap scan report for 192.168.56.242
Host is up (0.073s latency).
Nmap scan report for 192.168.56.243
Host is up (0.0046s latency).
Nmap scan report for 192.168.56.244
Host is up (0.0042s latency).
Nmap scan report for 192.168.56.245
Host is up (0.072s latency).
Nmap scan report for 192.168.56.246
Host is up (0.072s latency).
Nmap scan report for 192.168.56.247
Host is up (0.072s latency).
Nmap scan report for 192.168.56.248
Host is up (0.071s latency).
Nmap scan report for 192.168.56.249
Host is up (0.071s latency).
Nmap scan report for 192.168.56.250
Host is up (0.071s latency).
Nmap scan report for 192.168.56.251
Host is up (0.016s latency).
Nmap scan report for 192.168.56.252
Host is up (0.012s latency).
Nmap scan report for 192.168.56.253
Host is up (1.3s latency).
Nmap scan report for 192.168.56.254
Host is up (0.027s latency).
Nmap scan report for 192.168.56.255
Host is up (0.031s latency).
Nmap done: 256 IP addresses (223 hosts up) scanned in 65.12 seconds
```

TCP SYN Ping

The **-PS** option performs a TCP SYN ping.

The TCP SYN ping sends a SYN packet to the target system and listens for a response. This alternative discovery method is useful for systems that are configured to block standard ICMP pings.

TCP ACK Ping

The **-PA** performs a TCP ACK ping on the specified target.

cmd: nmap -PS scanme.insecure.org

nmap -PU 192.168.171.1

```
┌──(root㉿kali)-[~]
└─# nmap -PS scanme.insecure.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-11 02:20 EDT
Nmap scan report for scanme.insecure.org (45.33.49.119)
Host is up (0.19s latency).
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed ident
443/tcp   open   https
31337/tcp closed Elite

Nmap done: 1 IP address (1 host up) scanned in 31.67 seconds

┌──(root㉿kali)-[~]
└─# nmap -Pu 192.168.171.1
Illegal Argument to -P, use -Pn, -PE, -PS, -PA, -PP, -PM, -PU, -PY, or -PO
QUITTING!

┌──(root㉿kali)-[~]
└─# nmap -PU 192.168.171.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-11 02:24 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.07 seconds

┌──(root㉿kali)-[~]
└─# nmap -PY 192.168.171.1
```

UDP Ping

The **-PU** option performs a UDP ping on the target system.

This discovery method sends UPD packets in an attempt to solicit a response from a target. While most firewalled systems will block this type of connection, some poorly configured systems may allow it if they are only configured to filter TCP connections.

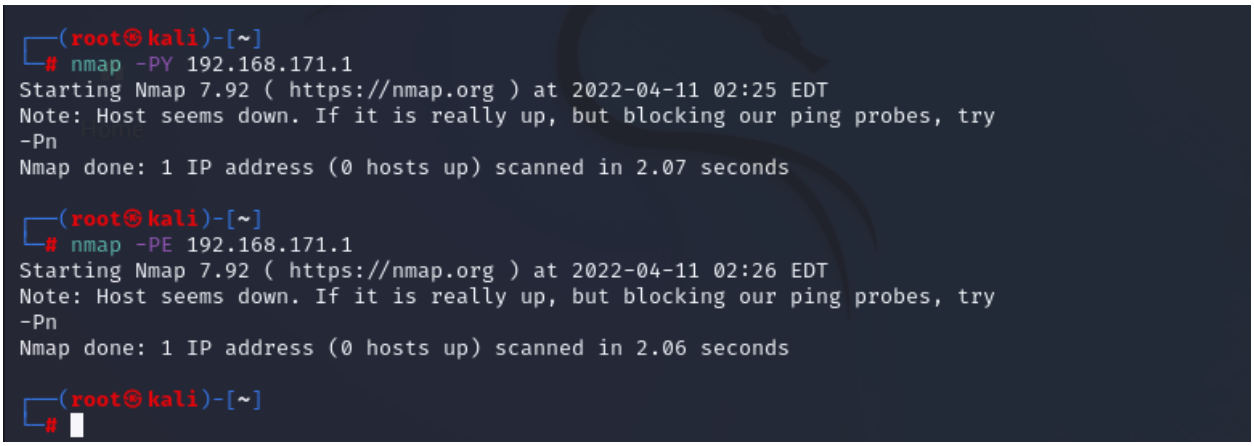
SCTP INIT Ping

The **-PY** parameter instructs Nmap to perform an SCTP INIT ping.

This discovery method attempts to locate hosts using the Stream Control Transmission Protocol (SCTP). SCTP is typically used on systems for IP based telephony.

cmd: nmap -PY 192.168.171.1

nmap -PE 192.168.171.1



ICMP Echo Ping

The **-PE** option performs an ICMP (Internet Control Message Protocol) echo ping on the specified system.

The **-PE** option sends a standard ICMP ping to the target to see if it replies. This type of discovery works best on local networks where ICMP packets can be transmitted with few restrictions. Many internet hosts, however, are configured not respond to ICMP packets for security reasons.

This option sends an SCTP packet containing a minimal INIT chunk. The default destination port is 80 (configurable at compile time by changing DEFAULT_SCTP_PROBE_PORT_SPEC in nmap.h). Alternate ports can be specified as a parameter. The syntax is the same as for the -p except that port type specifiers like S: are not allowed. Examples are -PY22 and -PY22,80,179,5060. Note that there can be no space between -PY and the port list. If multiple probes are specified they will be sent in parallel.

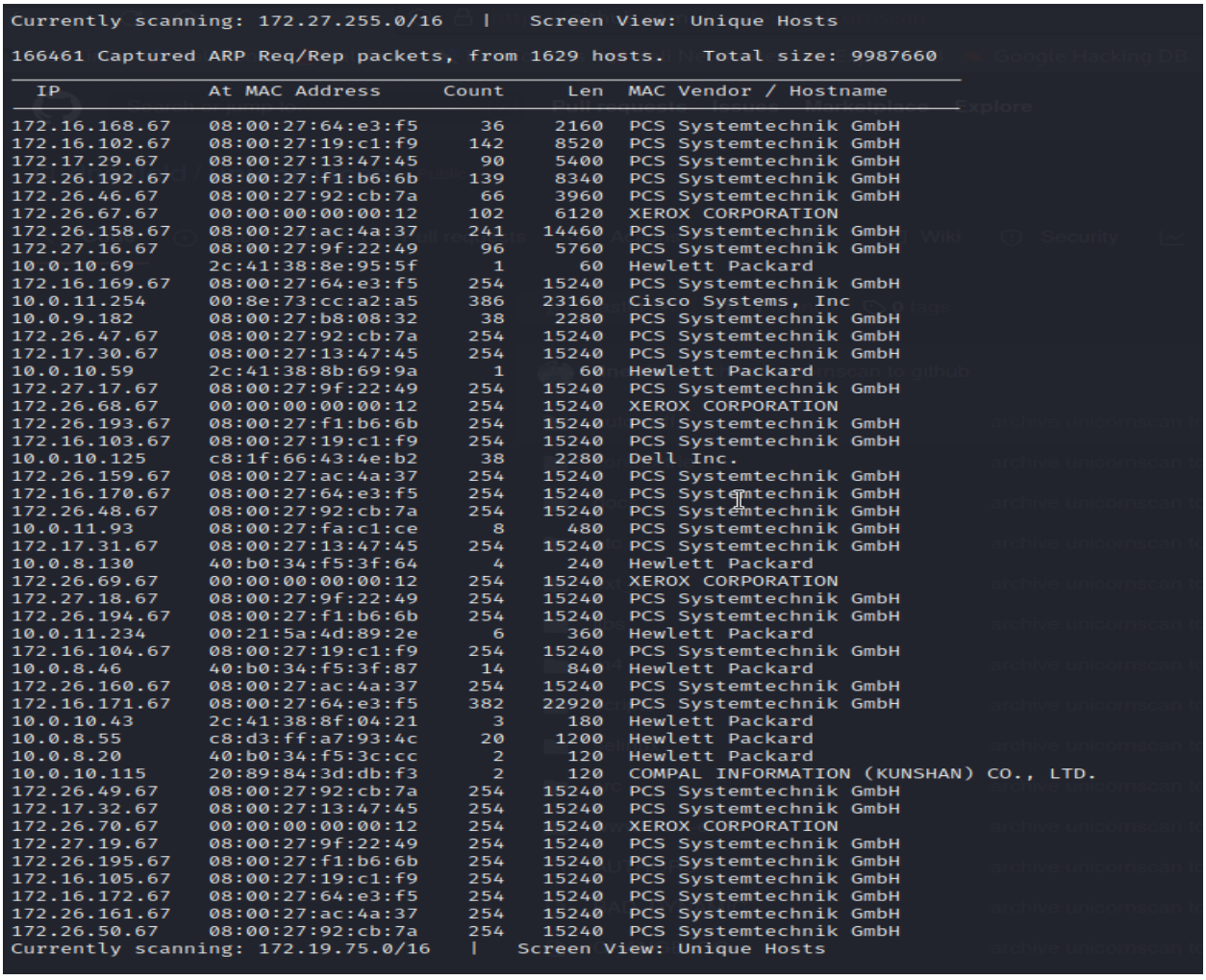
Nmap does not care whether the port is open or closed. Either the ABORT or INIT-ACK response discussed previously tell Nmap that the host is available and responsive.

On Unix boxes, only the privileged user root is generally able to send and receive raw SCTP packets. Using SCTP INIT Pings is currently not possible for unprivileged users.

