Date: 208W1A12A0

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

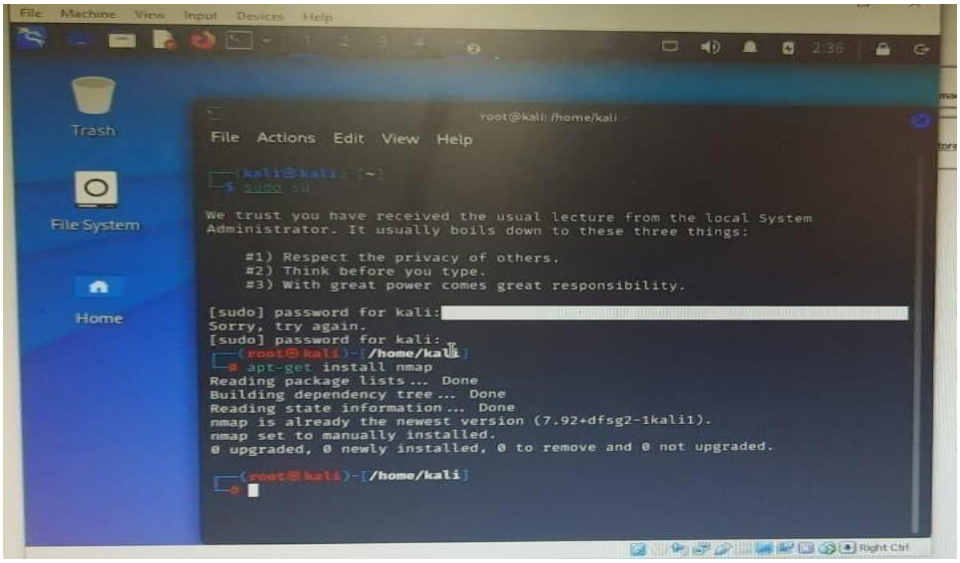
Command :

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 :



Date: 208W1A12A0

Host Scanning :

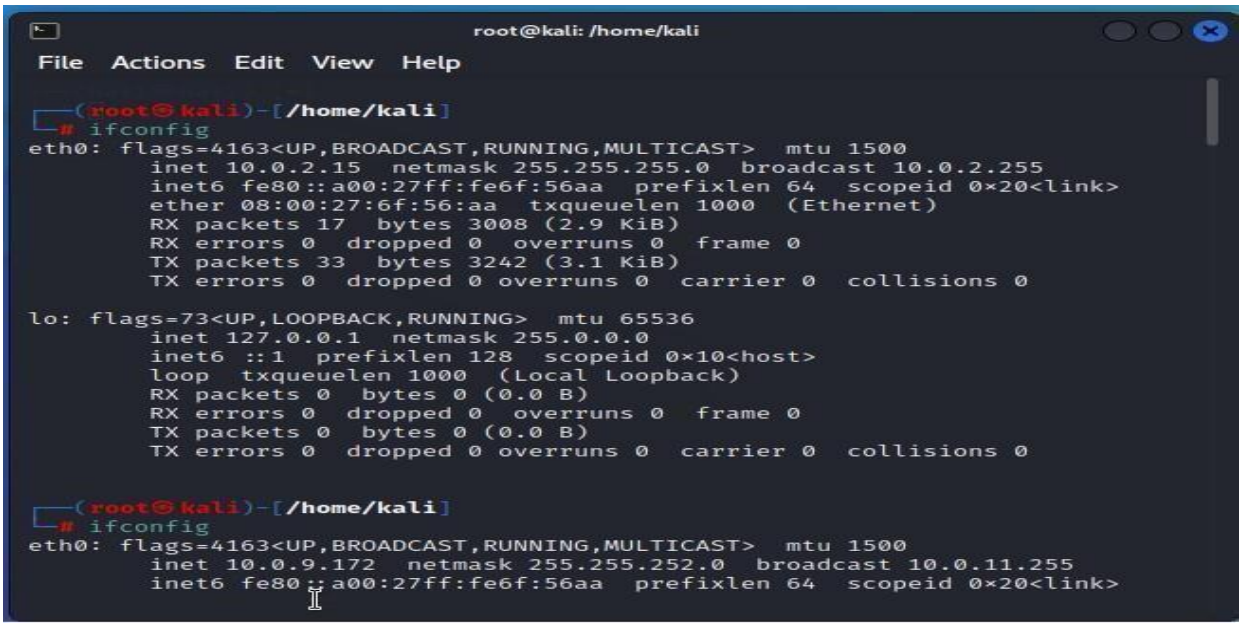
Host scanning returns more detailed information on a particular host or a range of IP addresses. As mentioned above, you can perform a host scan using the following

