**ETHICAL HACKING**

### 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 operatingsystems they are running.

**Command** : sudo su apt-get install nmap

### Description :

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

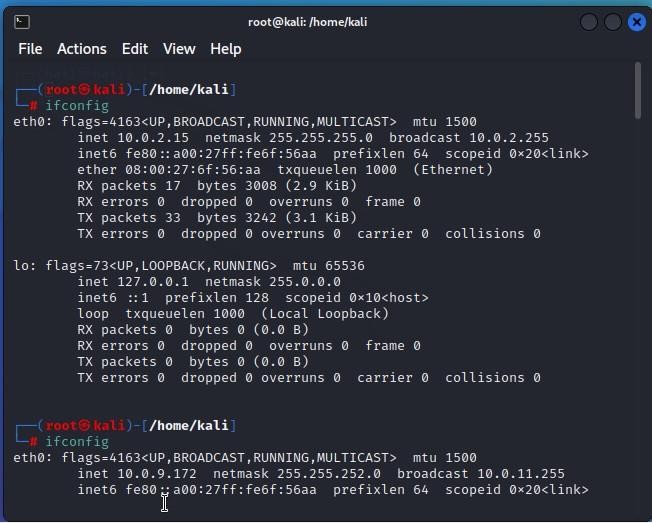
lead to undesirable results like system downtime and data loss. Always scan mission critical systems with caution.

### 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>

**Command** : if config



**Description :**

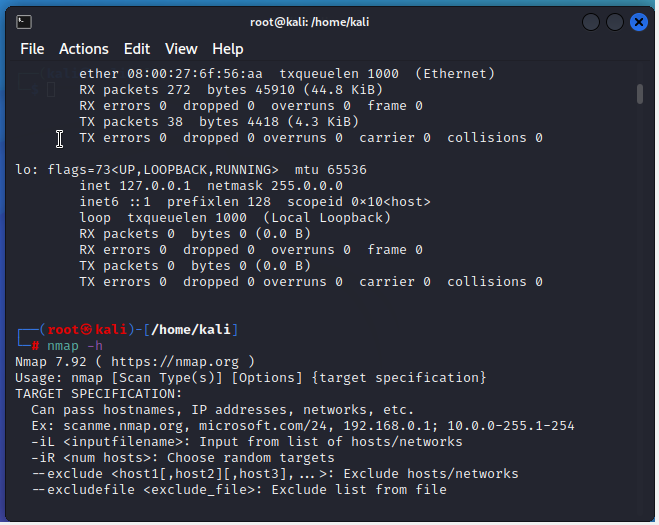
You can use the **ifconfig** command to assign an address to a network interface and to

configure or display the current network interface configuration information. The

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

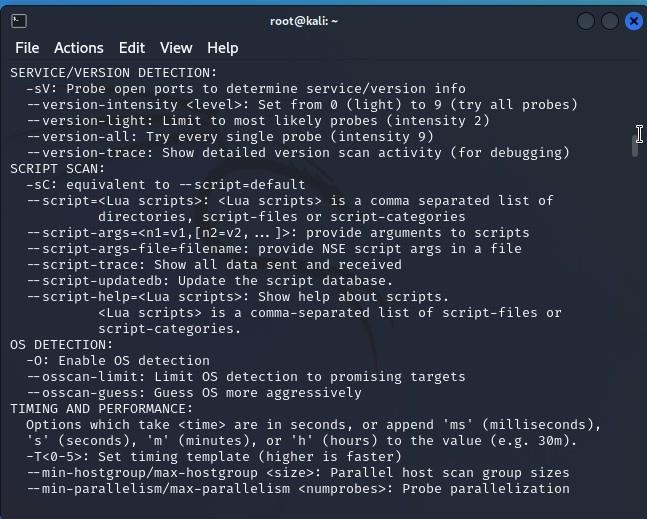
each interface present on a system. After system startup, it can also be used to redefine an interfaces address and its other operating parameters.

**Command** : 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*](https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command&ifconfig__row-d3e4363)[ [*addressfamily*](https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command&ifconfig__row-d3e4342)[ [*address*](https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command&ifconfig__row-d3e4330)[ [*destinationaddress*](https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command&ifconfig__row-d3e4357)] ] [

[*parameters*](https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command&ifconfig__row-d3e4426)... ] ]

**ifconfig** *interface* [ [*protocolfamily*](https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command&ifconfig__row-d3e4293) ] *interface protocolfamily*

**ifconfig** [**-a**](https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command&ifconfig__row-d3e4239) [ [**-l**](https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command&ifconfig__row-d3e4266) ] [ [**-d**](https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command&ifconfig__row-d3e4251) ] [ [**-u**](https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command&ifconfig__row-d3e4278) ] [ *protocolfamily* ]

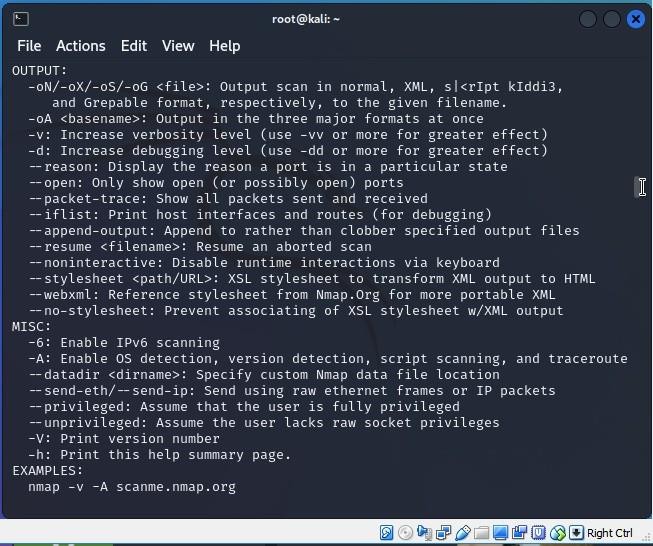
**ifconfig** *interface* [ **tcp\_low\_rto** [*rto*](https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command&ifconfig__row-d3e5268) | **-tcp\_low\_rto** ]

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

## Ping Scanning :

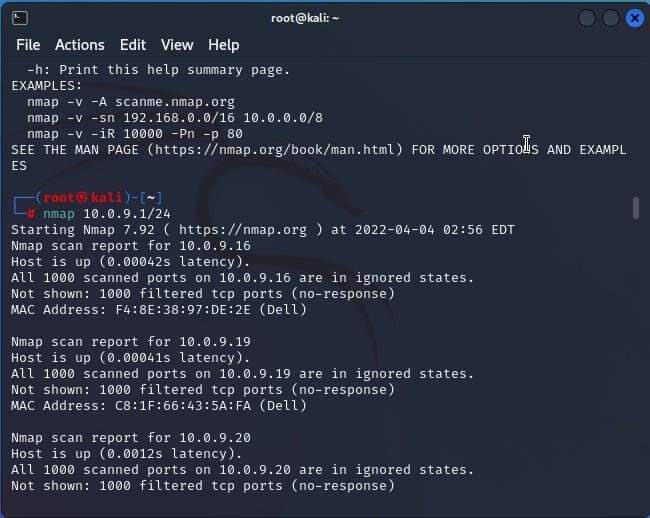
Ping scan returns information on every active IP on your network. You can execute a

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.