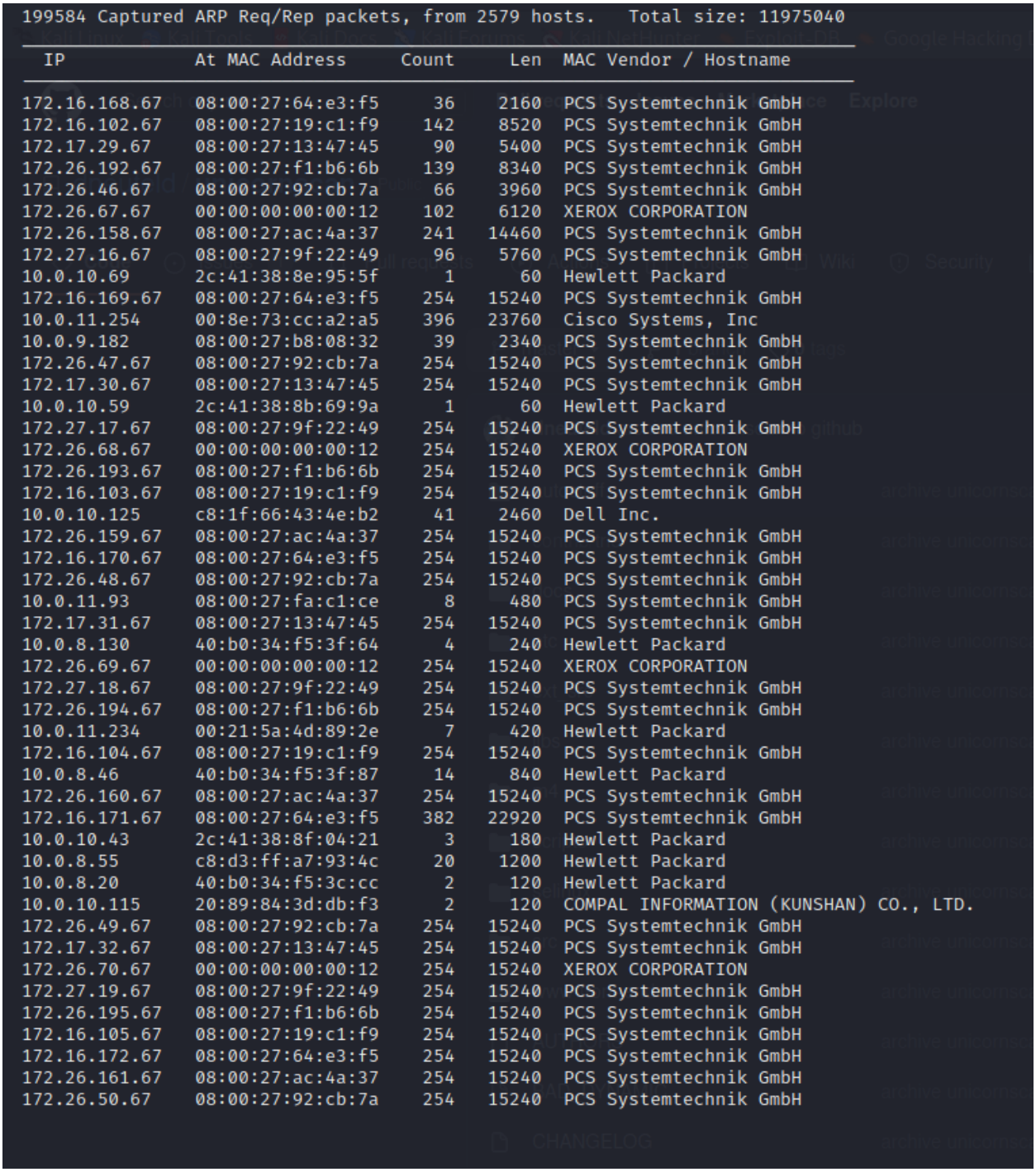
WEEK-2

Aim: Angry ip scanner

Procedure: Angry IP Scanner is a free, lightweight, cross-platform, and open source tool to scan networks. It helps you to scan a range of IP addresses to find live hosts, open ports, and other relevant information of each and every IP address.



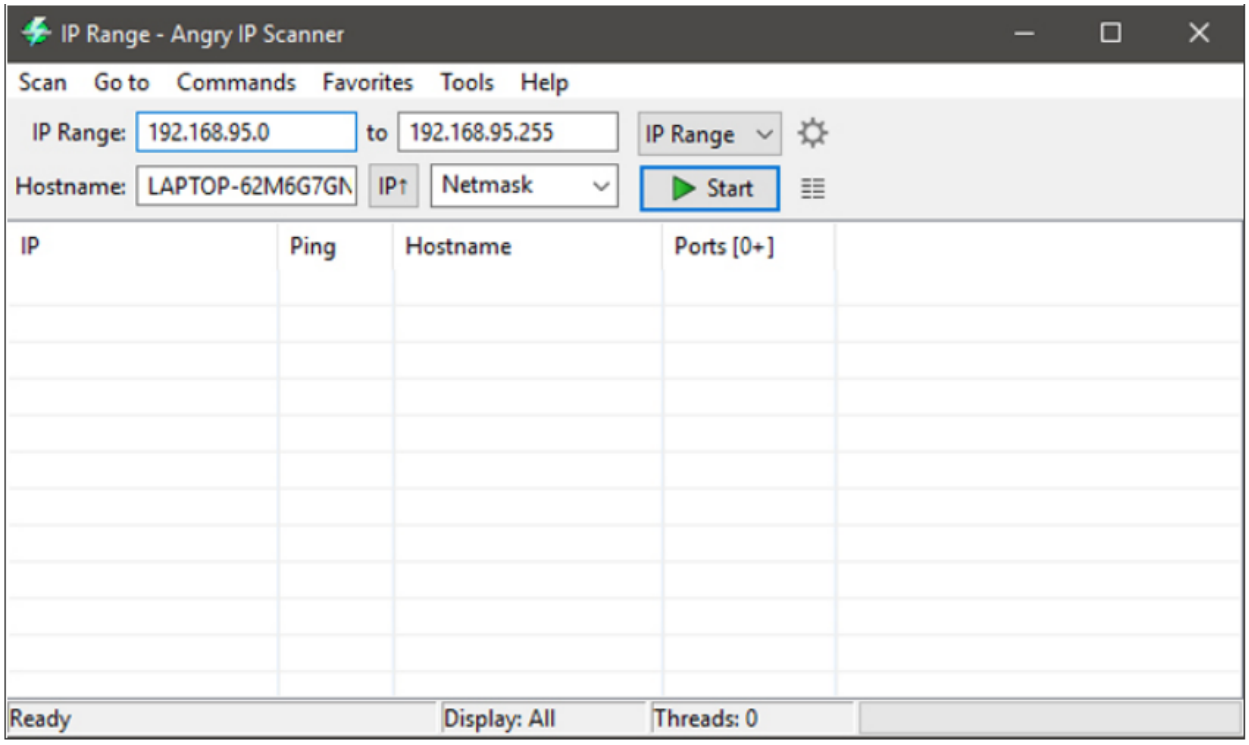
```
Currently scanning: 172.27.255.0/16   |   Screen View: Unique Hosts

166461 Captured ARP Req/Rep packets, from 1629 hosts.   Total size: 9987660
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
172.16.168.67   08:00:27:64:e3:f5     36    2160  PCS Systemtechnik GmbH
172.16.102.67   08:00:27:19:c1:f9    142    8520  PCS Systemtechnik GmbH
172.17.29.67    08:00:27:13:47:45     90    5400  PCS Systemtechnik GmbH
172.26.192.67   08:00:27:f1:b6:6b    139    8340  PCS Systemtechnik GmbH
172.26.46.67    08:00:27:92:cb:7a     66    3960  PCS Systemtechnik GmbH
172.26.67.67    00:00:00:00:00:12    102    6120  XEROX CORPORATION
172.26.158.67   08:00:27:ac:4a:37    241   14460  PCS Systemtechnik GmbH
172.27.16.67    08:00:27:9f:22:49     96    5760  PCS Systemtechnik GmbH
10.0.10.69      2c:41:38:8e:95:5f      1      60  Hewlett Packard
172.16.169.67   08:00:27:64:e3:f5    254   15240  PCS Systemtechnik GmbH
10.0.11.254     00:8e:73:cc:a2:a5    386   23160  Cisco Systems, Inc
10.0.9.182      08:00:27:b8:08:32     38    2280  PCS Systemtechnik GmbH
172.26.47.67    08:00:27:92:cb:7a    254   15240  PCS Systemtechnik GmbH
172.17.30.67    08:00:27:13:47:45    254   15240  PCS Systemtechnik GmbH
10.0.10.59      2c:41:38:8b:69:9a      1      60  Hewlett Packard
172.27.17.67    08:00:27:9f:22:49    254   15240  PCS Systemtechnik GmbH
172.26.68.67    00:00:00:00:00:12    254   15240  XEROX CORPORATION
172.26.193.67   08:00:27:f1:b6:6b    254   15240  PCS Systemtechnik GmbH
172.16.103.67   08:00:27:19:c1:f9    254   15240  PCS Systemtechnik GmbH
10.0.10.125     c8:1f:66:43:4e:b2     38    2280  Dell Inc.
172.26.159.67   08:00:27:ac:4a:37    254   15240  PCS Systemtechnik GmbH
172.16.170.67   08:00:27:64:e3:f5    254   15240  PCS Systemtechnik GmbH
172.26.48.67    08:00:27:92:cb:7a    254   15240  PCS Systemtechnik GmbH
10.0.11.93      08:00:27:fa:c1:ce      8     480  PCS Systemtechnik GmbH
172.17.31.67    08:00:27:13:47:45    254   15240  PCS Systemtechnik GmbH
10.0.8.130      40:b0:34:f5:3f:64      4     240  Hewlett Packard
172.26.69.67    00:00:00:00:00:12    254   15240  XEROX CORPORATION
172.27.18.67    08:00:27:9f:22:49    254   15240  PCS Systemtechnik GmbH
172.26.194.67   08:00:27:f1:b6:6b    254   15240  PCS Systemtechnik GmbH
10.0.11.234     00:21:5a:4d:89:2e      6     360  Hewlett Packard
172.16.104.67   08:00:27:19:c1:f9    254   15240  PCS Systemtechnik GmbH
10.0.8.46       40:b0:34:f5:3f:87     14     840  Hewlett Packard
172.26.160.67   08:00:27:ac:4a:37    254   15240  PCS Systemtechnik GmbH
172.16.171.67   08:00:27:64:e3:f5    382   22920  PCS Systemtechnik GmbH
10.0.10.43      2c:41:38:8f:04:21      3     180  Hewlett Packard
10.0.8.55       c8:d3:ff:a7:93:4c     20    1200  Hewlett Packard
10.0.8.20       40:b0:34:f5:3c:cc      2     120  Hewlett Packard
10.0.10.115     20:89:84:3d:db:f3      2     120  COMPAL INFORMATION (KUNSHAN) CO., LTD.
