ST. FRANCIS INSTITUTE OF TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY
SECURITY LAB

Experiment – 8: Study of network scanning tool NMAP/ZENMAP

Aim: To scan the network for vulnerabilities using different NMAP/ZENMAP commands.

Objective: After performing the experiment, the students will be able to –

- Install and use nmap and use it for gathering detailed network and remote host information.

Lab objective mapped: L502.6: Students should be able to Apply network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols, such as SSL, IPSEC, and PGP, and authentication mechanisms to design secure applications.

Prerequisite: Basic knowledge of network security.

Requirements: Windows OS/Unix/Linux, NMAP or ZENMAP

Pre-Experiment Theory:

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon. It is used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

Nmap features include:

- Host Discovery – Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.
- Port Scanning – Enumerating the open ports on one or more target hosts.
- Version Detection – Interrogating listening network services listening on remote devices to determine the application name and version number.
- OS Detection – Remotely determining the operating system and some hardware characteristics of network devices.

Basic commands working in Nmap:

- For target specifications: nmap <target's URL or IP with spaces between them>
- For OS detection: nmap -O <target-host's URL or IP>
- For version detection: nmap -sV <target-host's URL or IP>
- SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections

Implementation & Procedure:

Zenmap is the official graphical user interface (GUI) for the Nmap Security Scanner. It is a multi-platform, free and open-source application designed 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 scans can be compared with one another to see how they differ.

1) Learn the steps to install Zenmap tool on the system.
2) Study the Zenmap documentation for using its GUI.
3) Scan the network with following scan types.
    a. Ping scan
    b. Quick scan
    c. Intense scan

    Choose following targets,

    1. scanme.nmap.org
    2. Public IP address of SFIT website
4) Observe following features of Zenmap,
    a. Host
    b. Services
    c. Nmap output, Ports/Hosts, Topology, Host Details, Scans
5) Take Screenshots(SS) for all features. Write observations for each SS.

Post Experimental Exercise- *(to be handwritten on journal sheets)*

Answer the following Questions:

1. What is Nmap?
2. What is port scanning?
3. Explain the features of Nmap that you have studied.
4. Explain the commands used in Nmap.

Conclusion:

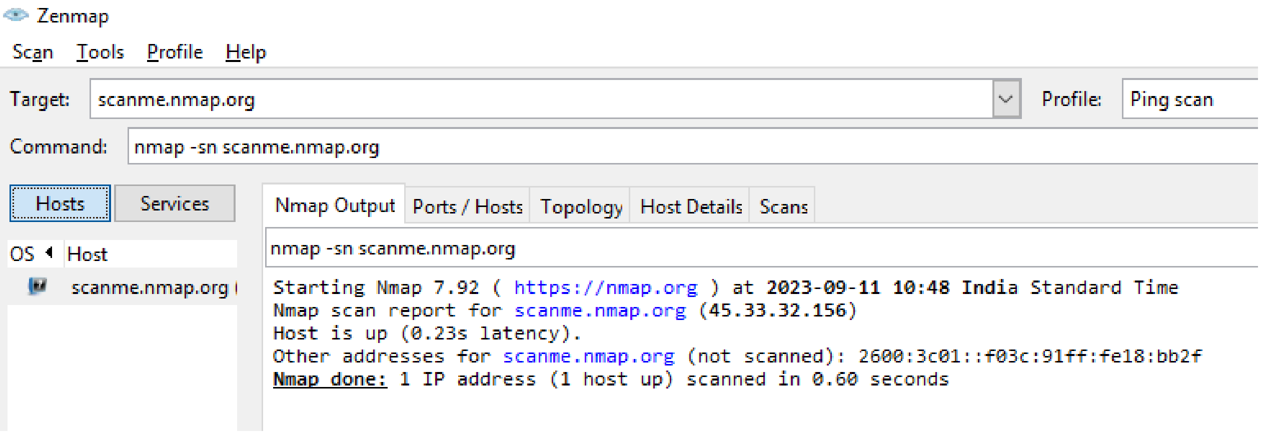
In this experiment Network mapping tool ‘Nmap’ was studied and different types of Nmap scans were used to gather host and network related information. We also learned that Nmap is an active reconnaissance tool which directly probes the target/victim for information gathering.