**Command** : nmap 10.0.9.1/24

nmap --top-ports 20 192.168.1.106

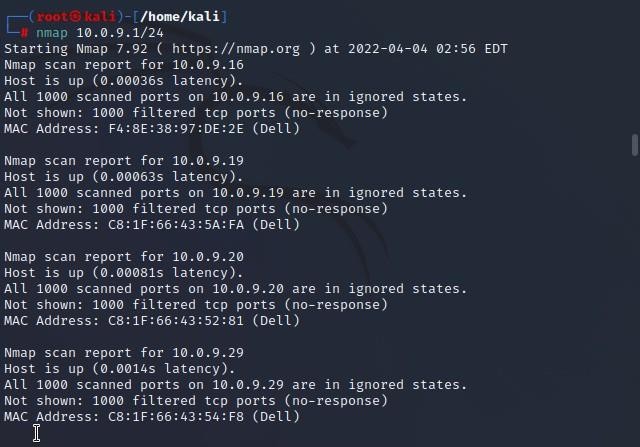
Replace the “20” with the number of ports to scan, and Nmap quickly scans that many ports. It returns a concise output that details the status of the most common ports, and this lets you quickly see whether you have any unnecessarily open ports.

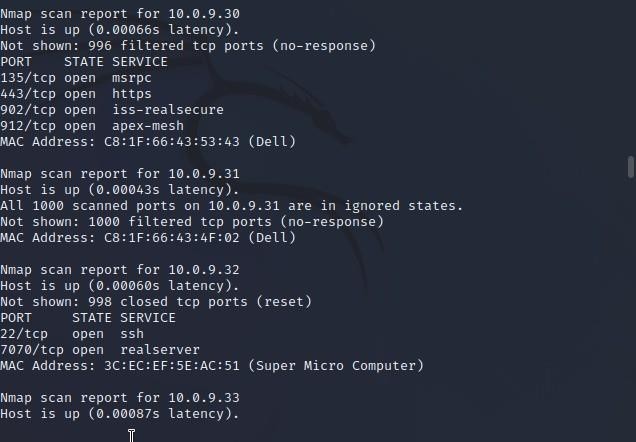
OS scanning is one of the most powerful features of Nmap. When using this type of scan, Nmap sends TCP and UDP packets to a particular port, and then analyze its response. It compares this response to a database of 2600 operating

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>

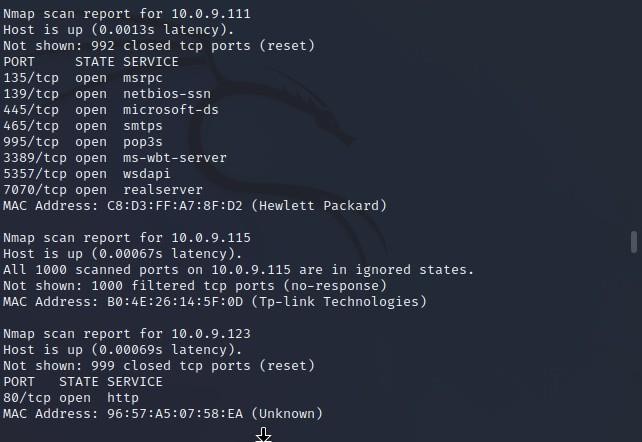
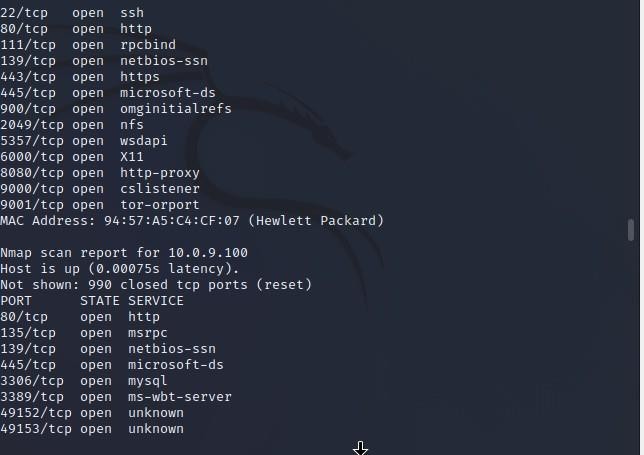
**Command :** nmap



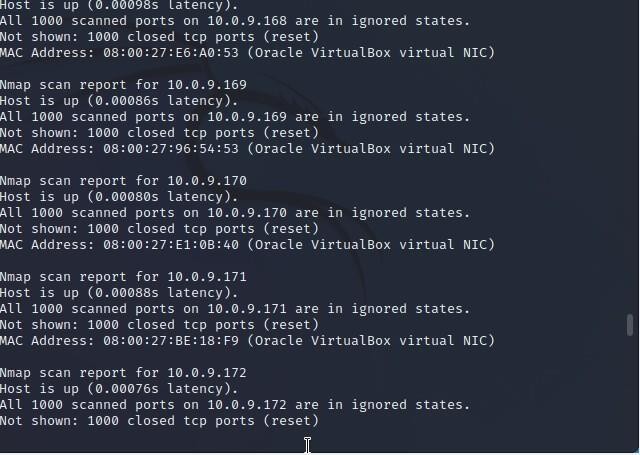
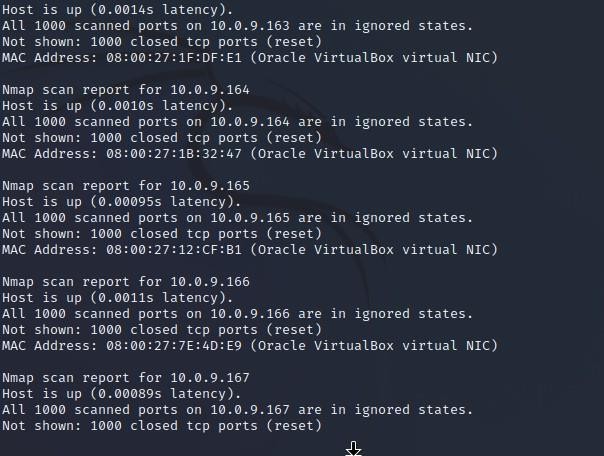
10.0.9.1/24

