# WEEK-1

**AIM: To Learn about the cyber security tools and techniques.**

**Nmap**

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities. Ability to quickly recognize all the devices including servers, routers, switches, mobile devices, etc on single or multiple networks. Helps identify services running on a system including web servers, DNS servers, and other common applications

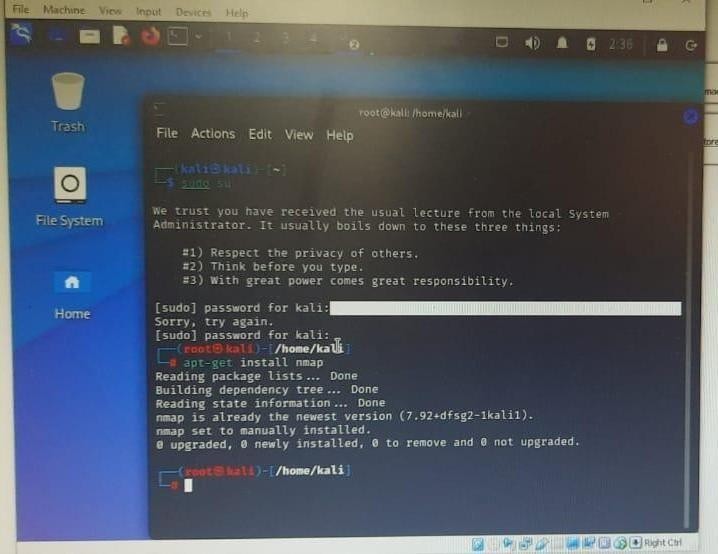
**Command** :

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

Output :

### 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

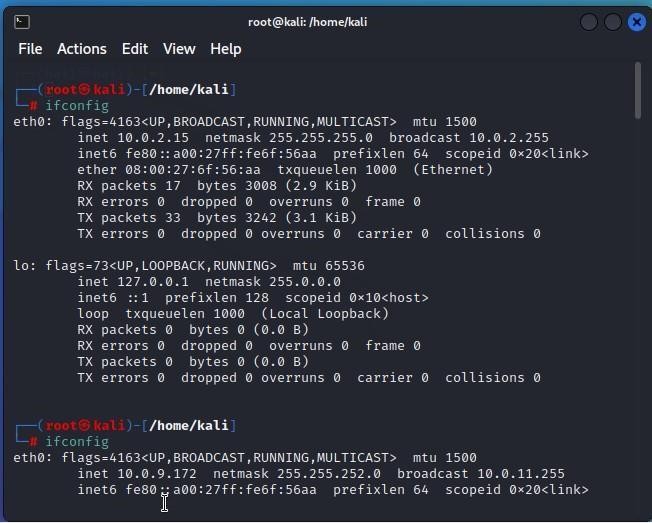
**Command :** if config

**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

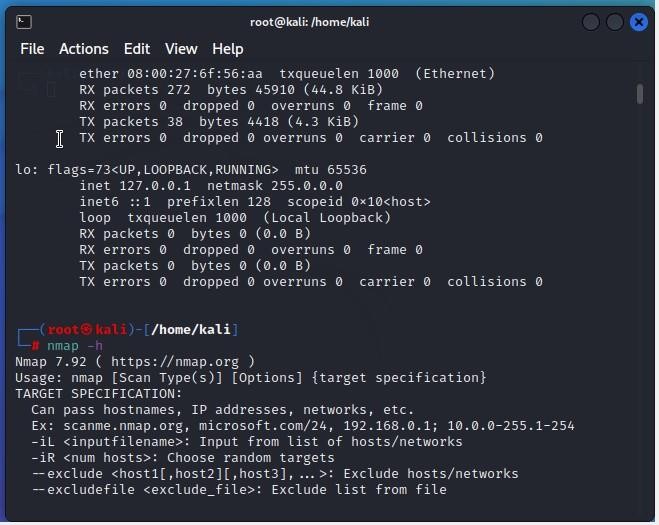
**output :**



**Command** : nmap –h

**DESCRPTION** :

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

**OUTPUT** :

### Commands :

**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** ]

## Ping Scanning :

Ping scan returns information on every active IP on your network. You can execute a ping scan using this command

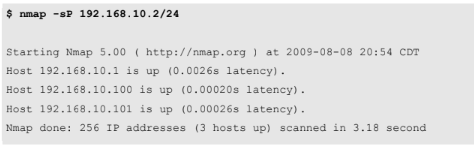
**Commands:**

nmap -sp 192.100.1.1/24

DESCRIPTION :