172.26.49.67    08:00:27:92:cb:7a    254   15240  PCS Systemtechnik GmbH
172.17.32.67    08:00:27:13:47:45    254   15240  PCS Systemtechnik GmbH
172.26.70.67    00:00:00:00:00:12    254   15240  XEROX CORPORATION
172.27.19.67    08:00:27:9f:22:49    254   15240  PCS Systemtechnik GmbH
172.26.195.67   08:00:27:f1:b6:6b    254   15240  PCS Systemtechnik GmbH
172.16.105.67   08:00:27:19:c1:f9    254   15240  PCS Systemtechnik GmbH
172.16.172.67   08:00:27:64:e3:f5    254   15240  PCS Systemtechnik GmbH
172.26.161.67   08:00:27:ac:4a:37    254   15240  PCS Systemtechnik GmbH
172.26.50.67    08:00:27:92:cb:7a    254   15240  PCS Systemtechnik GmbH
Currently scanning: 172.19.75.0/16   |   Screen View: Unique Hosts
```

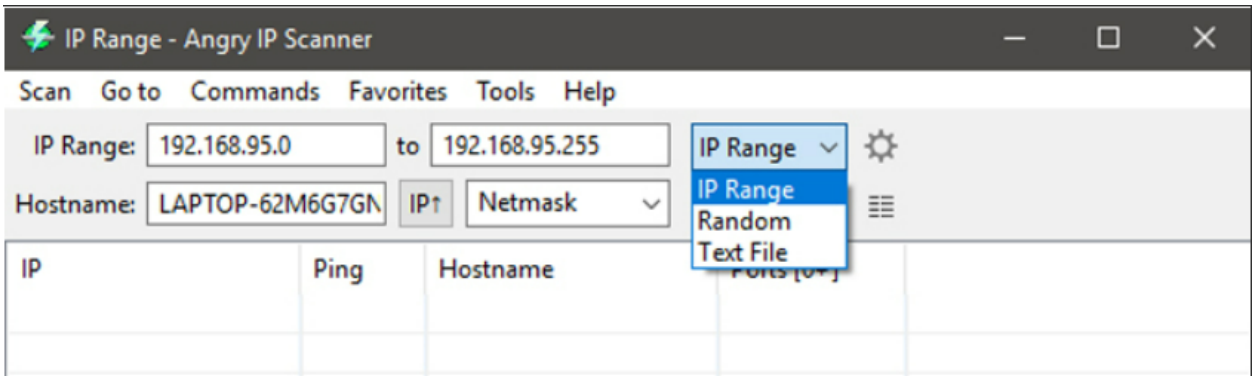


```
199584 Captured ARP Req/Rep packets, from 2579 hosts.   Total size: 11975040
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
172.16.168.67   08:00:27:64:e3:f5     36    2160  PCS Systemtechnik GmbH
172.16.102.67   08:00:27:19:c1:f9    142    8520  PCS Systemtechnik GmbH
172.17.29.67    08:00:27:13:47:45     90    5400  PCS Systemtechnik GmbH
172.26.192.67   08:00:27:f1:b6:6b    139    8340  PCS Systemtechnik GmbH
172.26.46.67    08:00:27:92:cb:7a     66    3960  PCS Systemtechnik GmbH
172.26.67.67    00:00:00:00:00:12    102    6120  XEROX CORPORATION
172.26.158.67   08:00:27:ac:4a:37    241   14460  PCS Systemtechnik GmbH
172.27.16.67    08:00:27:9f:22:49     96    5760  PCS Systemtechnik GmbH
10.0.10.69      2c:41:38:8e:95:5f      1      60  Hewlett Packard
172.16.169.67   08:00:27:64:e3:f5    254   15240  PCS Systemtechnik GmbH
10.0.11.254     00:8e:73:cc:a2:a5    396   23760  Cisco Systems, Inc
10.0.9.182      08:00:27:b8:08:32     39    2340  PCS Systemtechnik GmbH
172.26.47.67    08:00:27:92:cb:7a    254   15240  PCS Systemtechnik GmbH
172.17.30.67    08:00:27:13:47:45    254   15240  PCS Systemtechnik GmbH
10.0.10.59      2c:41:38:8b:69:9a      1      60  Hewlett Packard
172.27.17.67    08:00:27:9f:22:49    254   15240  PCS Systemtechnik GmbH
172.26.68.67    00:00:00:00:00:12    254   15240  XEROX CORPORATION
172.26.193.67   08:00:27:f1:b6:6b    254   15240  PCS Systemtechnik GmbH
172.16.103.67   08:00:27:19:c1:f9    254   15240  PCS Systemtechnik GmbH
10.0.10.125     c8:1f:66:43:4e:b2     41    2460  Dell Inc.
172.26.159.67   08:00:27:ac:4a:37    254   15240  PCS Systemtechnik GmbH
172.16.170.67   08:00:27:64:e3:f5    254   15240  PCS Systemtechnik GmbH
172.26.48.67    08:00:27:92:cb:7a    254   15240  PCS Systemtechnik GmbH
10.0.11.93      08:00:27:fa:c1:ce      8     480  PCS Systemtechnik GmbH
172.17.31.67    08:00:27:13:47:45    254   15240  PCS Systemtechnik GmbH
10.0.8.130      40:b0:34:f5:3f:64      4     240  Hewlett Packard
172.26.69.67    00:00:00:00:00:12    254   15240  XEROX CORPORATION
172.27.18.67    08:00:27:9f:22:49    254   15240  PCS Systemtechnik GmbH
172.26.194.67   08:00:27:f1:b6:6b    254   15240  PCS Systemtechnik GmbH
10.0.11.234     00:21:5a:4d:89:2e      7     420  Hewlett Packard
172.16.104.67   08:00:27:19:c1:f9    254   15240  PCS Systemtechnik GmbH
10.0.8.46       40:b0:34:f5:3f:87     14     840  Hewlett Packard
172.26.160.67   08:00:27:ac:4a:37    254   15240  PCS Systemtechnik GmbH
172.16.171.67   08:00:27:64:e3:f5    382   22920  PCS Systemtechnik GmbH
10.0.10.43      2c:41:38:8f:04:21      3     180  Hewlett Packard
10.0.8.55       c8:d3:ff:a7:93:4c     20    1200  Hewlett Packard
10.0.8.20       40:b0:34:f5:3c:cc      2     120  Hewlett Packard
10.0.10.115     20:89:84:3d:db:f3      2     120  COMPAL INFORMATION (KUNSHAN) CO., LTD.
172.26.49.67    08:00:27:92:cb:7a    254   15240  PCS Systemtechnik GmbH
172.17.32.67    08:00:27:13:47:45    254   15240  PCS Systemtechnik GmbH
172.26.70.67    00:00:00:00:00:12    254   15240  XEROX CORPORATION
172.27.19.67    08:00:27:9f:22:49    254   15240  PCS Systemtechnik GmbH
172.26.195.67   08:00:27:f1:b6:6b    254   15240  PCS Systemtechnik GmbH
172.16.105.67   08:00:27:19:c1:f9    254   15240  PCS Systemtechnik GmbH
172.16.172.67   08:00:27:64:e3:f5    254   15240  PCS Systemtechnik GmbH
172.26.161.67   08:00:27:ac:4a:37    254   15240  PCS Systemtechnik GmbH
172.26.50.67    08:00:27:92:cb:7a    254   15240  PCS Systemtechnik GmbH
```

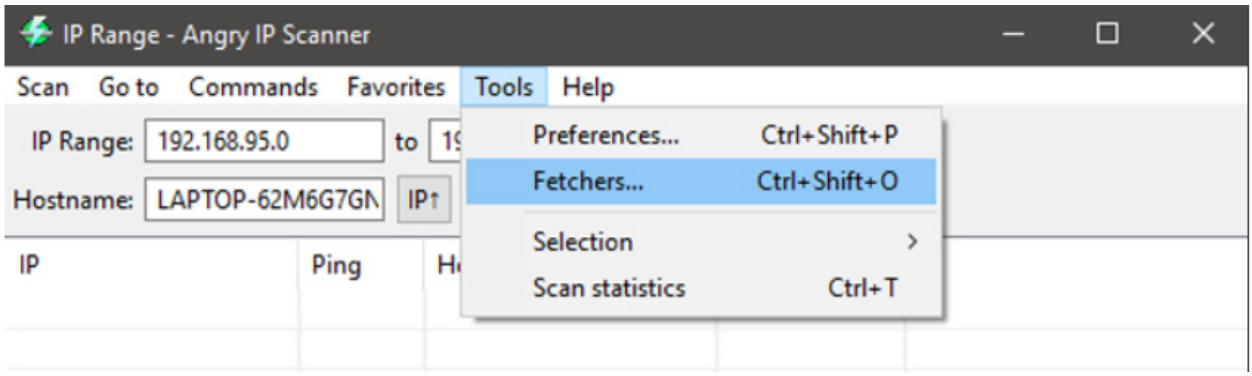
Once installed, open the application by searching for it in the Start Menu. As you can see, the home screen of the application is pretty simple and

straightforward. By default, Angry IP scanner will enter your local IP address range and your computer name as the hostname.