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 :



```
root@kali: /home/kali
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe6f:56aa  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6f:56:aa  txqueuelen 1000  (Ethernet)
        RX packets 17  bytes 3008 (2.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33  bytes 3242 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.9.172  netmask 255.255.252.0  broadcast 10.0.11.255
        inet6 fe80::a00:27ff:fe6f:56aa  prefixlen 64  scopeid 0x20<link>
```

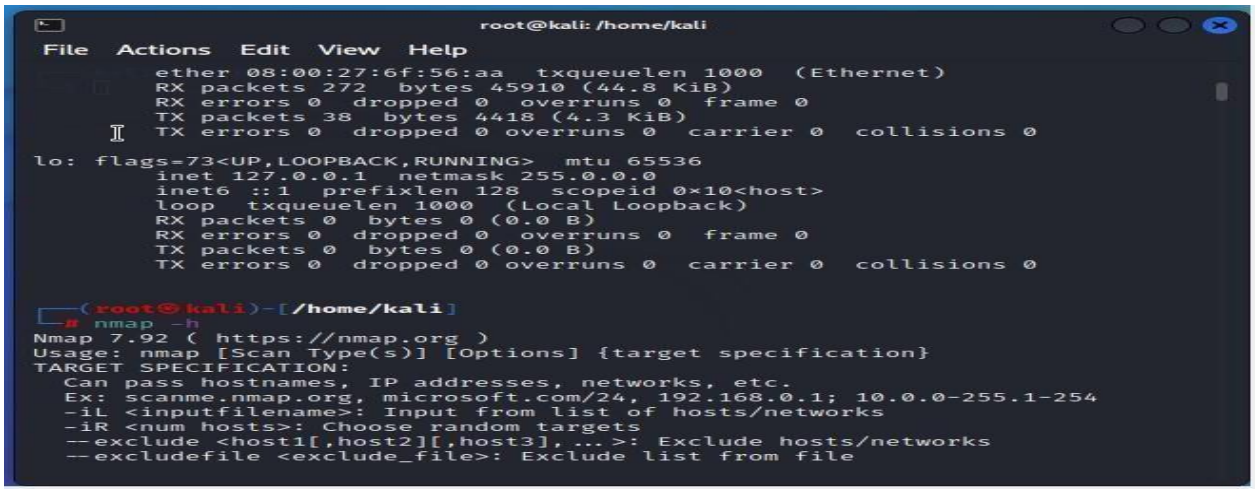
Date: 208W1A12A0

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

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

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

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

Date: 208W1A12A0

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 :

```
$ nmap -sP 192.168.10.2/24

Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-08 20:54 CDT
Host 192.168.10.1 is up (0.0026s latency).
Host 192.168.10.100 is up (0.00020s latency).
Host 192.168.10.101 is up (0.00026s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.18 second
```

Date: 208W1A12A0

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 :

```
root@kali: ~
File  Actions  Edit  View  Help
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPL
ES

┌──(root㉿kali)-[~]
└─# nmap 10.0.9.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-04 02:56 EDT
Nmap scan report for 10.0.9.16
Host is up (0.00042s latency).
All 1000 scanned ports on 10.0.9.16 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: F4:8E:38:97:DE:2E (Dell)

Nmap scan report for 10.0.9.19
Host is up (0.00041s latency).
All 1000 scanned ports on 10.0.9.19 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: C8:1F:66:43:5A:FA (Dell)

Nmap scan report for 10.0.9.20
Host is up (0.0012s latency).
All 1000 scanned ports on 10.0.9.20 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

Date: 208W1A12A0

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 :

```
┌──(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).
```

Date: 208W1A12A0

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 :