Ping scan returns information on every active IP on your network

**OUTPUT :**



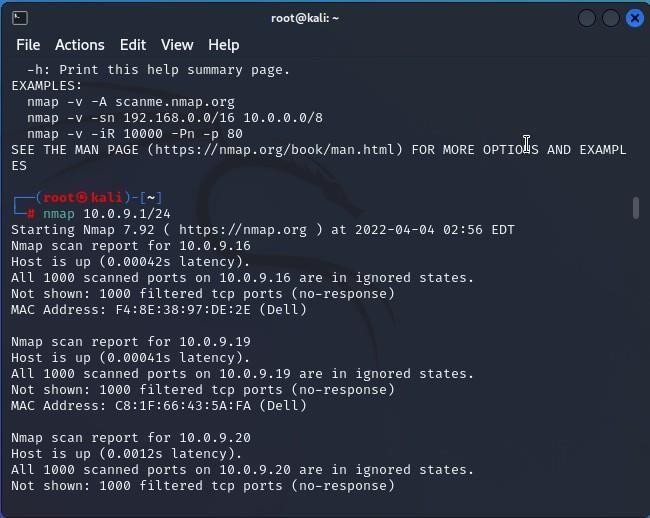
# Scan an Entire Subnet

# Description :

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

**Command** : nmap 10.0.9.1/24

Output :



# Ping Only Scan

Description :

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

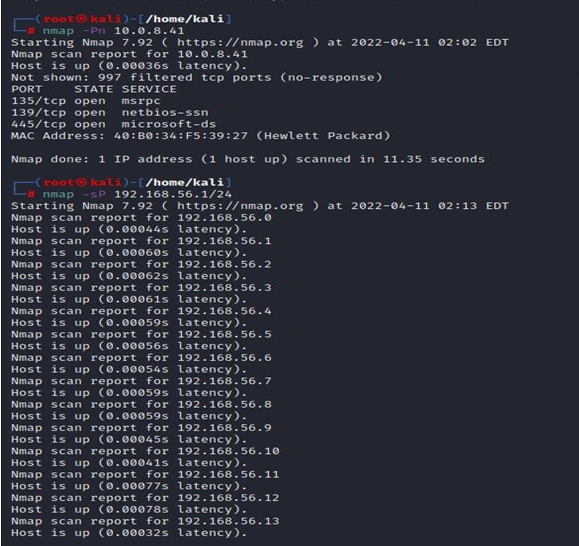
When scanning a local network, you can execute Nmap with root privileges for additional ping functionality. When doing this, the -sP option will perform an ARP ping and return the MAC addresses of the discovered system(s).

Command :

nmap -Pn 10.0.8.41

nmap -sP 192.168.56.1/24

output :



**TCP SYN Ping and TCP ACK Ping**

## DESCRIPTION:

The -PS option performs a TCP SYN ping.

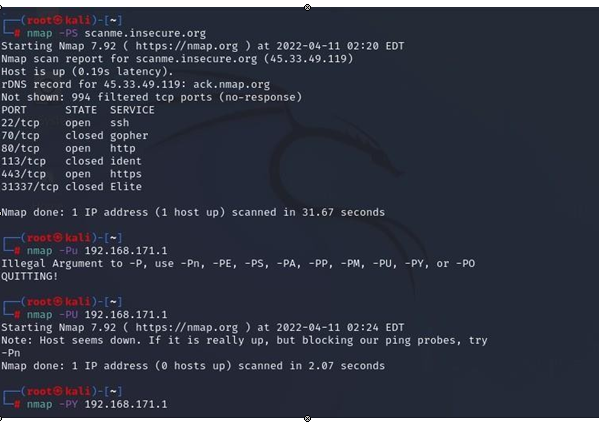
The TCP SYN ping sends a SYN packet to the target system and listens for a response. This alternative discovery method is useful for systems that are configured to block standard ICMP pings.

**Command** :

nmap -PS scanme.insecure.org

nmap -PU 192.168.171.1

Output :



# WEEK 2

# AIM: Implument ZENMAP

## DESCRIPTION:

# Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database

**Commands:**

Open the zenmap tool.