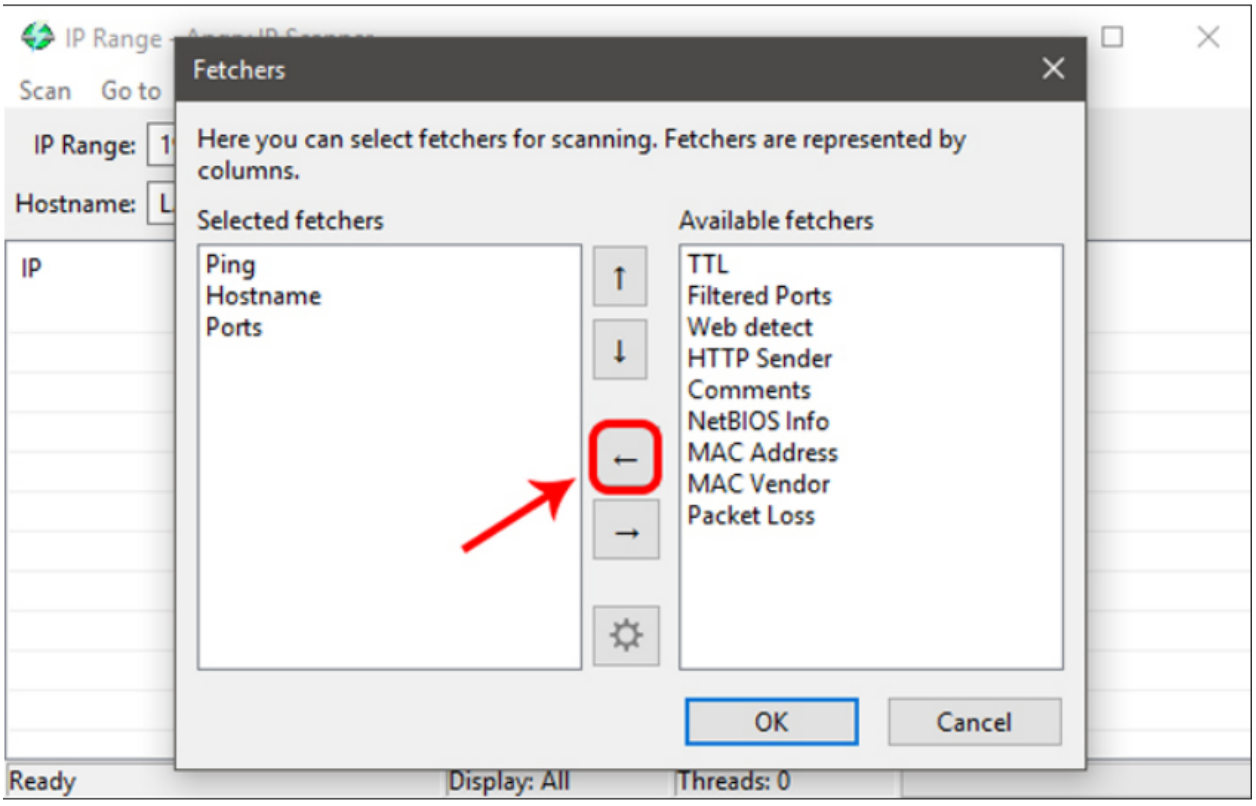




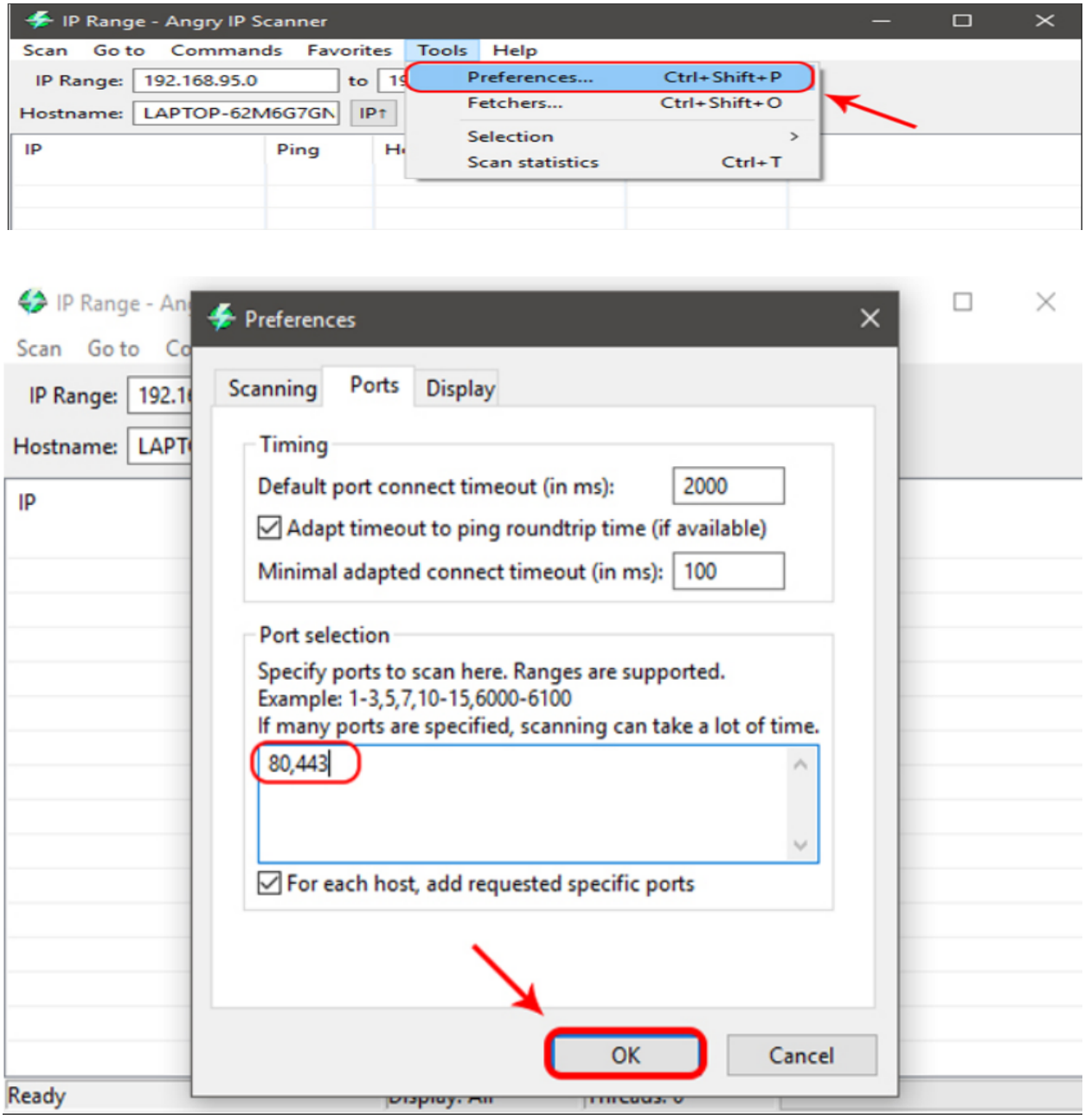
As you can see from the above image, the Angry IP Scanner will only include default fetchers like Ping, Hostname, and Ports. However, you can add more fetchers to get and see more information about an IP address. To do that, select “Tools > Fetchers.”



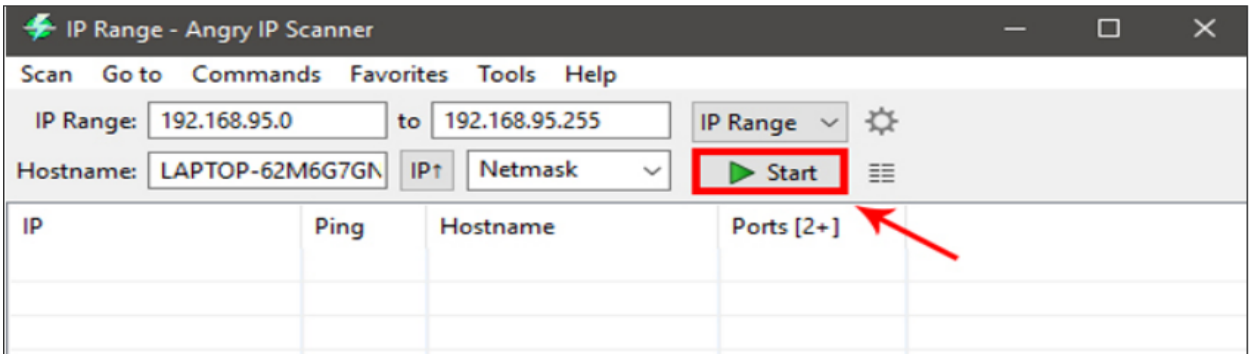
In this window, you will see all the current fetchers on the left pane and all the available fetchers in the right pane. To add a fetcher, select the fetcher on the right pane and then click on the button that looks like “Less than” sign. In my case, I’ve added new fetchers like MAC address, NetBIOS info, Filtered ports, and the Web detects.



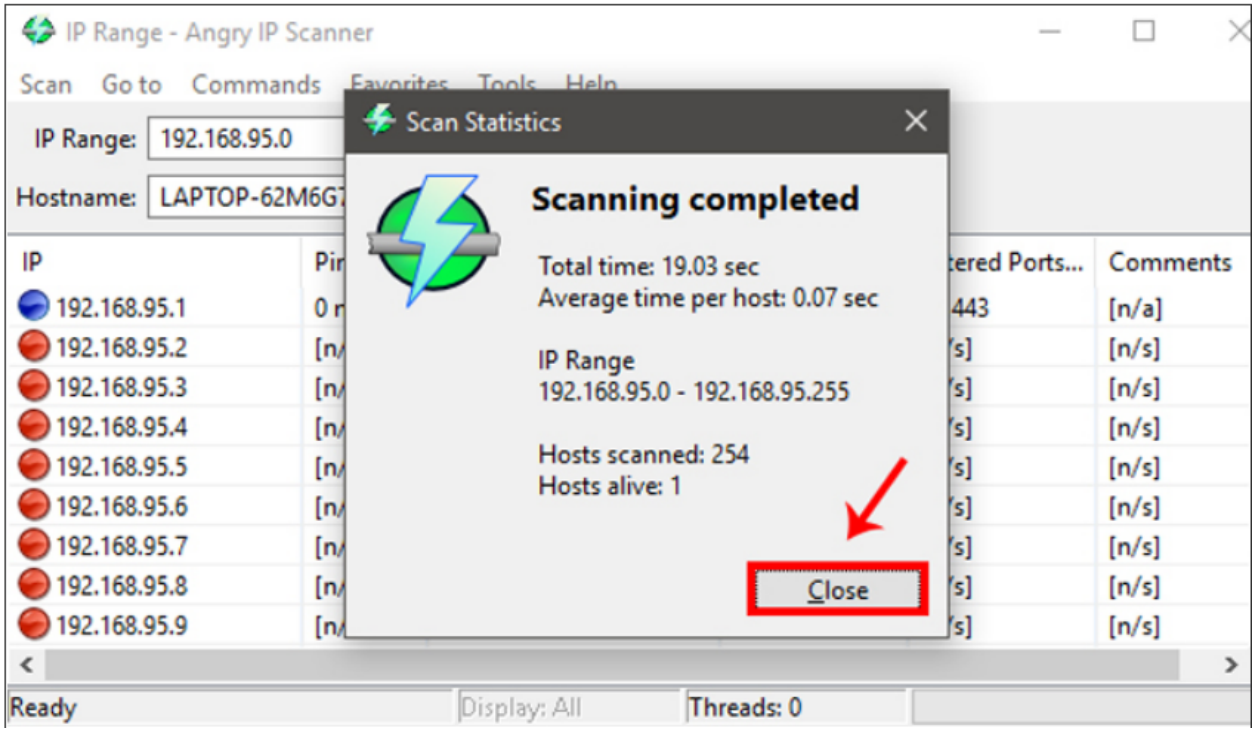
Moreover, Angry IP Scanner will only tell whether the ports are open or not. It will not list the individual ports that are open. So, if you want to do a port scan, then you need to configure the application. To do that, simply navigate to “Tools” and then select the option “Preferences.”



Once you are done configuring the Angry IP Scanner, you can continue to scan. To start off, set the scan mode to “IP Range,” enter the IP address range in the “IP address” fields and then click on the button “Start.” For instance, I’ve entered an IP range that is known to have live devices connected to it.



Depending on the number of addresses in the range, it may take some time to complete. Once completed, the application will show you a summary of the scan. The summary includes the number of hosts that are alive and the number of hosts that have open ports. Just click on the button “Close” to continue.