```
┌──(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
```

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

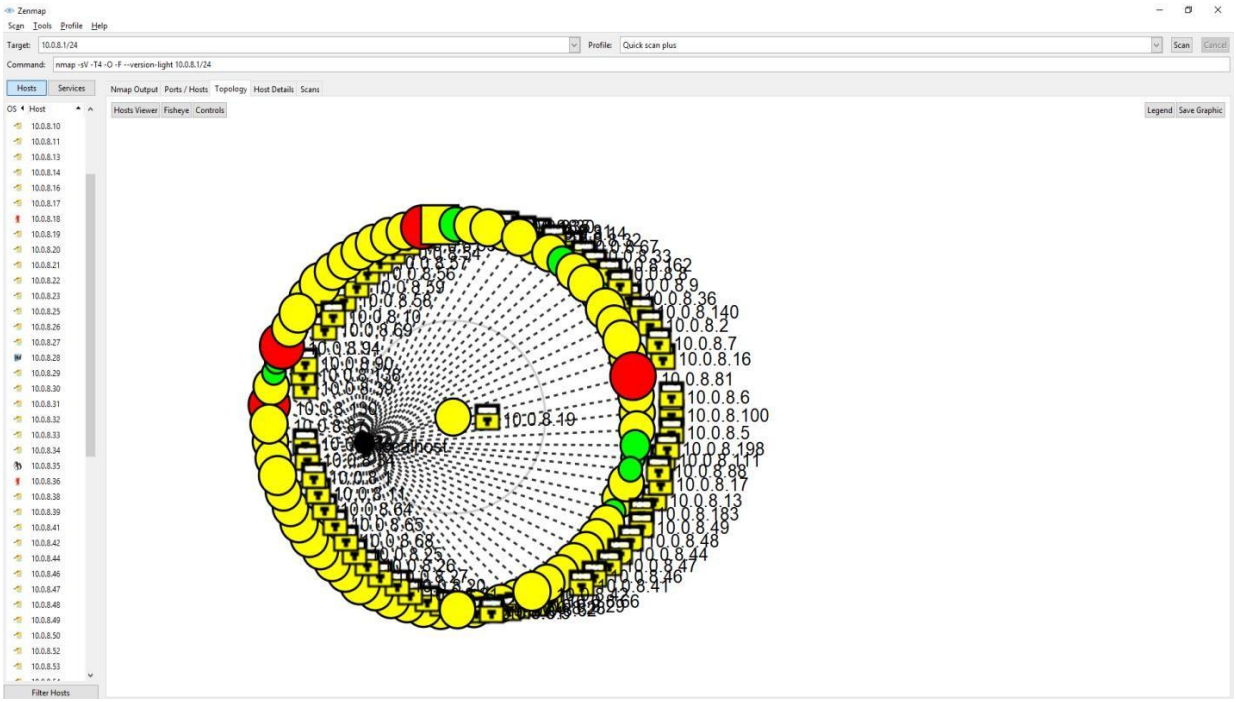
Profile: Quick scan plus

Then click on scan to scan the network.

We can see the image in the topology section.

Date: 208W1A12A0

OUTPUT :



Date: 208W1A12A0

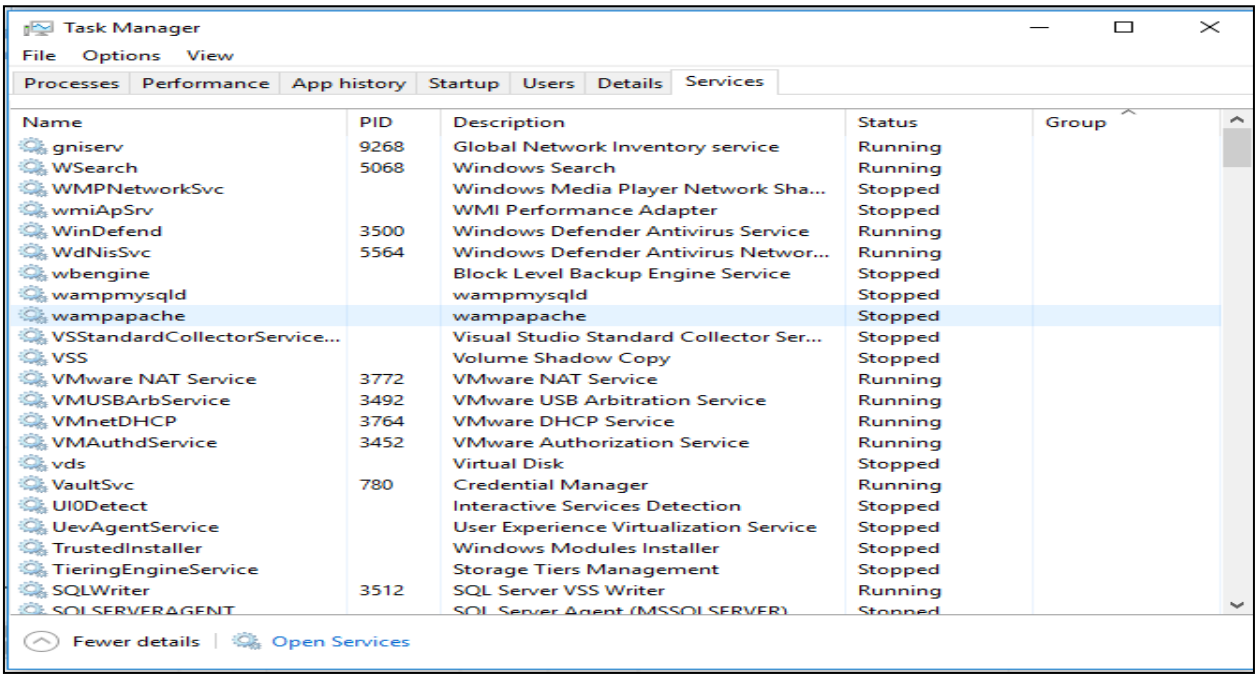
Task Manager

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 :



Name	PID	Description	Status	Group
gniserv	9268	Global Network Inventory service	Running	
WSearch	5068	Windows Search	Running	
WMPNetworkSvc		Windows Media Player Network Sha...	Stopped	