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

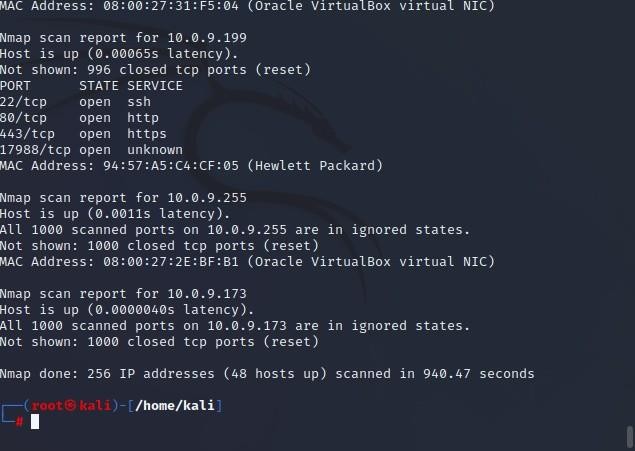
**Command** : nmap 10.0.9.1/24



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



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

**Command** : nmap 10.0.9.1/2

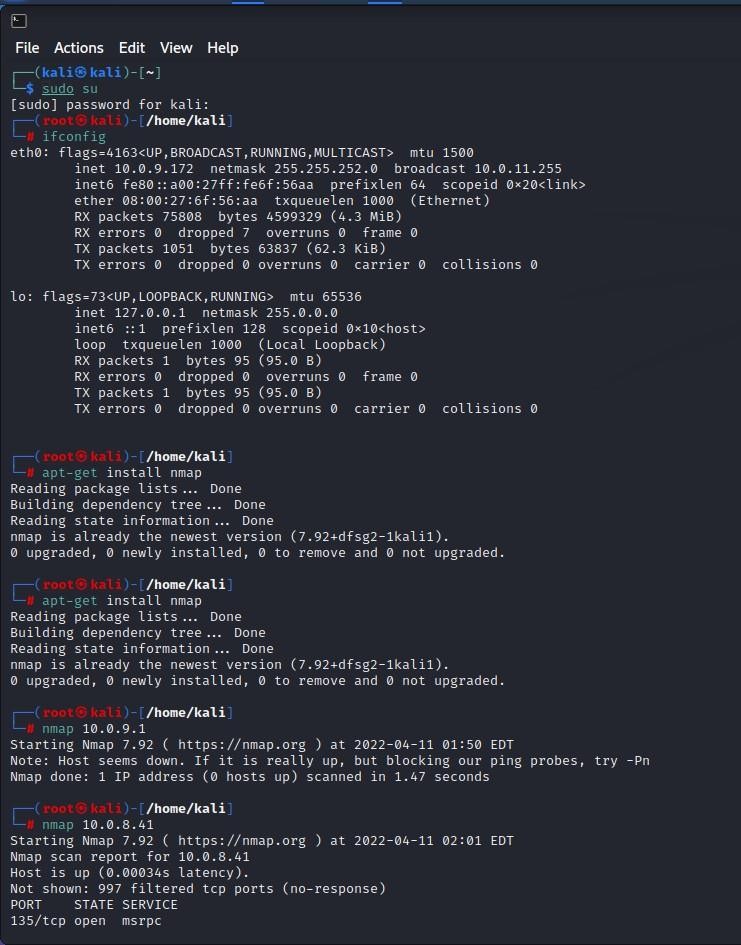
**AIM :-**

About nmap tools commands cmd: sudo su

ifconfig

apt-get install nmap nmap 10.0.9.1

nmap 10..8.4



**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).

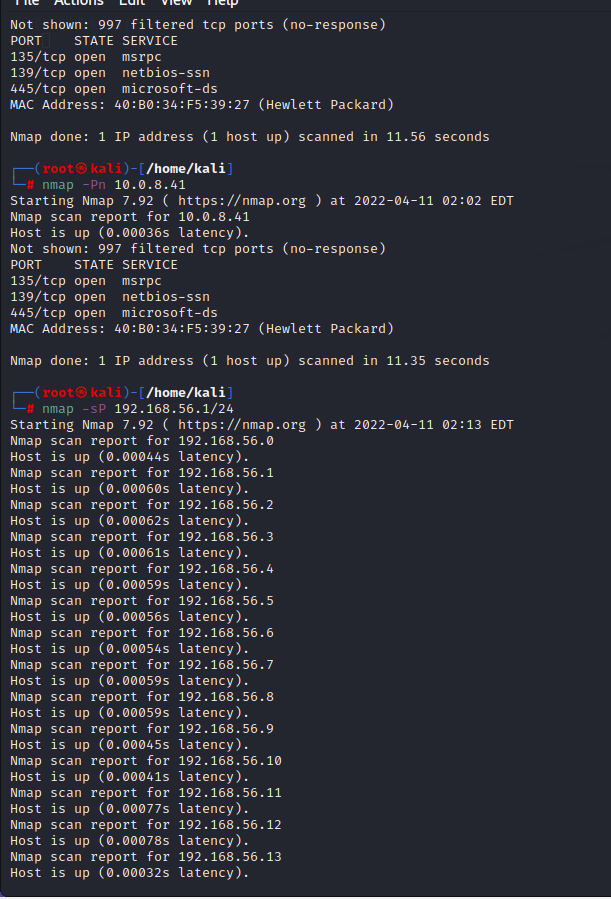
Nmap supports several ping scanning techniques using different protocols. For example, the default ping scan command with no arguments (nmap -sn

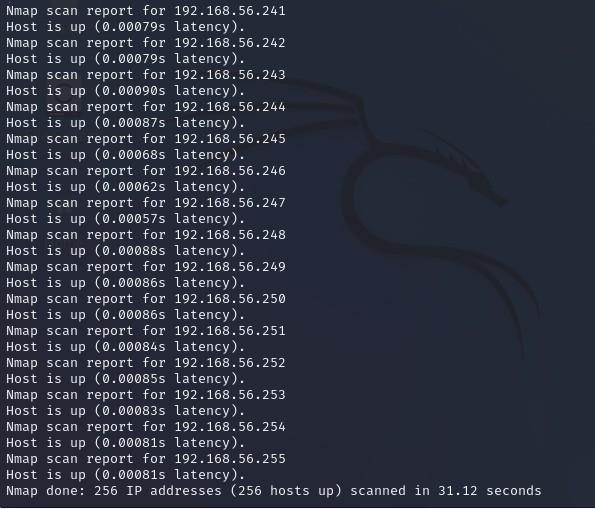
<target>) as a privileged user internally executes the -PS443 -PA80 -PE -PP options corresponding to TCP SYN to port 443, TCP ACK to port 80, and ICMP echo and timestamps requests.