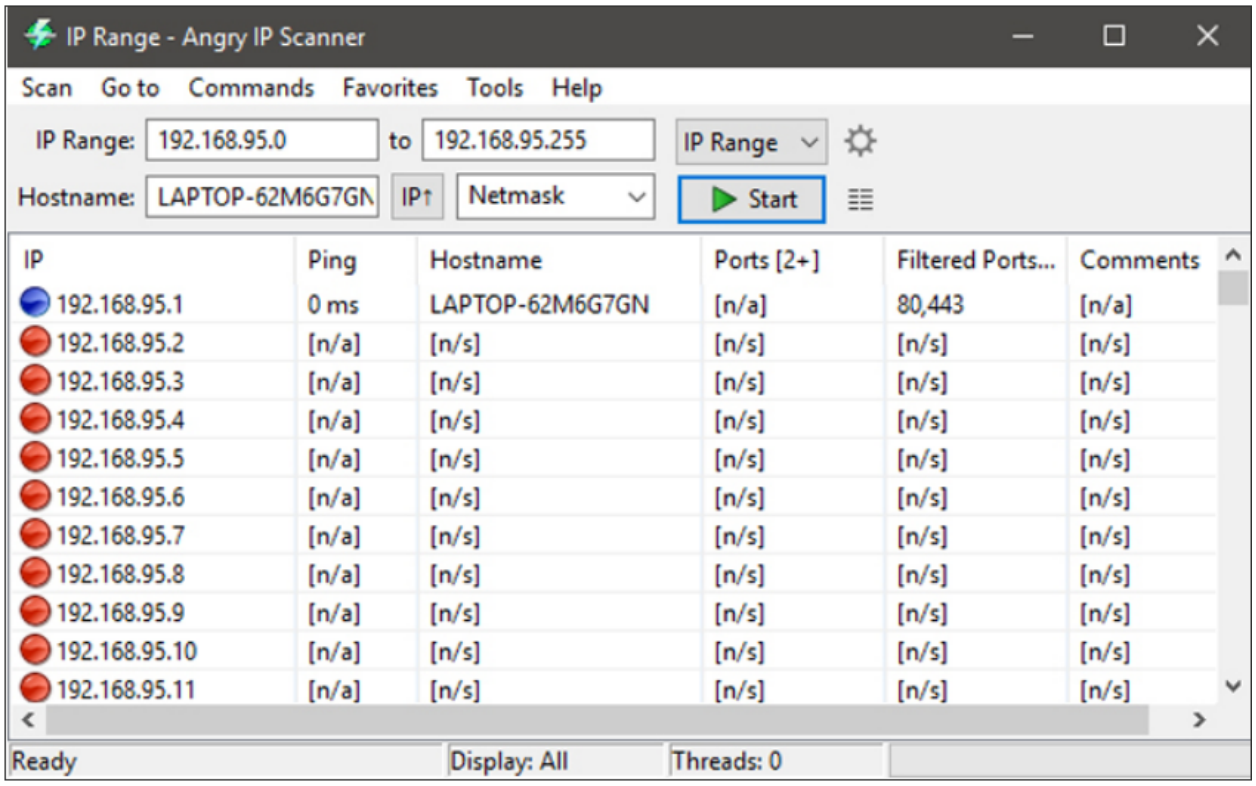


Once you close the summary window, you will see the list of all the IP address. You can also see additional details in different “fetcher” columns. In case you are wondering, here’s what the colored dots next to each IP address mean.

Red: The IP address is inactive, dead or there is no device connected to this IP address.

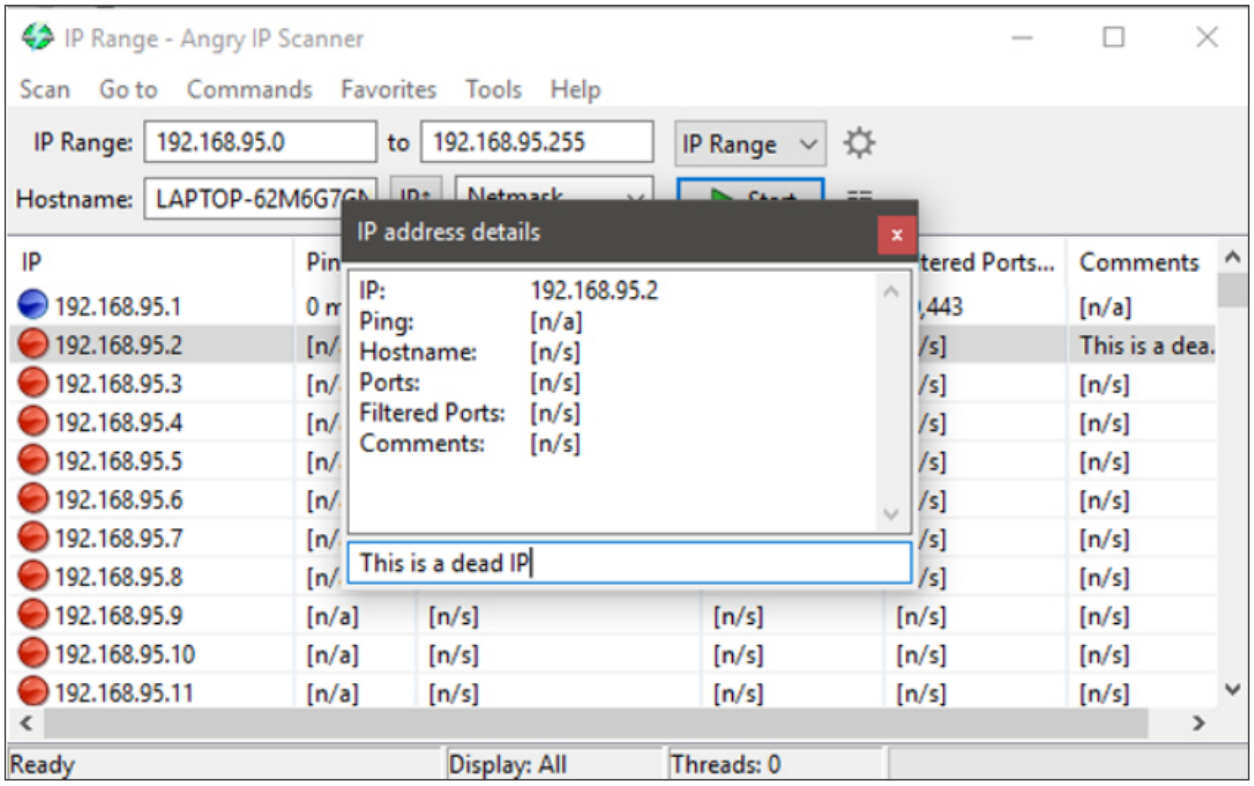
Blue: The IP address is either active or busy and not responding to the requests sent by Angry IP Scanner. This usually will be your own IP Address.

Green: The IP address is active, and the device connected to it is responding to the requests made by Angry IP Scanner. There may also be open ports.



By double-clicking on any IP address, Angry IP Scanner will show you all the details that it has gathered in a simple summary window. You can also add your own comments in the blank field at the bottom of the window.

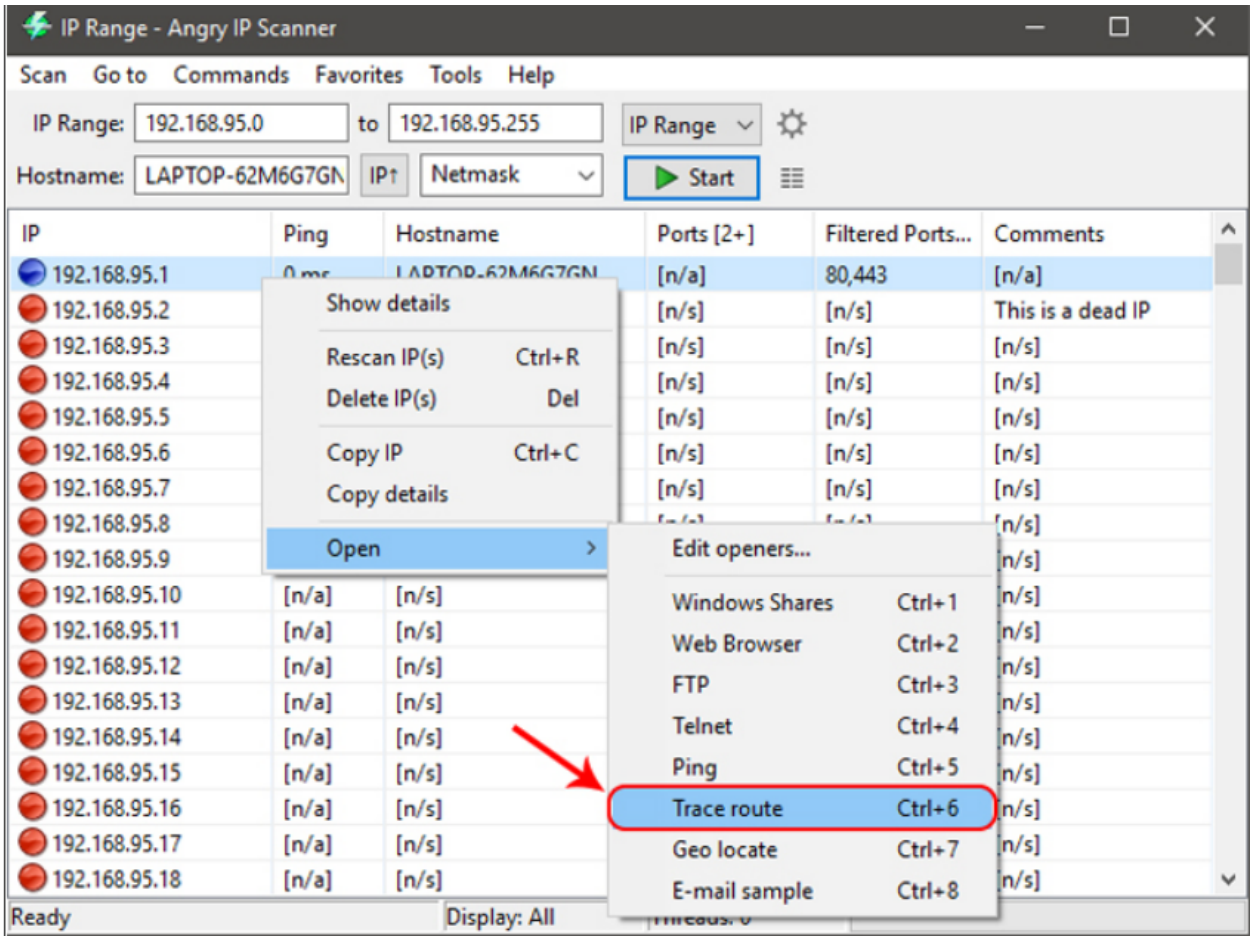
You can also easily copy all the details of an IP address. To do that, right-click on the IP address and select the option “Copy details.” This action will copy the information from all the fetchers. Alternatively, you can also select the IP and press Ctrl + C.