Set target and set the profile

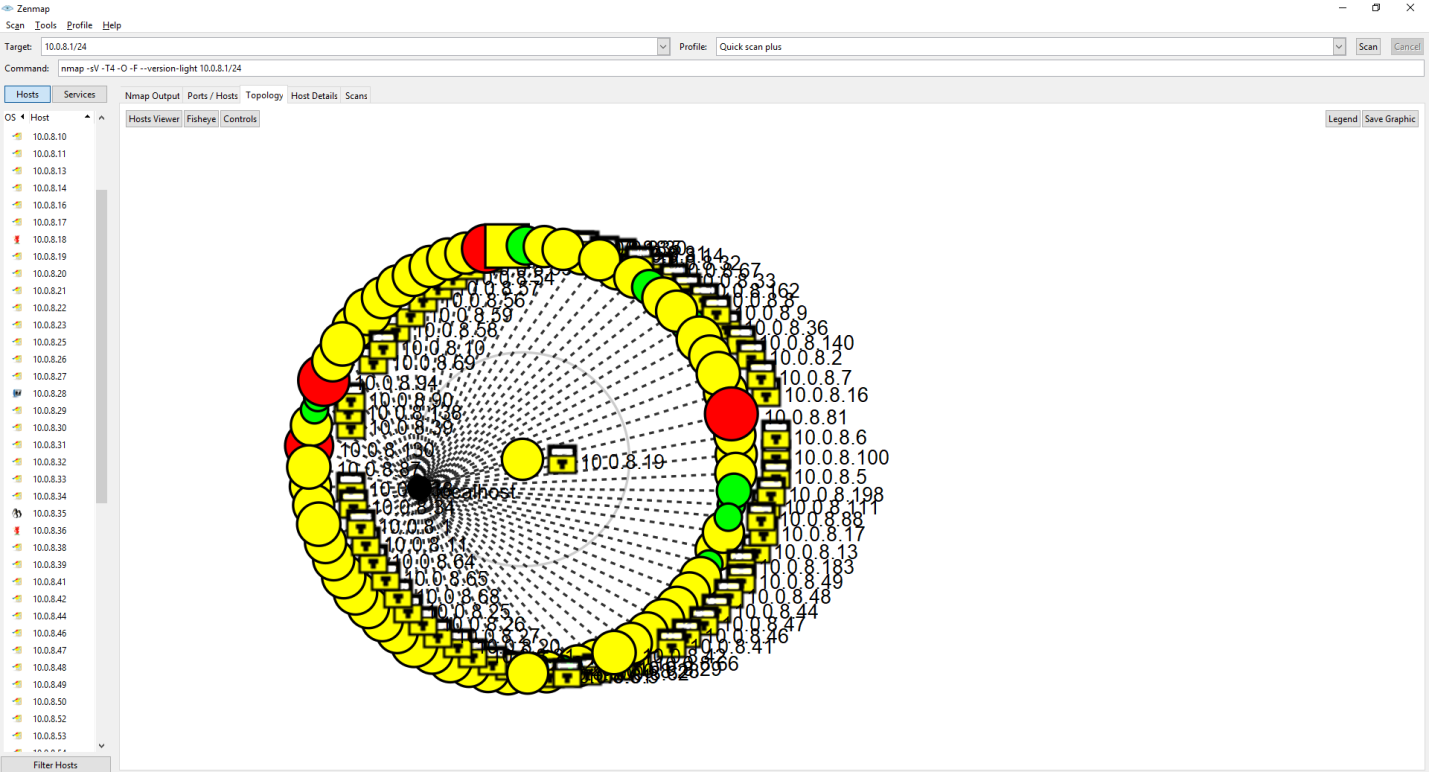
Target: 10.0.8.1/24

Profile: Quick scan plus

Then click on scan to scan the network.

We can see the image in the topology section.

OUTPUT :



**Task Manager**

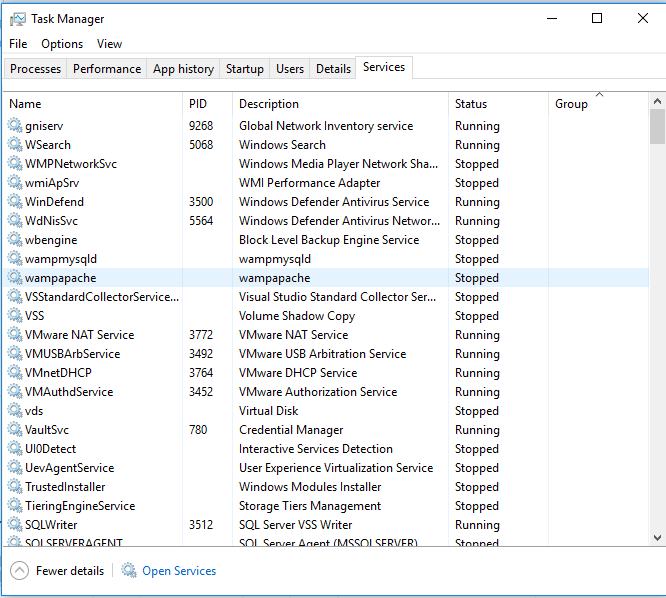
## DESCRIPTION:

Open task manager and click on services option.