References: *(Mention your references here.)*

1. ‘Nmap official website’, https://nmap.org/ *(Use for installation of Nmap)*
2. “Chapter 12. Zenmap GUI Users' Guide”, https://nmap.org/book/zenmap.html

Screenshot:

Scan: Ping scan & Target: scanme.nmap.org



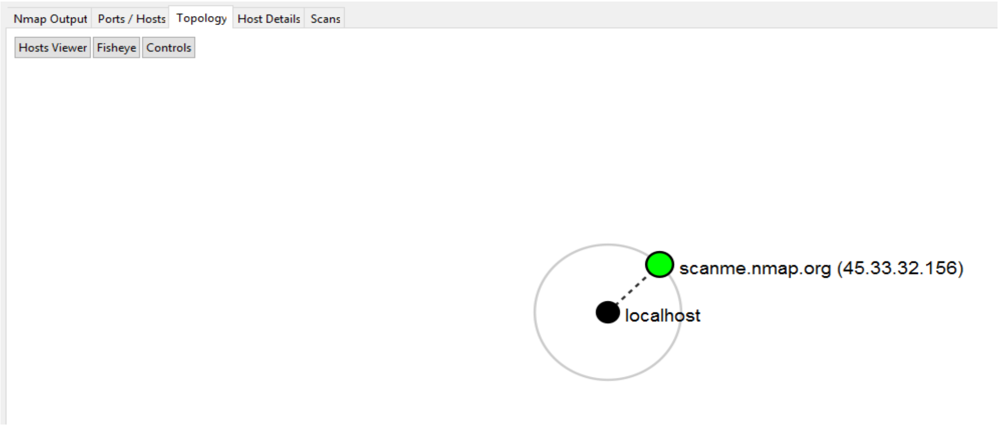
Target: scanme.nmap.org

Profile: Ping scan

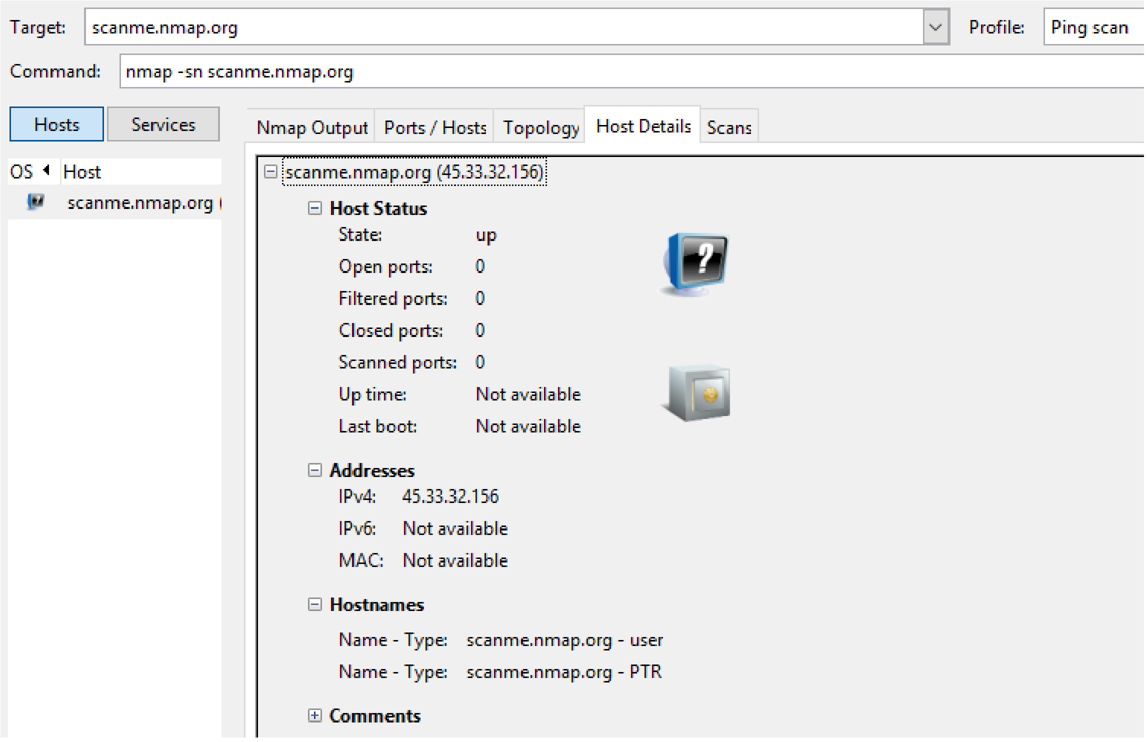
Command: nmap -sn scanme.nmap.org

```
nmap -sn scanme.nmap.org

Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-11 10:48 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

In the Screenshot above, we used Zenmap GUI to Scan the network with ping scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. We executed this in the Windows operating system but if we want to execute the same thing in Linux then the provided command in the screenshot is being used in the command line interface. We observe the Nmap Output which shows us the ip address and host up.