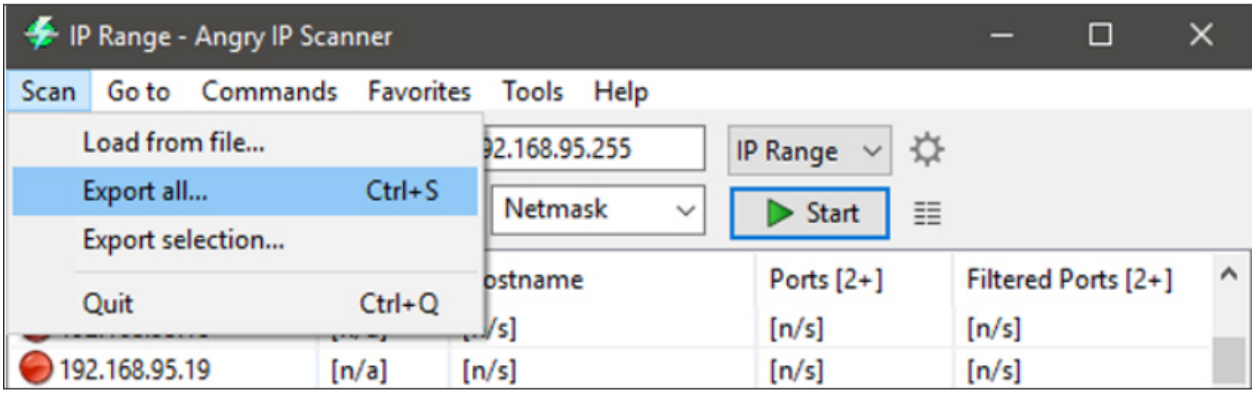


Apart from copying the details of an IP address, you can also perform a range of different activities on the entries. You can open an IP address in the web browser, do an FTP, trace routing, etc. For instance, if you want to traceroute an IP address, simply right-click on the target IP address. After that, select the option **Open** and click on **Traceroute**.

Once you are done scanning an IP address or the IP address range, you can save the scan results. To do that, select the option Scan from the menu bar. From the drop down click on “Export All”.

Angry IP Scanner is a simple yet very useful utility when you want to quickly scan a wide range of IP addresses and ports. It doesn’t have any complicated settings and is very beginner friendly. Once you get comfortable with the application, you can start other network tasks like assigning static IPs to your devices or block people out of your Wi-Fi.

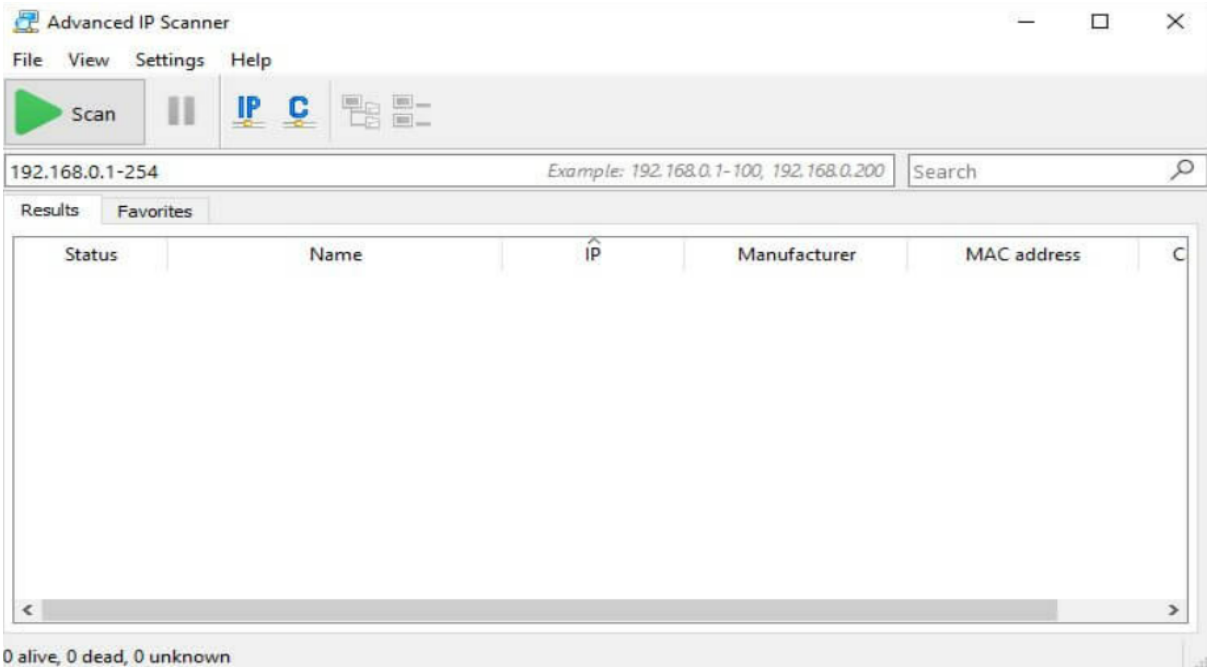


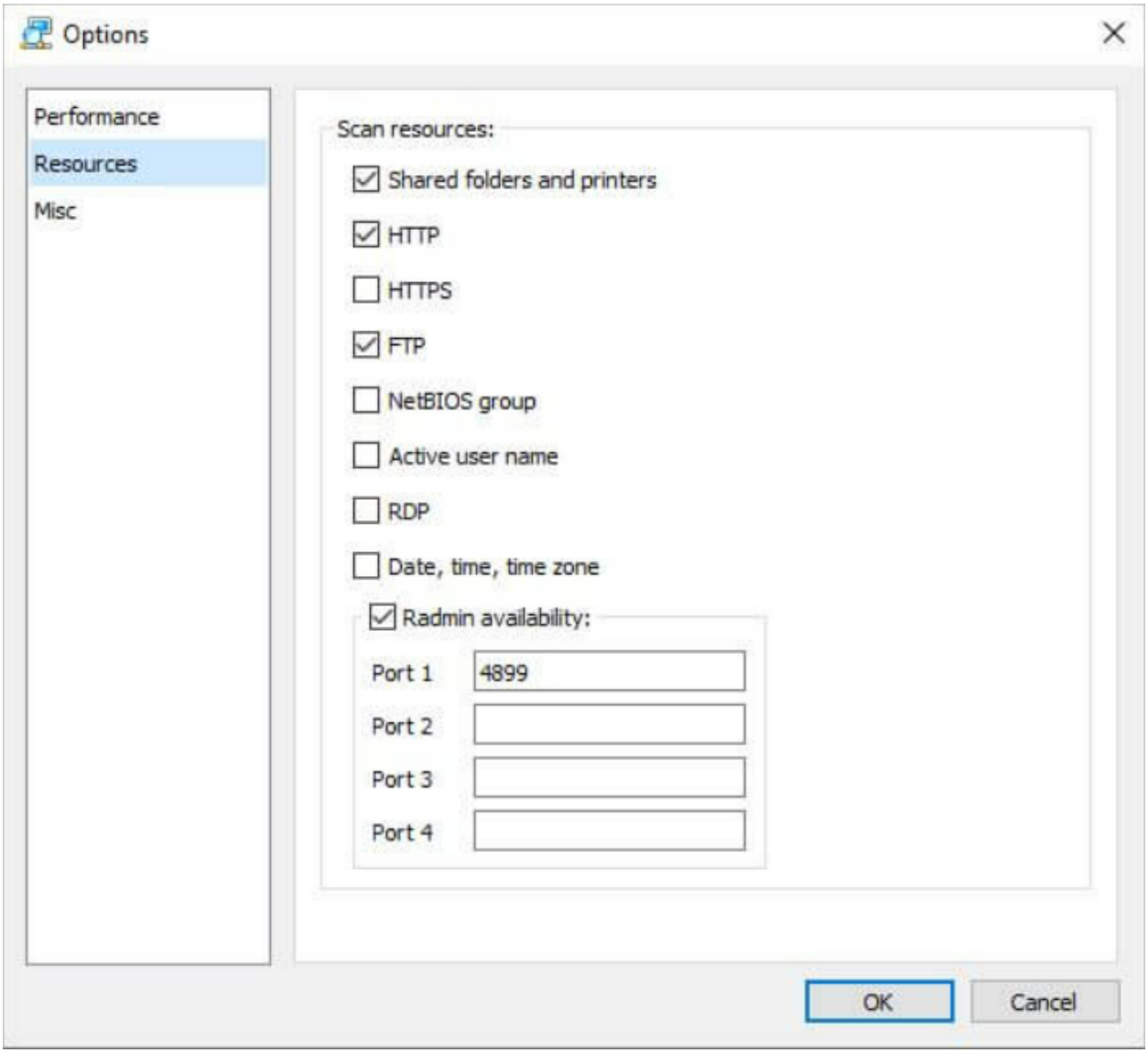


Aim: Advanced IP scanner

Procedure: **Advanced IP Scanner** is a comprehensive network scanning solution that can do more than what its name hints at. You may be thinking that a tool called “Advanced IP Scanner” can’t do much besides scanning for IPs in an advanced mode.

In fact, this tool can handle a lot of other network-related tasks. For instance, you can see all the devices available on your network, and even access remote-shared folders. However, we'll get into more detail in the following sections.