It shows all the services that are going in the syst

em up to present.

OUTPUT :



**WEEK-3**

**Angry IP Scanner**

Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has [many other features](https://angryip.org/about/).

It is widely used by network administrators and just curious users around the world, including large and small enterprises, banks, and government agencies.

It runs on Linux, Windows, and Mac OS X, possibly supporting other platforms as well.

**Commands:**

open the Angry IP scanner..

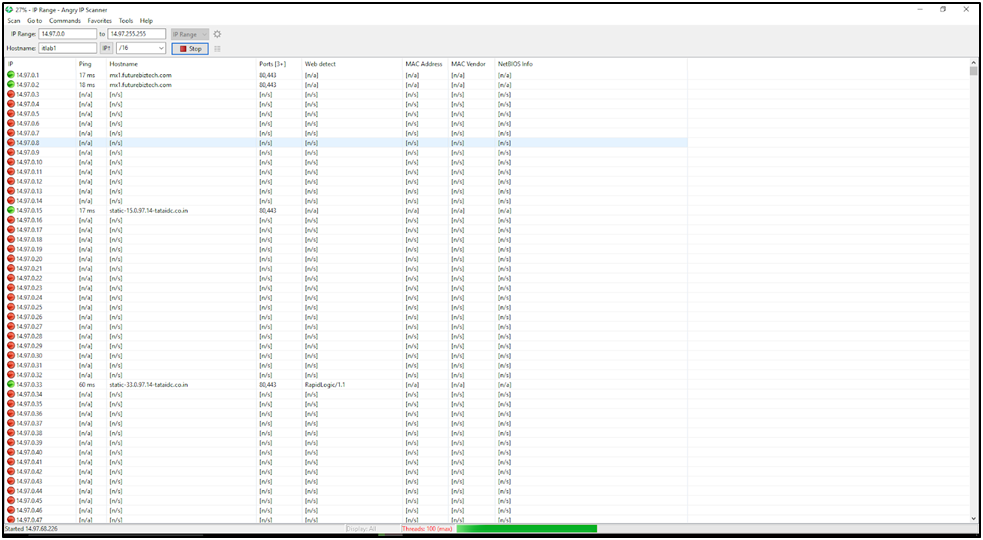
set Ip range and set the IP

Ip range : 10.0.8.0 -10.0.8.255

IP:\24

Then click on scan to scan the network.

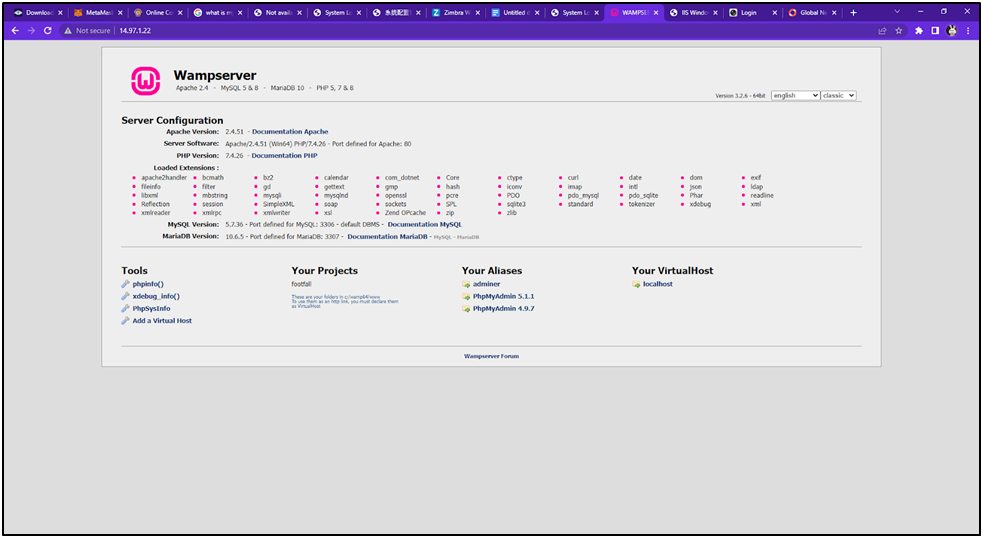
OUTPUT :