In the Screenshot above, we used Zenmap GUI to Scan the network with ping scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. We observe the topology and find that there are less than 3 hosts at the given network.



Target: scanme.nmap.org

Profile: Ping scan

Command: nmap -sn scanme.nmap.org

scanme.nmap.org (45.33.32.156)

Host Status

State: up

Open ports: 0

Filtered ports: 0

Closed ports: 0

Scanned ports: 0

Up time: Not available

Last boot: Not available

Addresses

IPv4: 45.33.32.156

IPv6: Not available

MAC: Not available

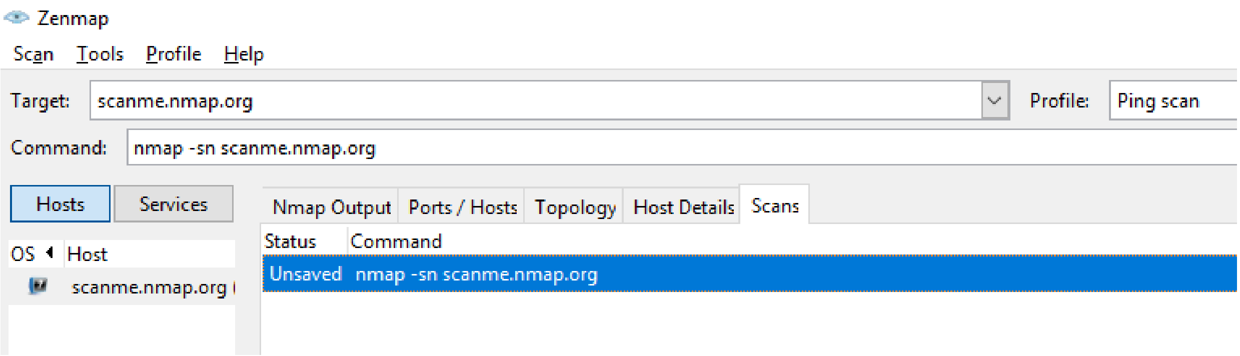
Hostnames

Name - Type: scanme.nmap.org - user

Name - Type: scanme.nmap.org - PTR

Comments