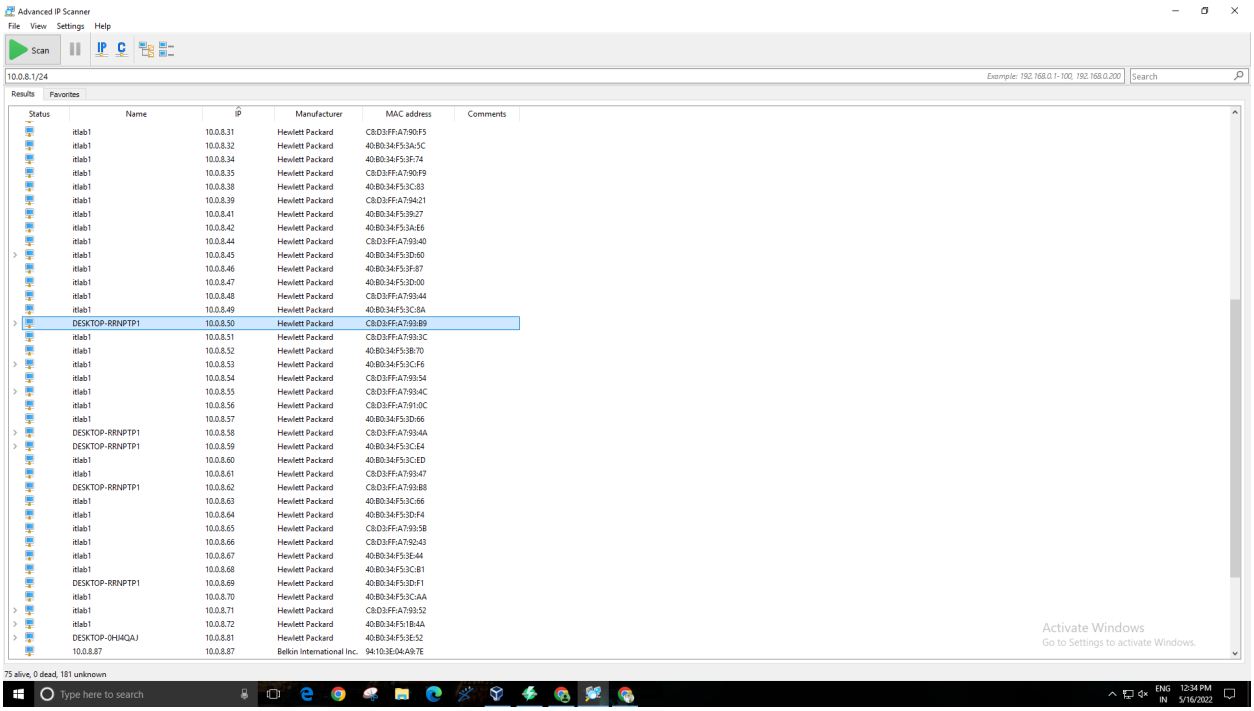




You can use this tool on your computer without installing it necessarily. When you launch its installer, you would be asked to choose one among two options:

- Run the program
- Go through a standard setup process.

As a result of the tool's portable version, it would not create extra folders or files on your system. You get some temporary ones that you need to run the application. In addition to this, the tool will never tamper with the registry entries present on your computer.



you are allowed to set the scanning in a relatively slow manner. As a result of which CPU usage will be low, but the time taken would be longer. On the contrary, you can also enable the app to run fast scanning, which will consume more CPU.

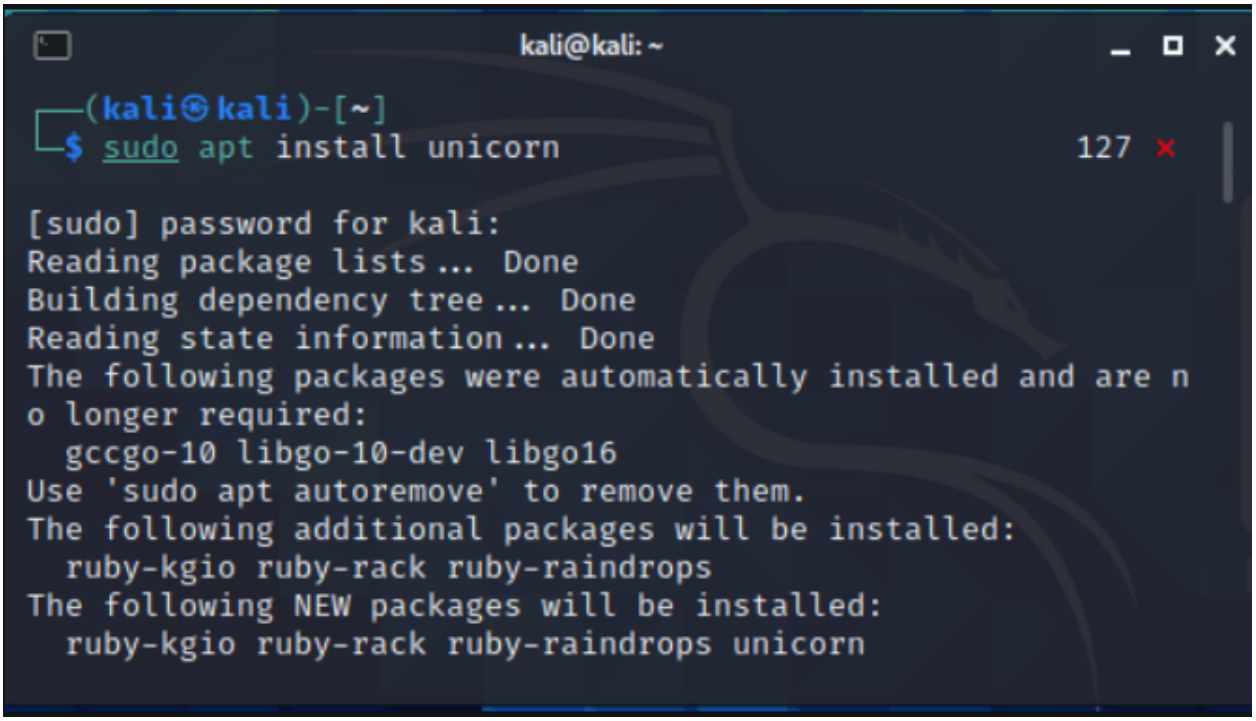
Apart from that, you can set high-accuracy scanning to get more output, but in a longer time. You can toggle scan your resources, including RDP, FTP, HTTP, etc., from the category – “Resources”.

WEEK-3

Aim: Unicorn scan - penetration testing tool

Procedure:

Unicornscan is a free and open-source Automated Penetration Testing tool available on GitHub which is very useful for security researchers for information gathering and testing of the security of websites and web servers.Unicornscan provides many integrated tools to perform penetration testing on the target system.

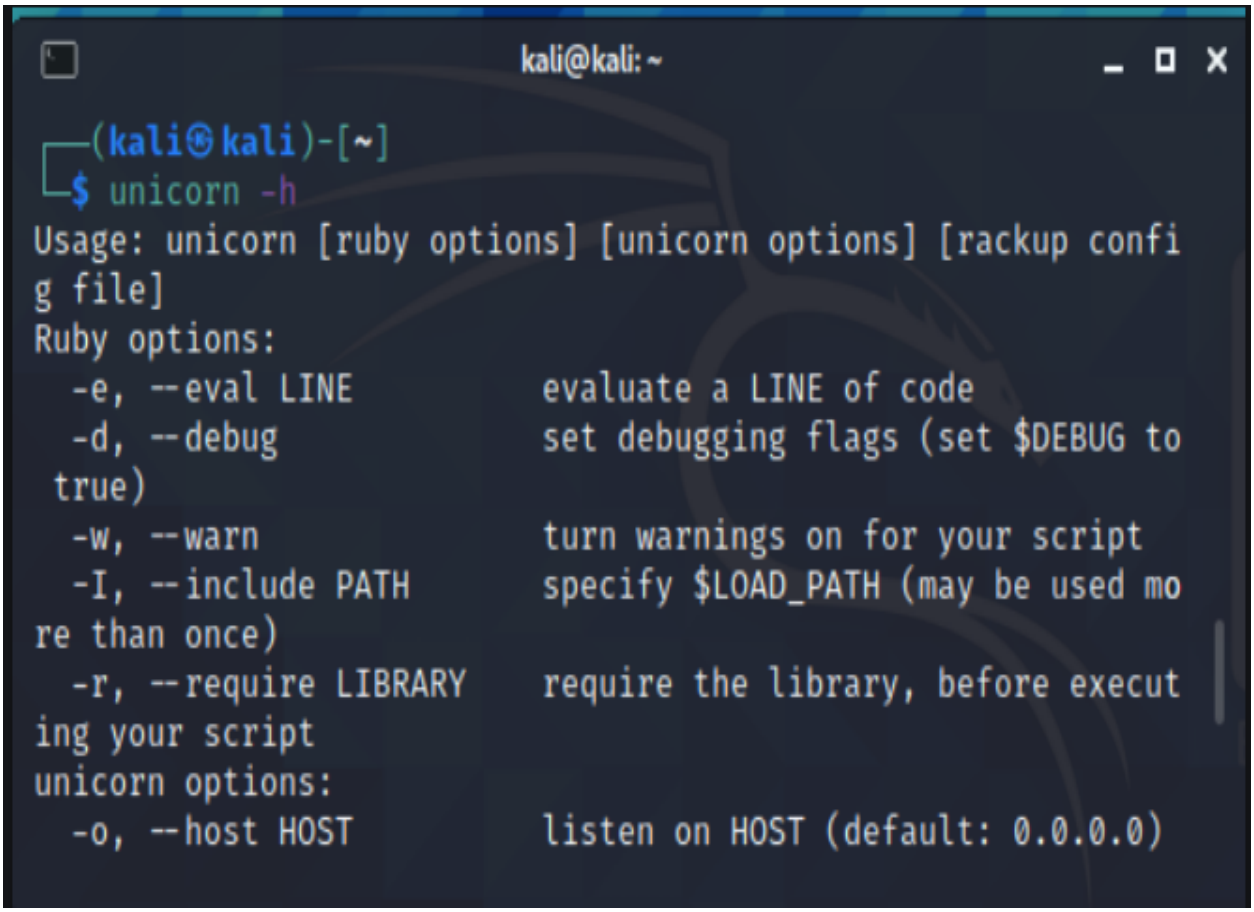


Features and Uses of Unicornscan tool :

- Unicornscan can detect asynchronous TCP banner.
- Unicornscan can tell you information about OS, application and system service detection on the host.
- Unicornscan tool has ability to use custom data sets to perform reconnaissance.
- Unicornscan tool supports SQL relational output from networks.
- Unicornscan can perform TCP asynchronous scan on hosts
- Unicornscan can perform asynchronous UDP scan on hosts.

The tool has been downloaded into your kali linux machine. Now to open the flags and help menu of the tool use the following command.