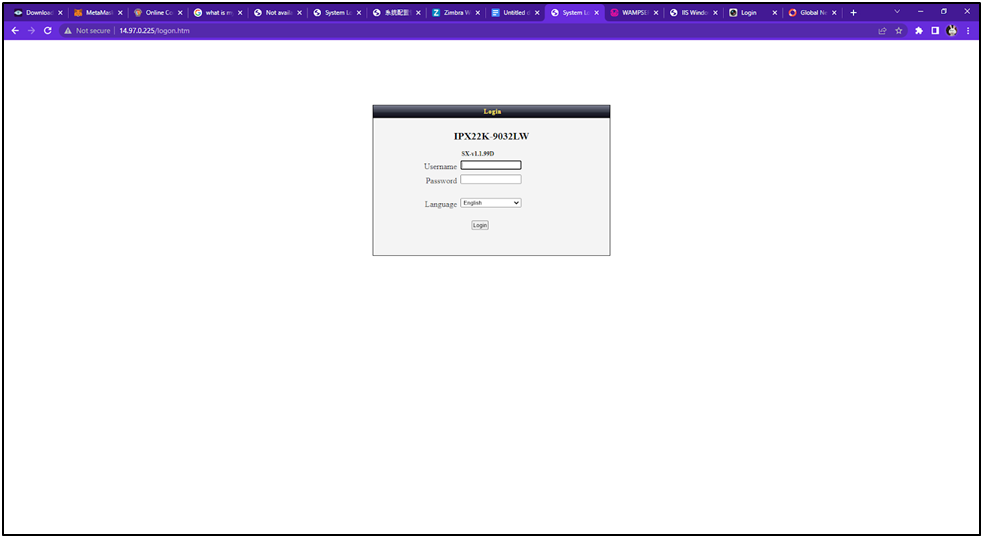
Open the green color which is services on the Google chrome we get some of the services as

Shown below.

Ip 14.97.1.22



Ip 14.97.0.225



**WEEK-4**

**Advanced IP Scanner**

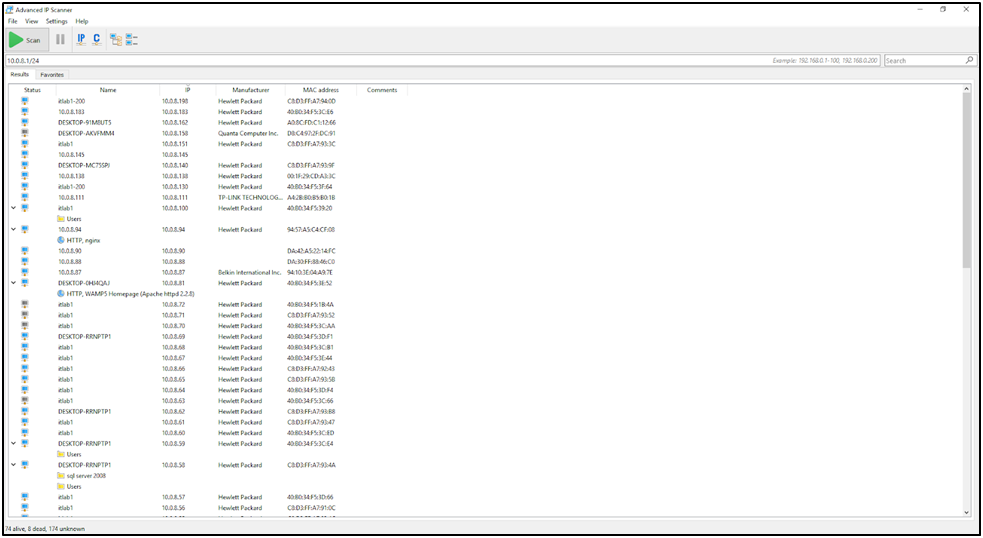
Advanced IP Scanner is a free network scanner that can locate and analyze all computers available on your wireless or wired local network. With its help, you can get remote access to all PCs, such that you can copy and share files present on the shared folders and turn off systems remotely. The application is portable and can be used by network admins anytime, anywhere. The primary purpose of a network scanner is to help administrators manage devices connected to a local network. It’s also useful in keeping track of all IP addresses and ensuring that all devices are connected properly.