-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)

**Command** : nmap -Pn 10.0.8.41 nmap -sP 192.168.56.1/24





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.

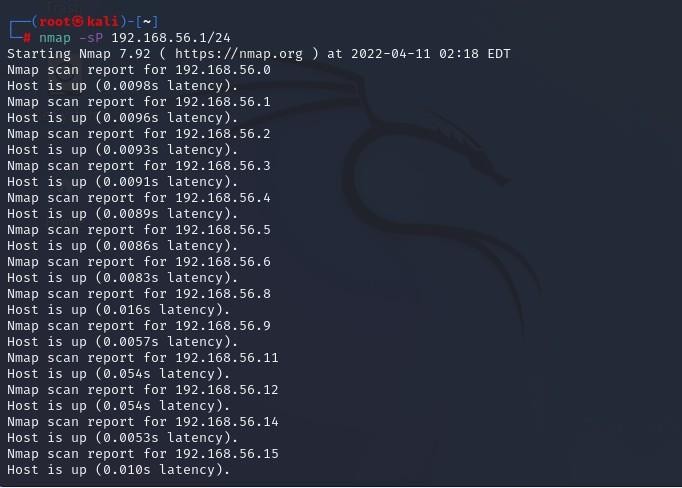
A more powerful way to scan your networks is to use Nmap to perform a host scan.

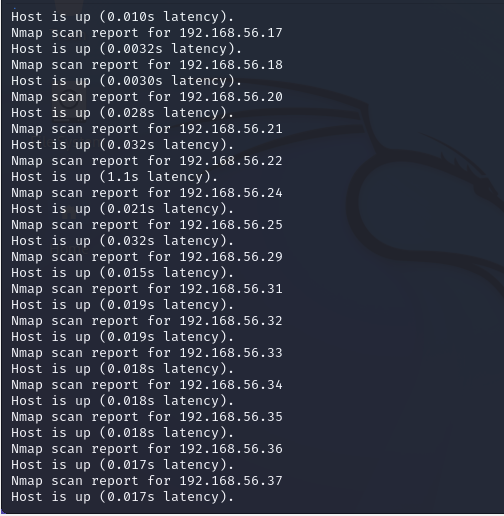
Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts

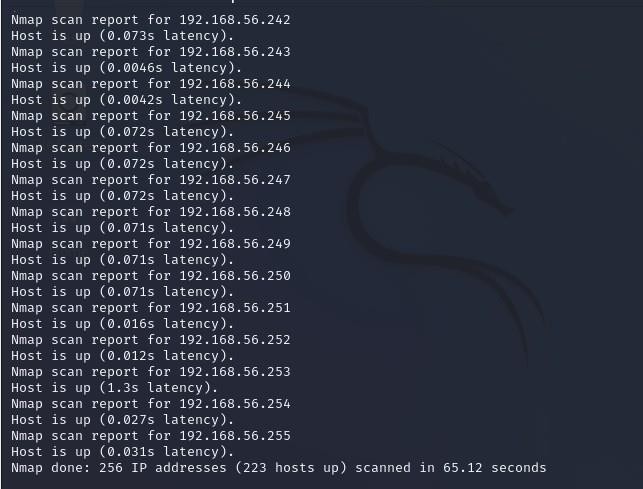
connected to your network. Each host then responds to this packet with another ARP

packet containing its status and MAC address. To run a host scan, use the following command: # nmap -sp <target IP range>

**Command** : nmap -sP 192.168.56.1/24







## 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.

**Command** : nmap -PS scanme.insecure.org

nmap -PU 192.168.171.1

**UDP Ping**

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

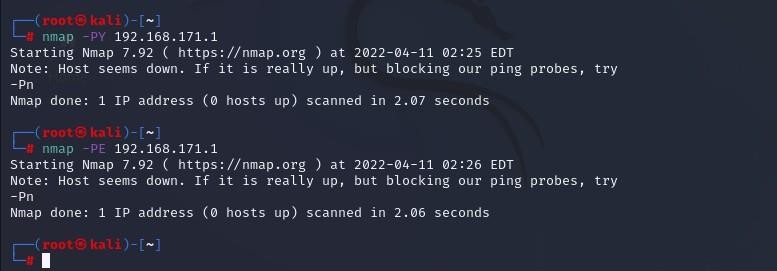
This discovery method sends UPD packets in an attempt to solicit a response from a target. While most firewalled systems will block this type of connection, some poorly configured systems may allow it if they are only configured to filter TCP connections.

## 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.

**Command** : 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) echoping, on the specified system.

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.