wmiApSrv		WMI Performance Adapter	Stopped	
WinDefend	3500	Windows Defender Antivirus Service	Running	
WdNisSvc	5564	Windows Defender Antivirus Networ...	Running	
wbengine		Block Level Backup Engine Service	Stopped	
wampmysqld		wampmysqld	Stopped	
wampapache		wampapache	Stopped	
VSStandardCollectorService...		Visual Studio Standard Collector Ser...	Stopped	
VSS		Volume Shadow Copy	Stopped	
VMware NAT Service	3772	VMware NAT Service	Running	
VMUSBArbService	3492	VMware USB Arbitration Service	Running	
VMnetDHCP	3764	VMware DHCP Service	Running	
VMAuthdService	3452	VMware Authorization Service	Running	
vds		Virtual Disk	Stopped	
VaultSvc	780	Credential Manager	Running	
UI0Detect		Interactive Services Detection	Stopped	
UevAgentService		User Experience Virtualization Service	Stopped	
TrustedInstaller		Windows Modules Installer	Stopped	
TieringEngineService		Storage Tiers Management	Stopped	
SQLWriter	3512	SQL Server VSS Writer	Running	
SQLSERVERAGENT		SQL Server Agent (MSSQLSERVER)	Stopped	

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.

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.

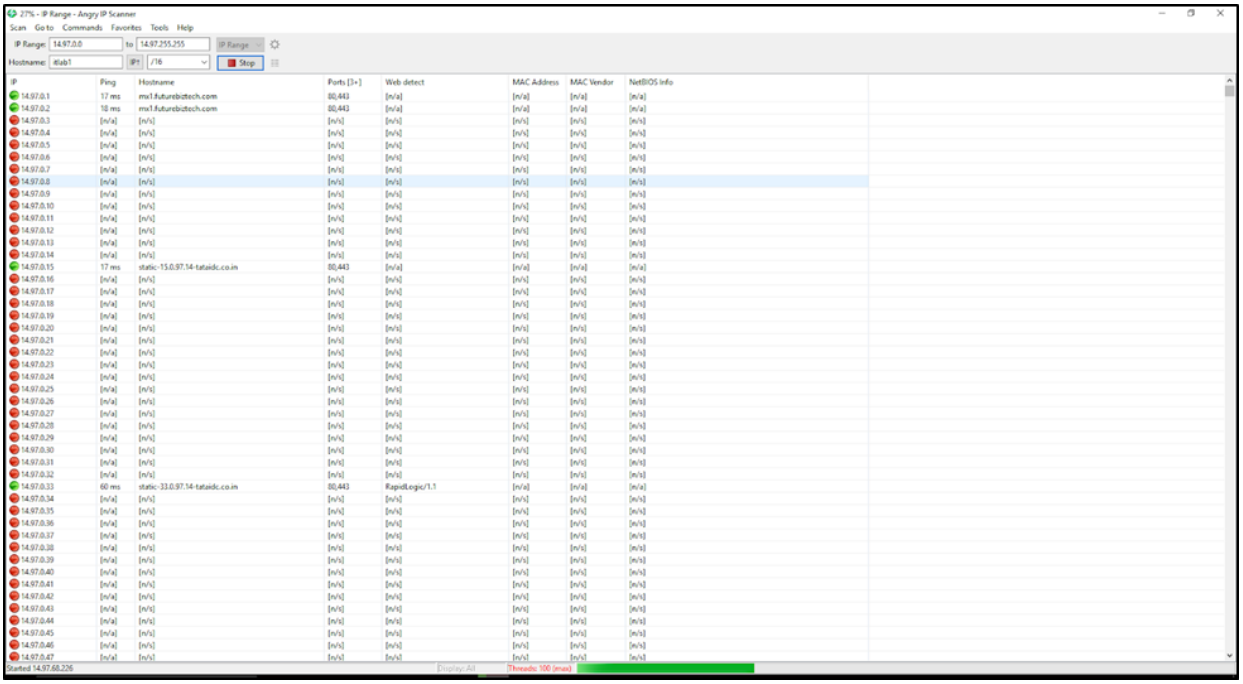
Commands:

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.

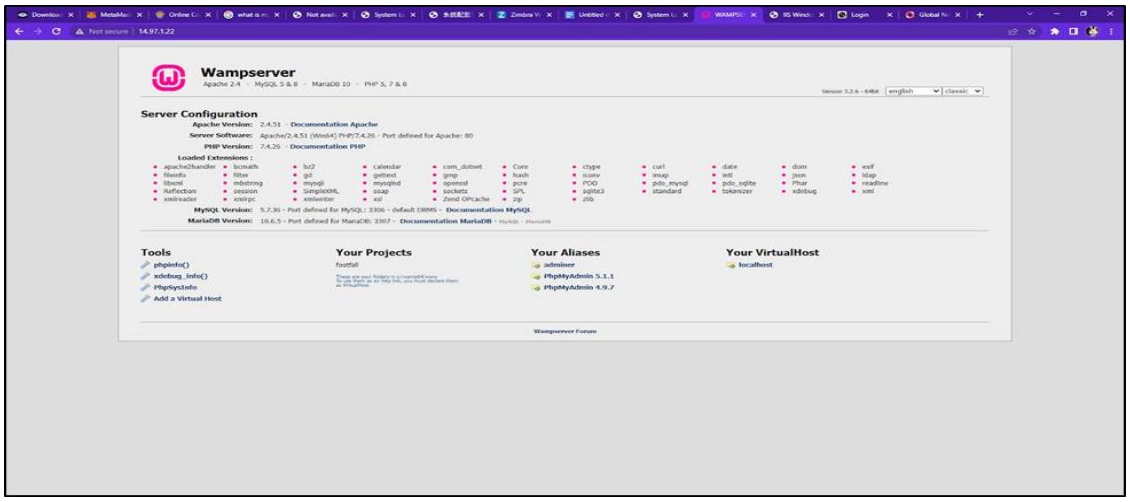
DATE : 208W1A12A0

OUTPUT :



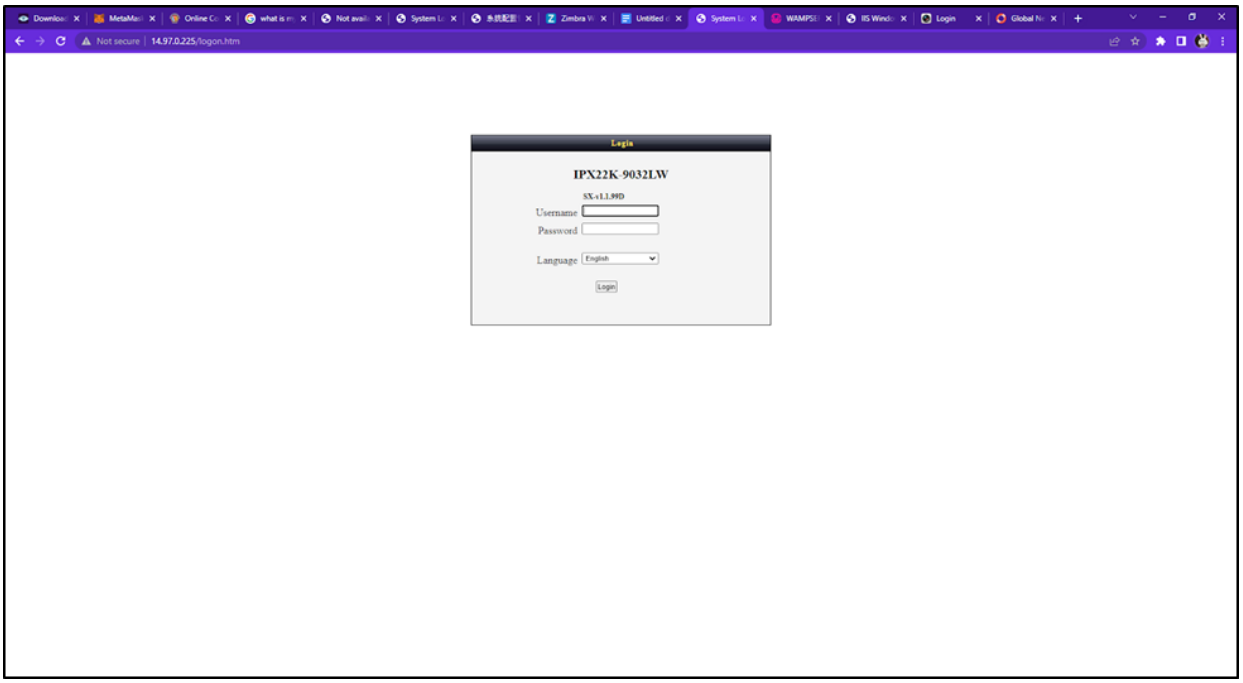
Open the green color which is services on the Google chrome we get some of the services as Shown below.

Ip 14.97.1.22



DATE : 208W1A12A0

Ip 14.97.0.225



WEEK-4

Advanced IP Scanner

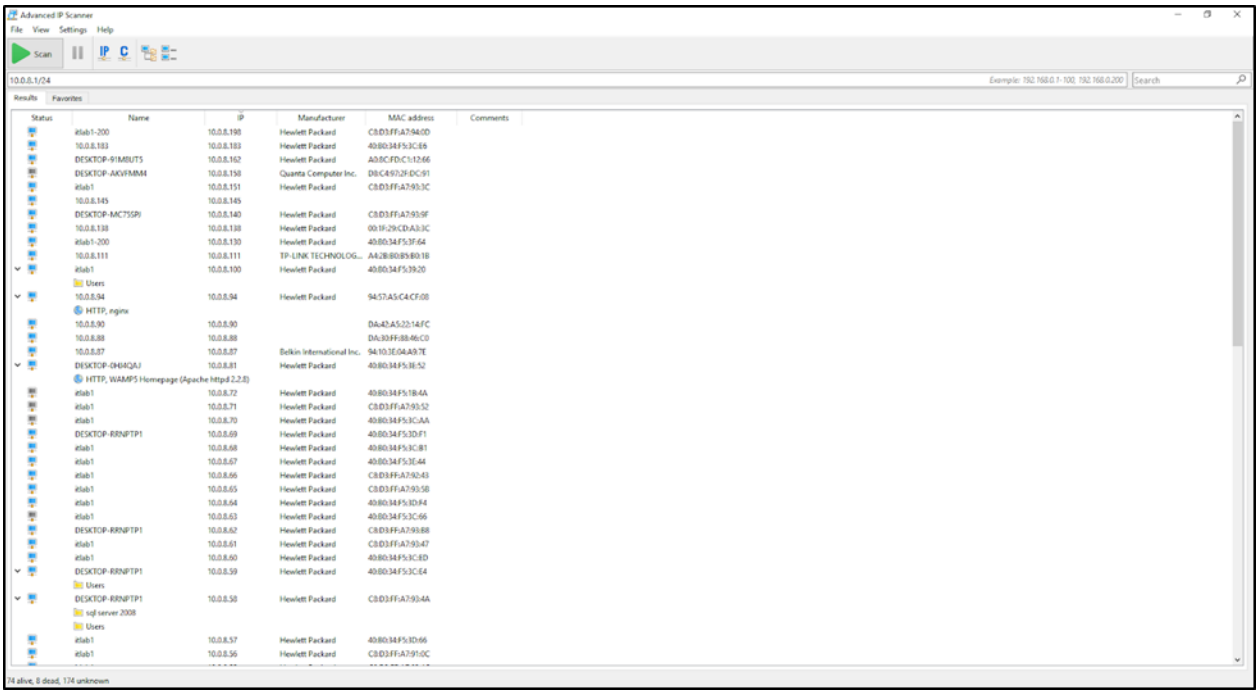
Advanced IP Scanner is a free network scanner that can locate and analyze all computers available on your wireless or wired local network. With its help, you can get remote access to all PCs, such that you can copy and share files