**Commands:**

Give the Ip range : 10.0.8./24

Then click on scan to scan the network.

**OUTPUT:**

****

**WEEK-5**

**Global network inventory**

Global Network Inventory is a powerful and flexible software and hardware inventory system that can be used as an audit scanner in an agent-free and zero deployment environments. If used as an audit scanner, it only requires full administrator rights to the remote computers you wish to scan. Global Network Inventory can audit remote computers and even network appliances, including switches, network printers, document centers, etc.

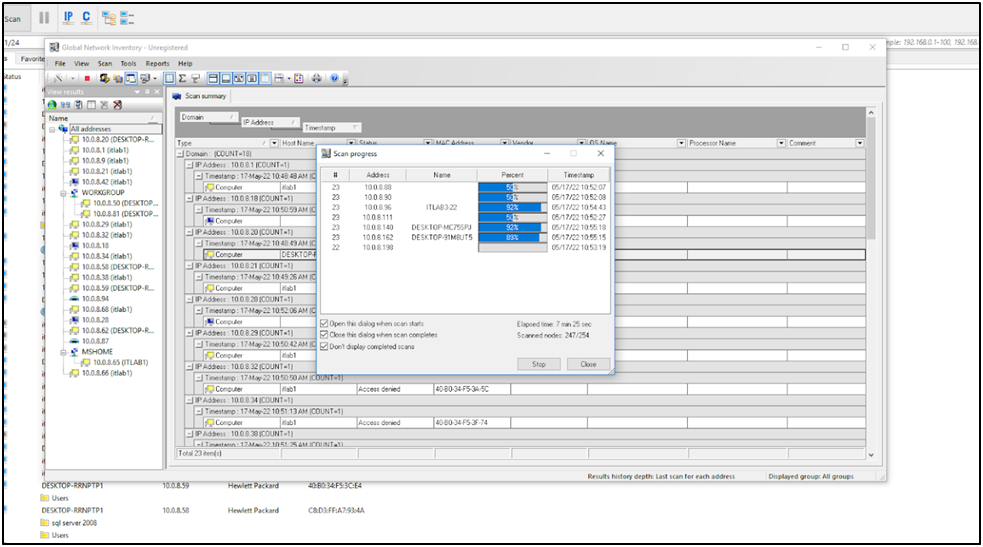
Global Network Inventory agent can also be deployed to perform regular audits initiated through the domain login script when your users log on the network. In this scenario, Global Network Inventory agent is exported to a shared network directory, and audit results are collected in audit repository directory as snap files and later merged into the main database.

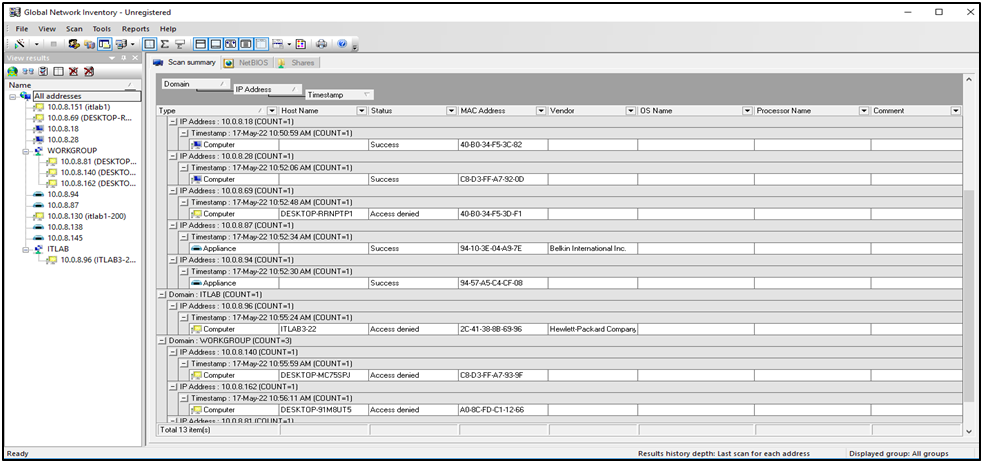
**Commands:**

Select all the default commands to proceed for scan.

And then click on scan then new scan and then the type of scan to i.e., ip range scan and give the IP range and click on next and proceed

OUTPUT:





.

.

.