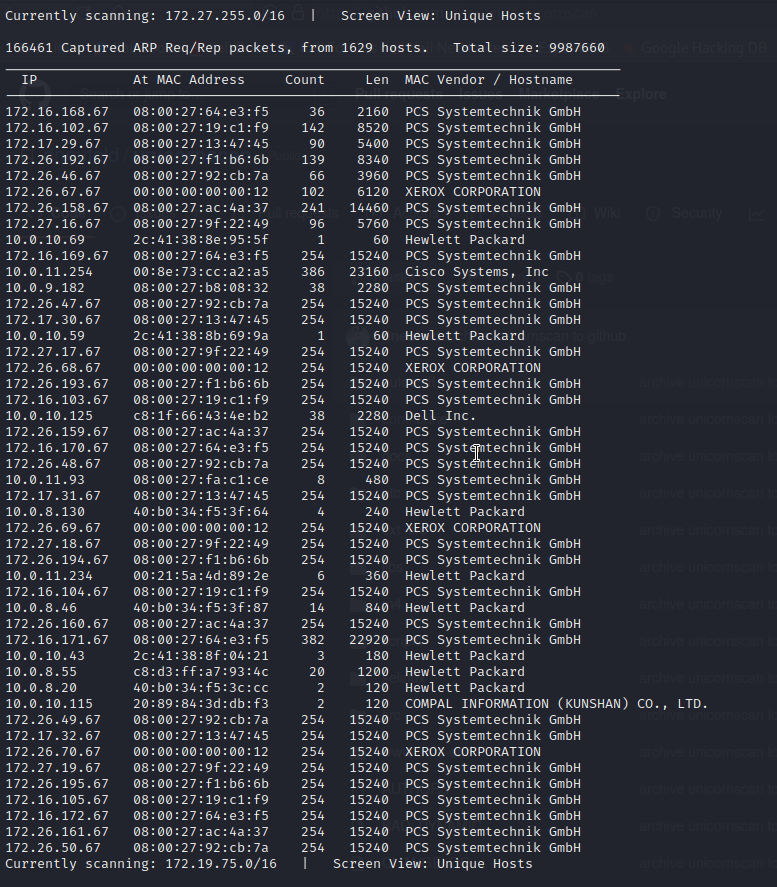
Nmap does not care whether the port is open or closed. Either the ABORT or INIT-ACK response discussed previously tell Nmap that the host is available and responsive.

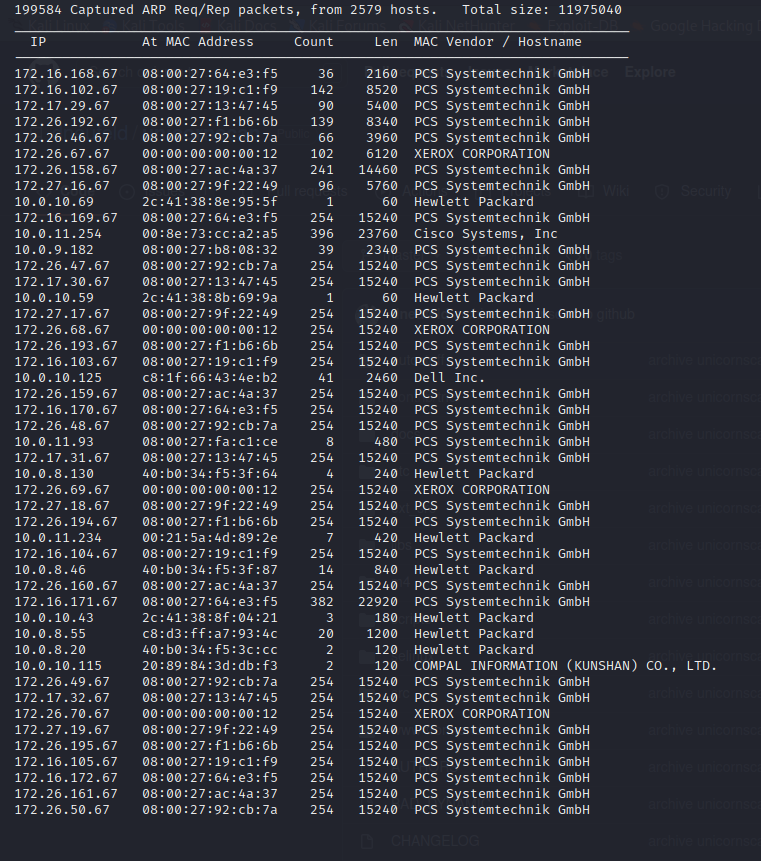
On Unix boxes, only the privileged user root is generally able to send and receive raw SCTP packets. Using SCTP INIT Pings is currently not possible for unprivileged users.

### WEEK-2

**Aim:** Angry ip scanner

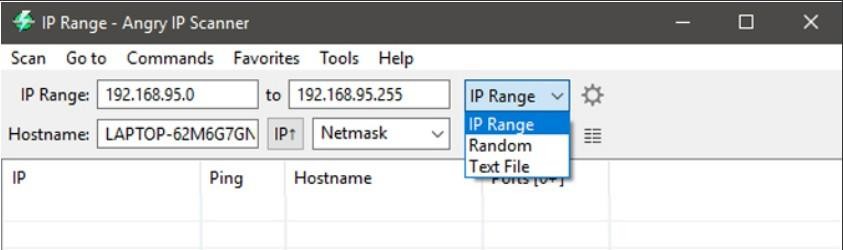
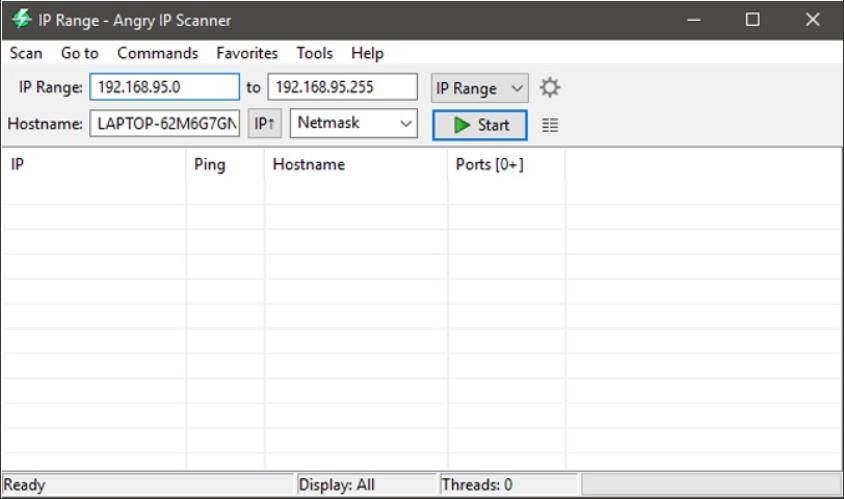
**Procedure:** Angry IP Scanner is a free, lightweight, cross-platform, and open source tool to [scan networks](https://techwiser.com/?s=wifi). It helps you to scan a range of IP addresses to find live hosts, open ports, and other relevant information of each and every IP address.