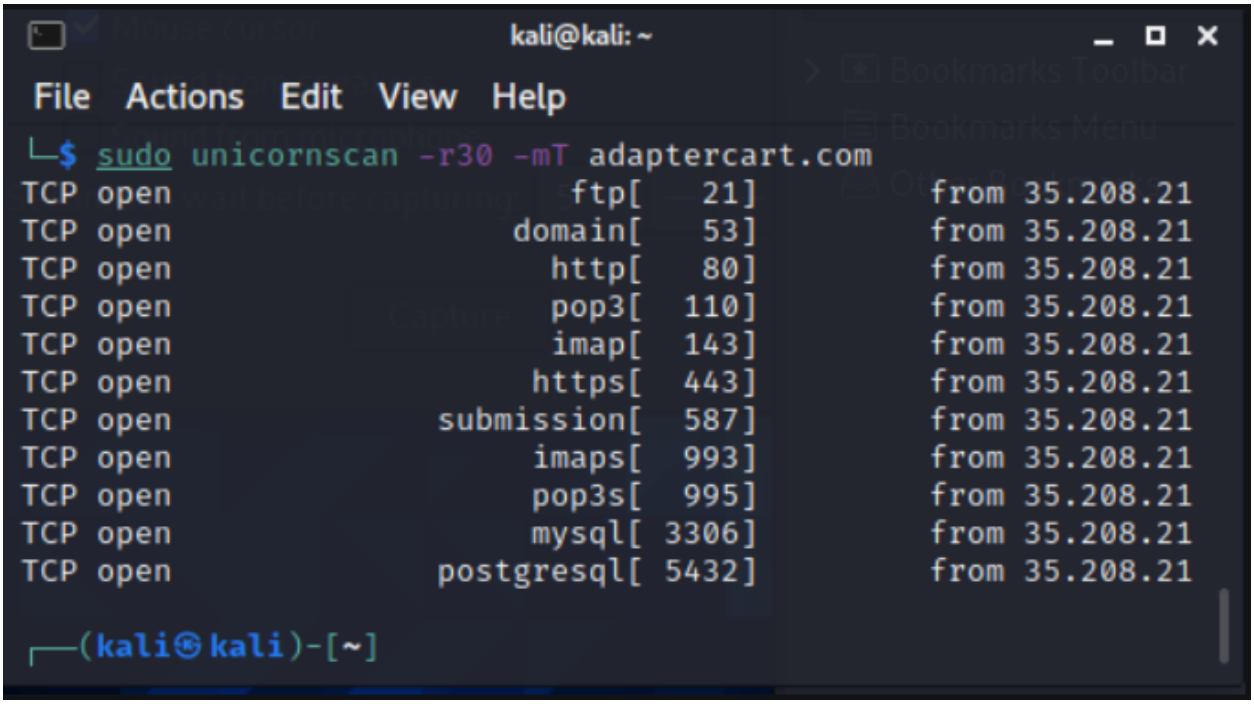
cmd : unicorn -h



Use the unicorn tool to scan a ip address to get details of open and closed ports of a website called adaptercart.

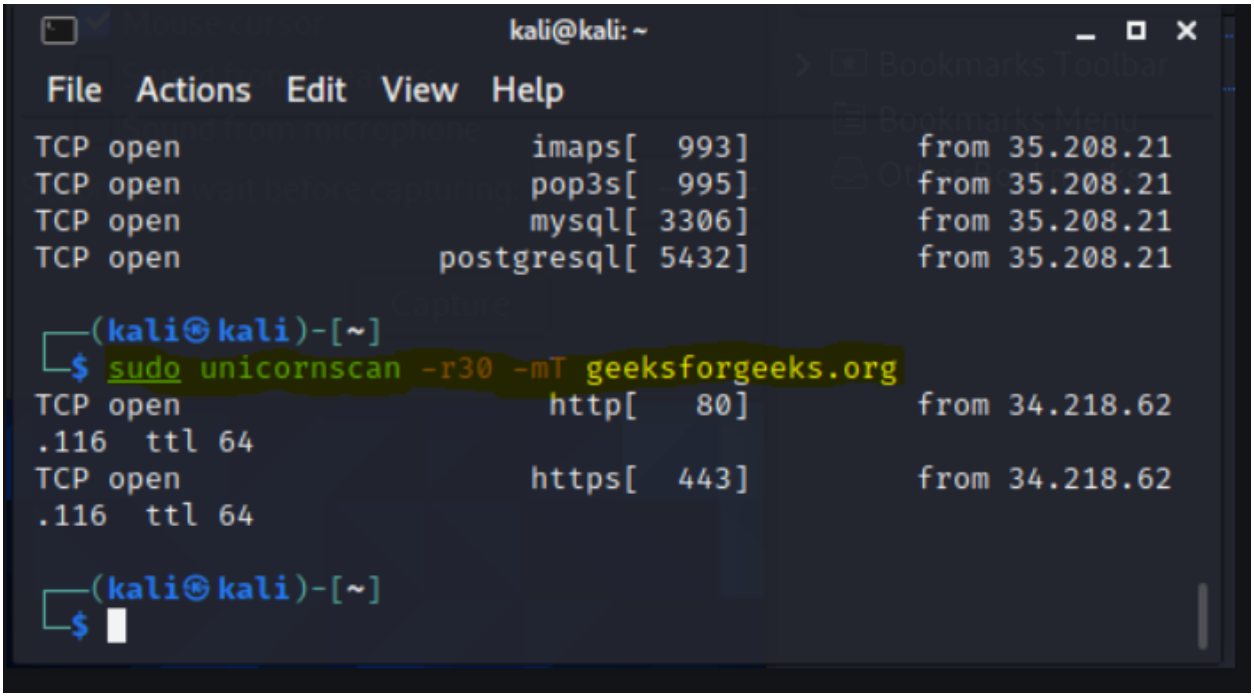
sudo unicornscan -r30 -mT adaptercart.com

cmd : unicorn -r30 -mT adaptercart.com



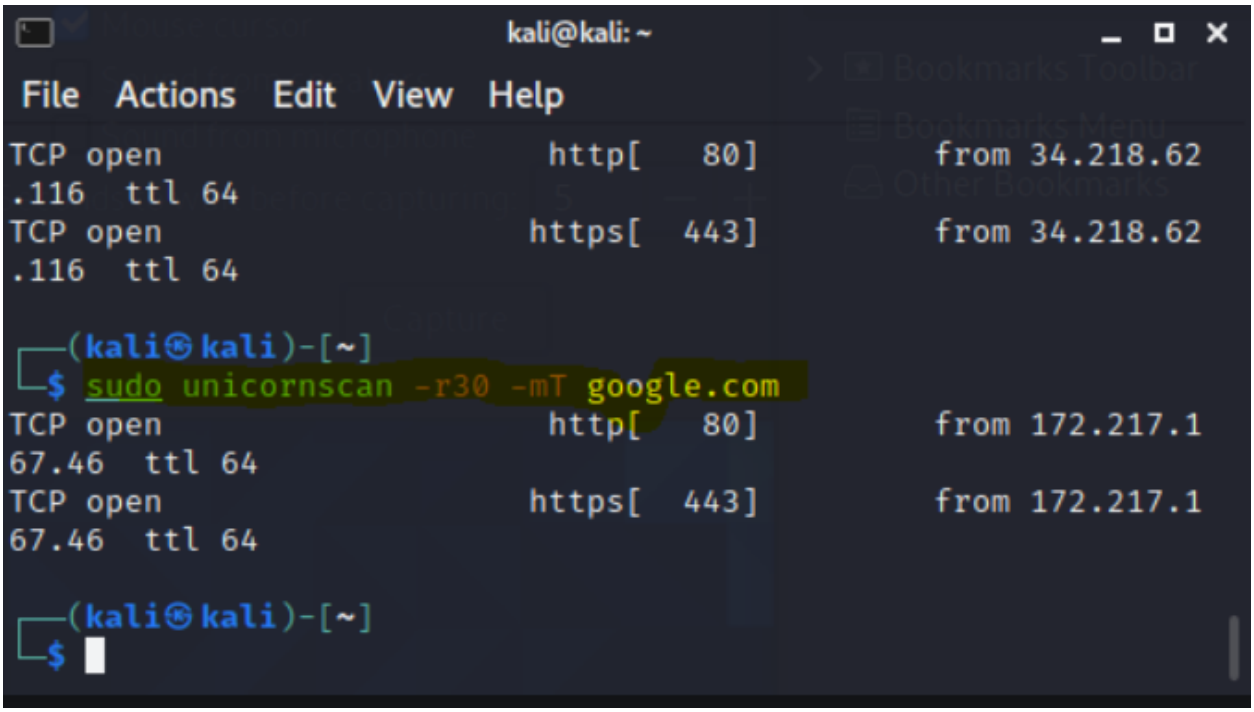
Use the unicorn tool to scan an ip address to get details of open and closed ports of a website called geeksforgeeks.

cmd: sudo unicornscan -r30 -mT geeksforgeeks.org



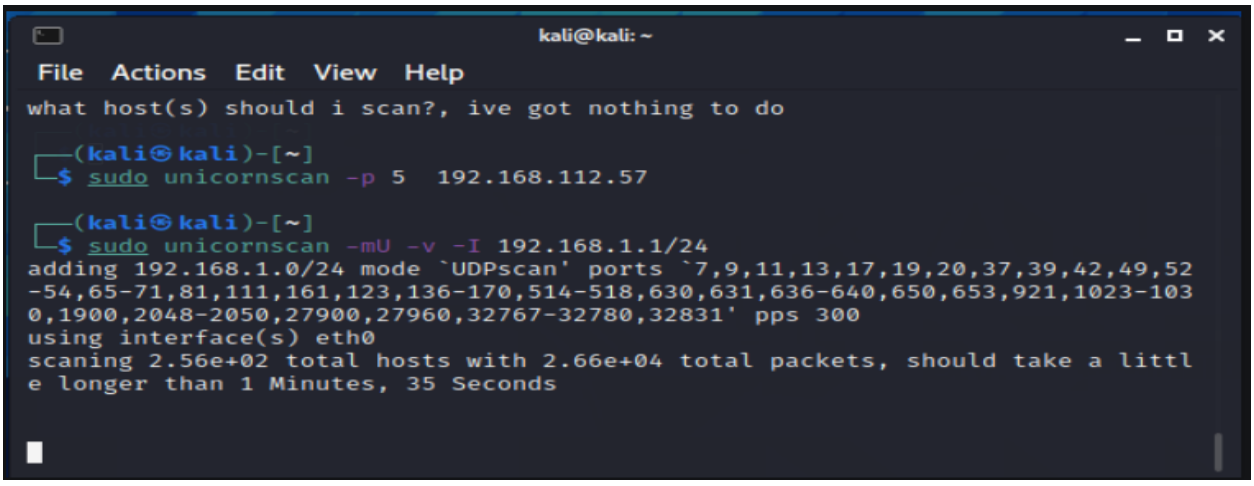
Use the unicorn tool to scan a ip address to get details of open and closed ports of a website called google.com

cmd: sudo unicornscan -r30 -mT google.com



Use the Unicornscan tool to perform a UDP scan on the whole network

cmd: sudo unicornscan –mU –v –I 192.168.1.1/24



Use the Unicornscan tool to perform a TCP SYN Scan on a whole network.

cmd: unicornscan -msf -v 192.168.1.1/24