present on the shared folders and turn off systems remotely. The application 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:



DATE : 208W1A12A0

WEEK-5

Global network inventory

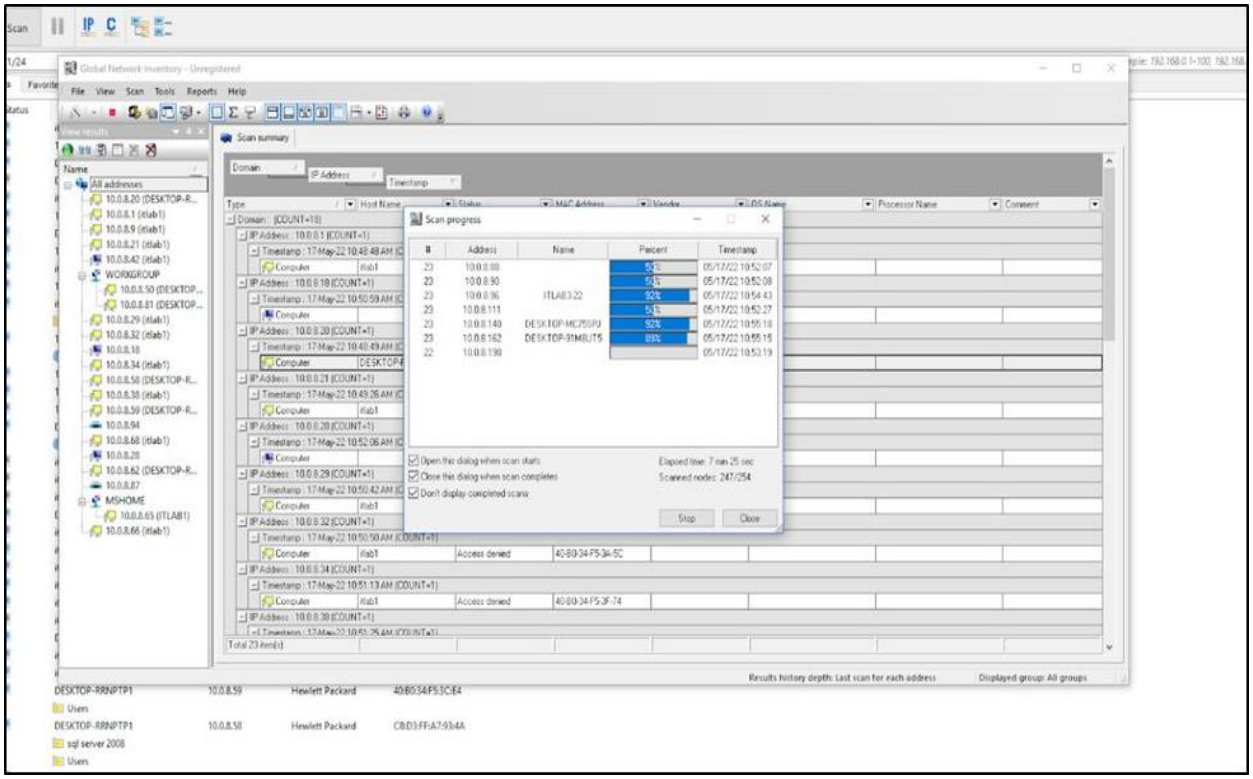
Global Network Inventory is a powerful and flexible software and hardware inventory system that can be used as an audit scanner in an agent-free and zero deployment environments. If used as an audit scanner, it only requires full administrator rights to the remote computers you wish to scan. Global Network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



DATE : 208W1A12A0