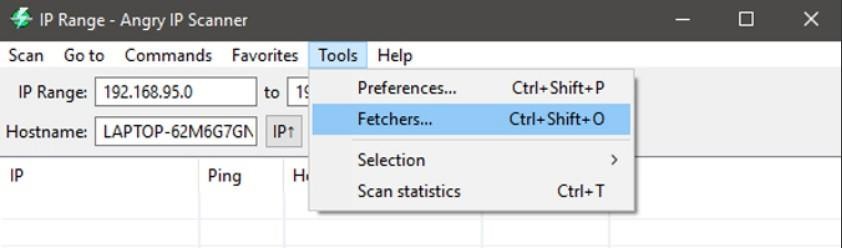


Once installed, open the application by searching for it in the Start Menu. As you can see, the home screen of the application is pretty simple and

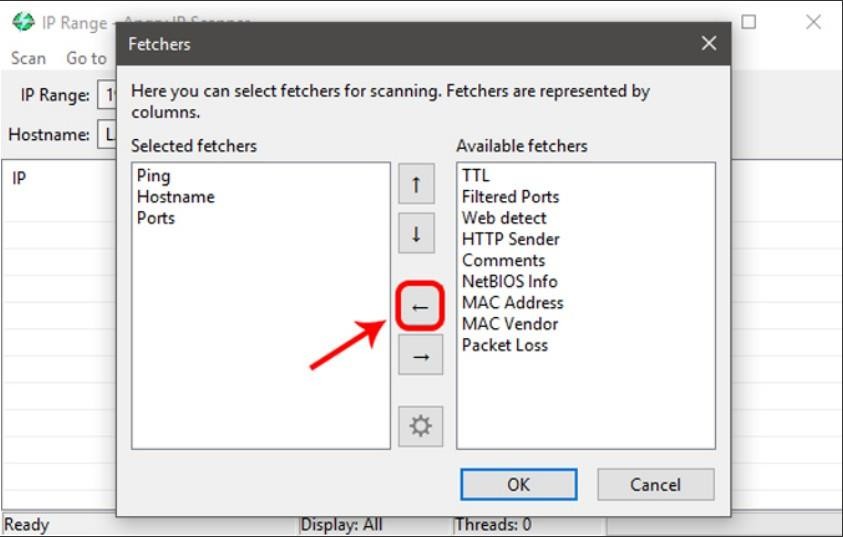
straightforward. By default, Angry IP scanner will enter your local IP address range and your computer name as the hostname.



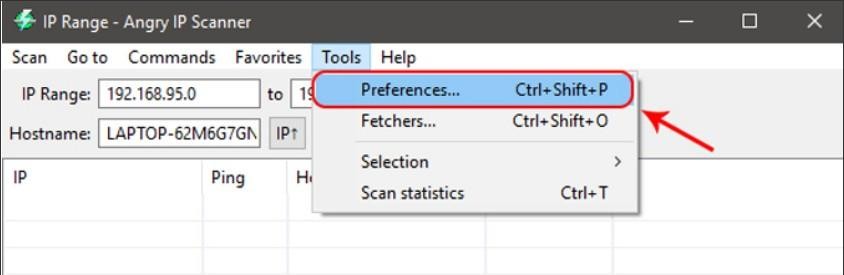
As you can see from the above image, the Angry IP Scanner will only include default fetchers like Ping, Hostname, and Ports. However, you can add more fetchers to get and see more information about an IP address. To do that, select “Tools > Fetchers.”

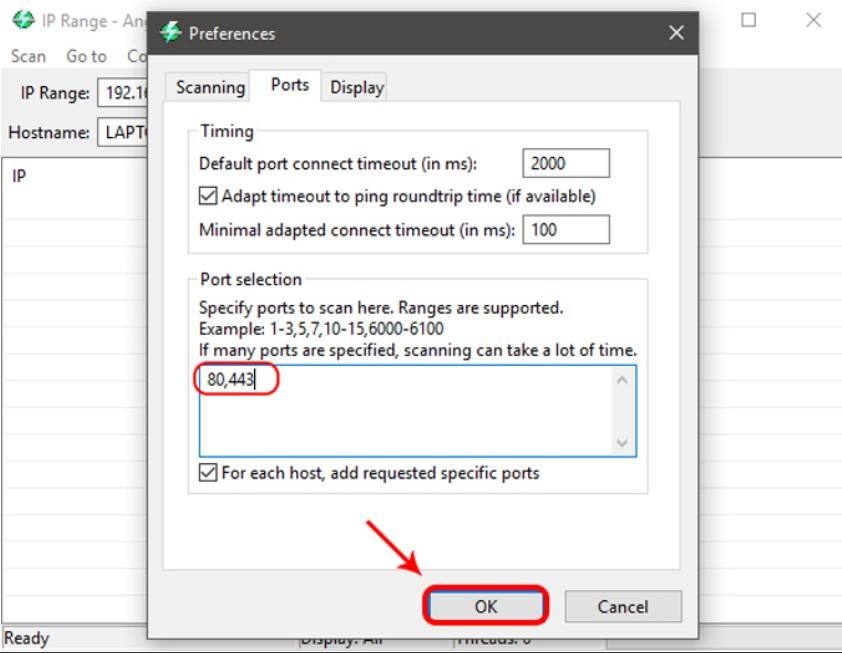


In this window, you will see all the current fetchers on the left pane and all the available fetchers in the right pane. To add a fetcher, select the fetcher on the right pane and then click on the button that looks like “Less than” sign. In my case, I’ve added new fetchers like MAC address, NetBIOS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

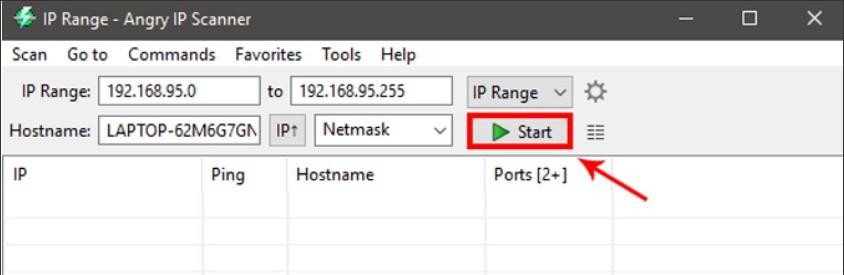


Moreover, Angry IP Scanner will only tell whether the ports are open or not. It will not list the individual ports that are open. So, if you want to do a port scan, then you need to configure the application. To do that, simply navigate to “Tools” and then select the option “Preferences.”

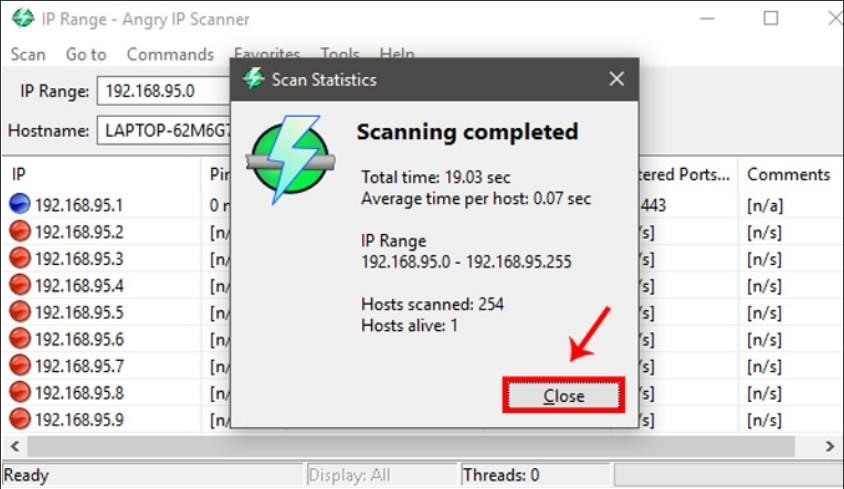




Once you are done configuring the Angry IP Scanner, you can continue to scan. To start off, set the scan mode to “IP Range,” enter the IP address range in the “IP address” fields and then click on the button “Start.” For instance, I’ve entered an IP range that is known to have live devices connected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



Depending on the number of addresses in the range, it may take some timeto 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.

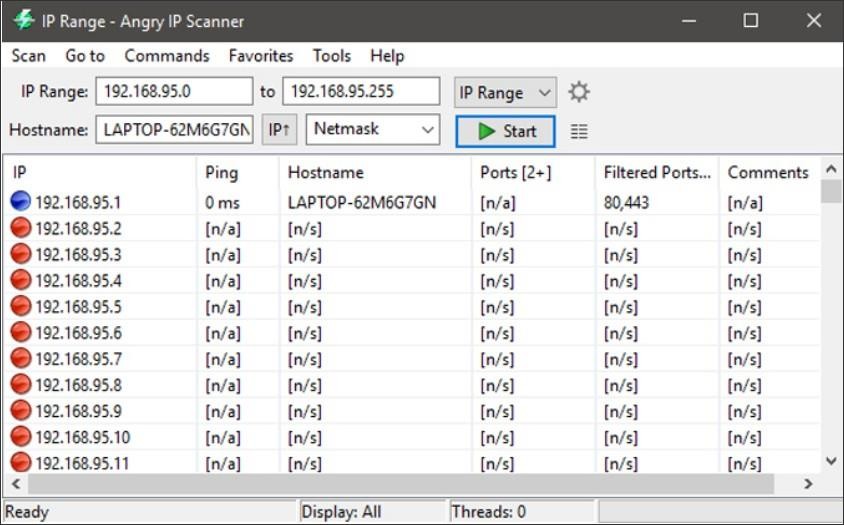


Once you close the summary window, you will see the list of all the IP address. You can also see additional details in different “fetcher” columns. In case you are wondering, here’s what the colored dots next to each IP address mean.

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

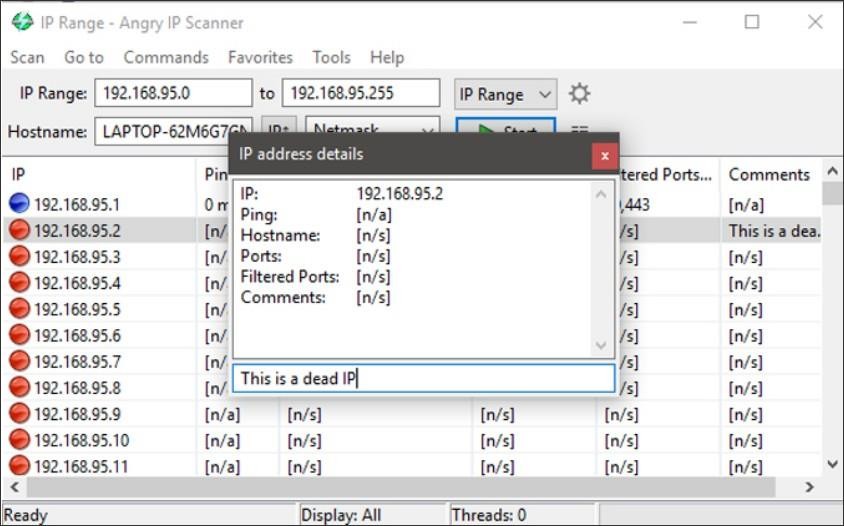
**Blue:** The IP address is either active or busy and not responding to the requests sent by Angry IP Scanner. This usually will be your own IP Address.

**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.

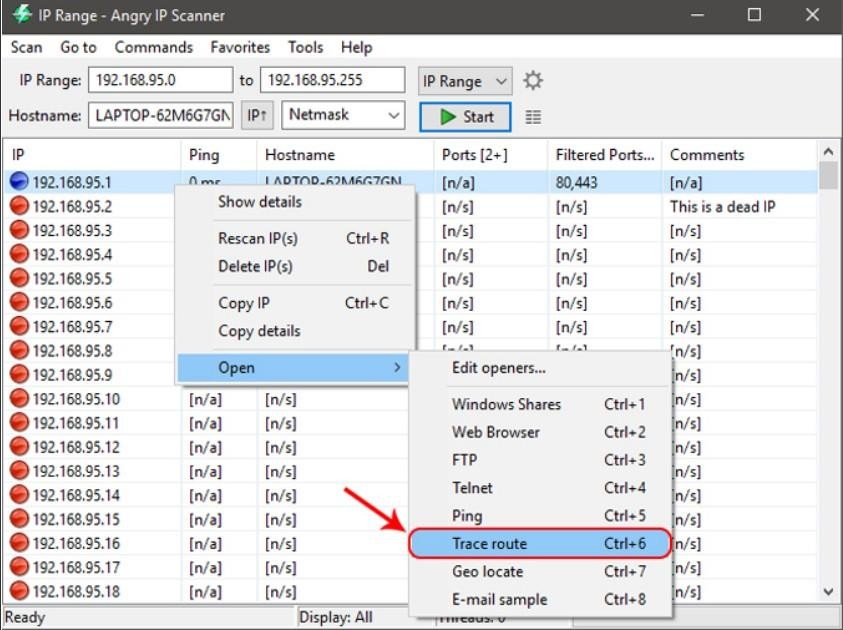
You can also easily copy all the details of an IP address. To do that, right-click on the IP address and select the option “Copy details.” This action will copy the information from all the fetchers. Alternatively, you can also select the IP and press Ctrl + C.

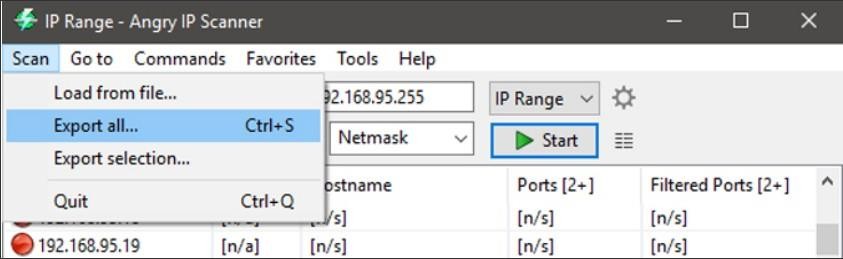


Apart from copying the details of an IP address, you can also perform a range of different activities on the entries. You can open an IP address in the web browser, do an FTP, trace routing, etc. For instance, if you want to traceroute an IP address, simply right-click on the target IP address. After 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 staticIPs](https://techwiser.com/assign-static-ip-address/) to your devices or [block people out of your Wi-Fi](https://techwiser.com/kick-people-off-your-wifi-network/).

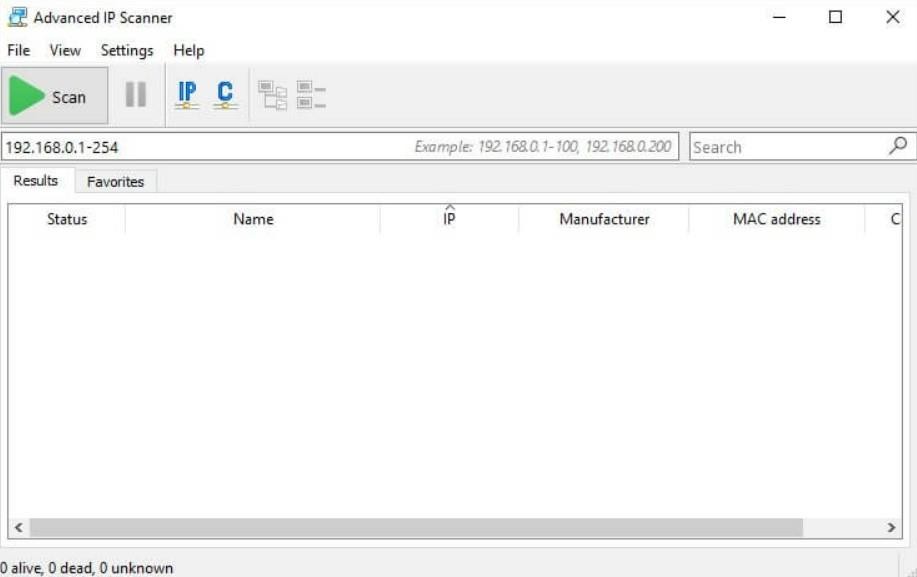




**Aim:** Advanced IP scanner

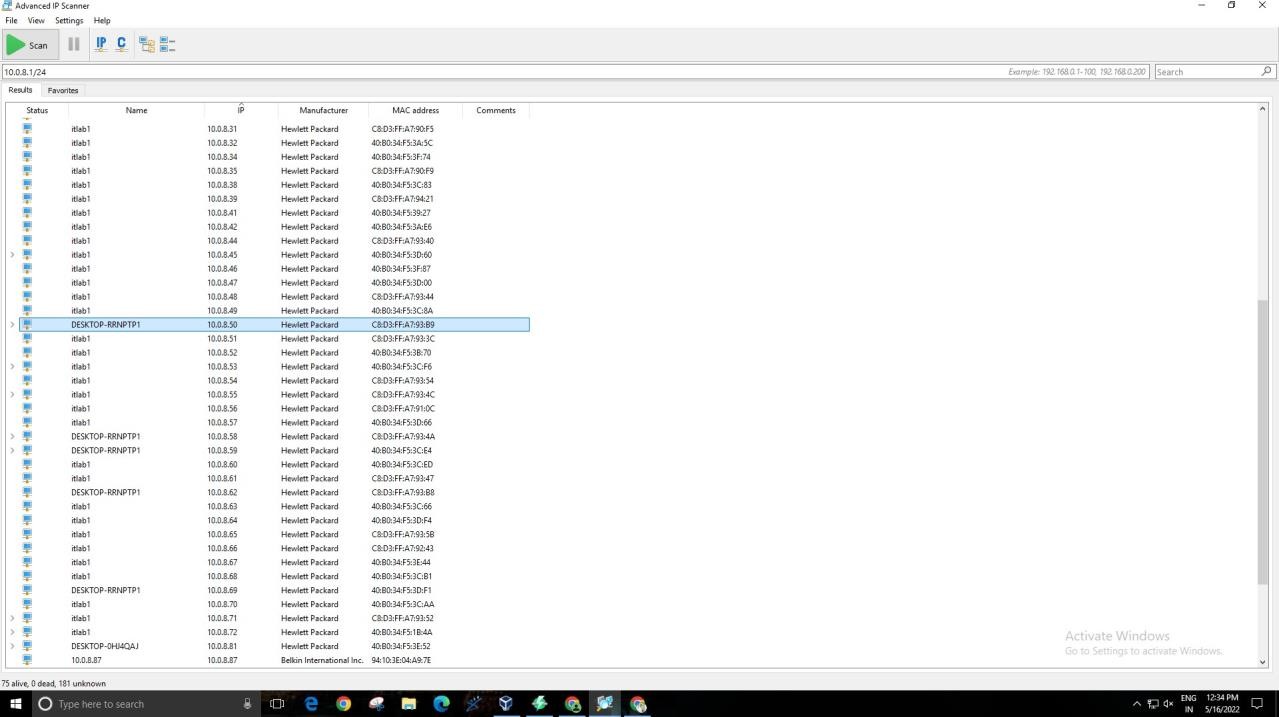
**Procedure: Advanced IP Scanner** is a comprehensive network scanning solution that can do more than what its name hints at. You may be thinking that a tool called “Advanced IP Scanner” can’t do much besides scanning for IPs in an advanced mode.

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

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](https://geekflare.com/rdp-introduction-guide/), FTP, HTTP, etc., from the category