In the Screenshot above, we used Zenmap GUI to Scan the network with ping scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. We observe that the state of the host is up which means the network is active right now and can see the ipv4 address.



Target: scanme.nmap.org

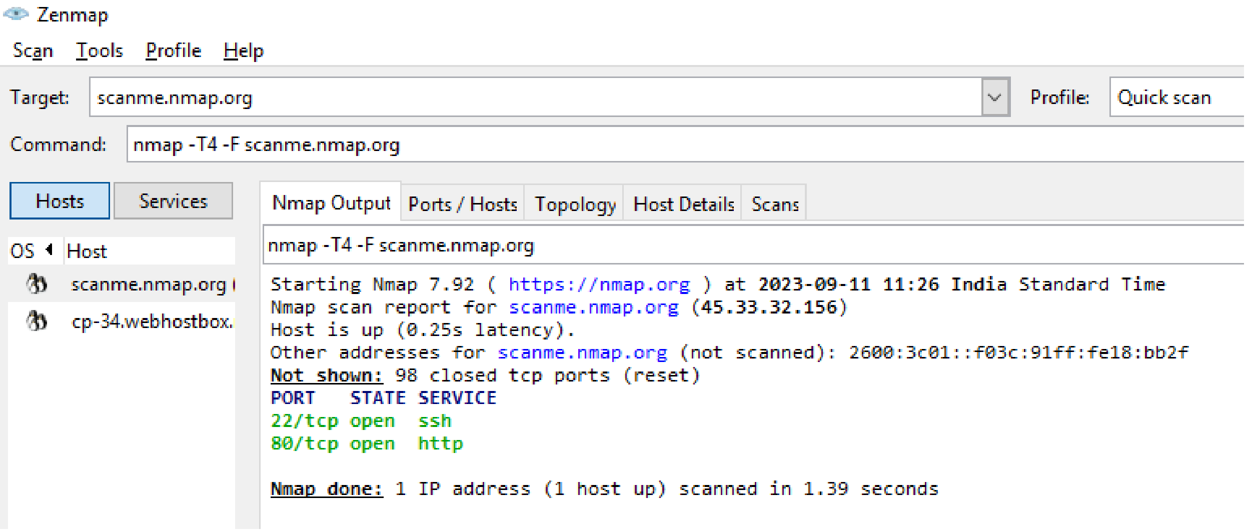
Profile: Ping scan

Command: nmap -sn scanme.nmap.org

Status	Command
Unsaved	nmap -sn scanme.nmap.org

In the Screenshot above, we used Zenmap GUI to Scan the network with ping scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. We observe that we have not saved the inputs.

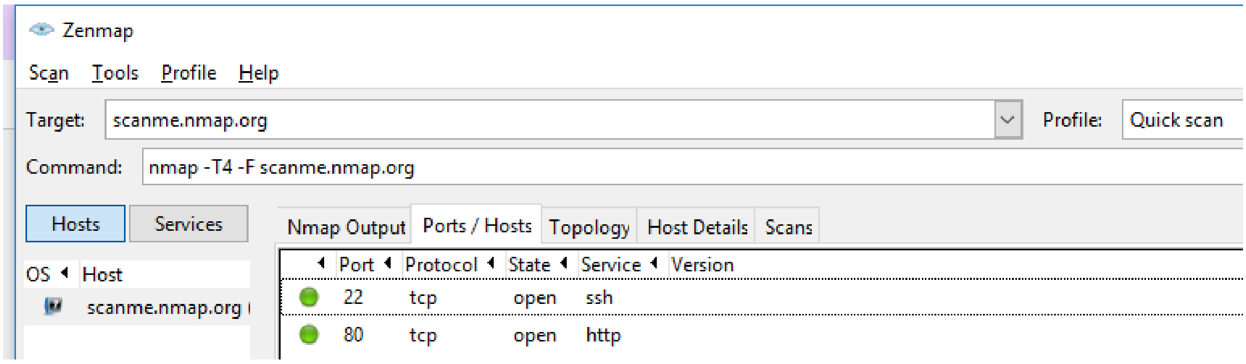
Scan: Quick Scan   & Target: scanme.nmap.org



Target: scanme.nmap.org
Profile: Quick scan
Command: nmap -T4 -F scanme.nmap.org

```
nmap -T4 -F scanme.nmap.org

Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-11 11:26 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 98 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds
```

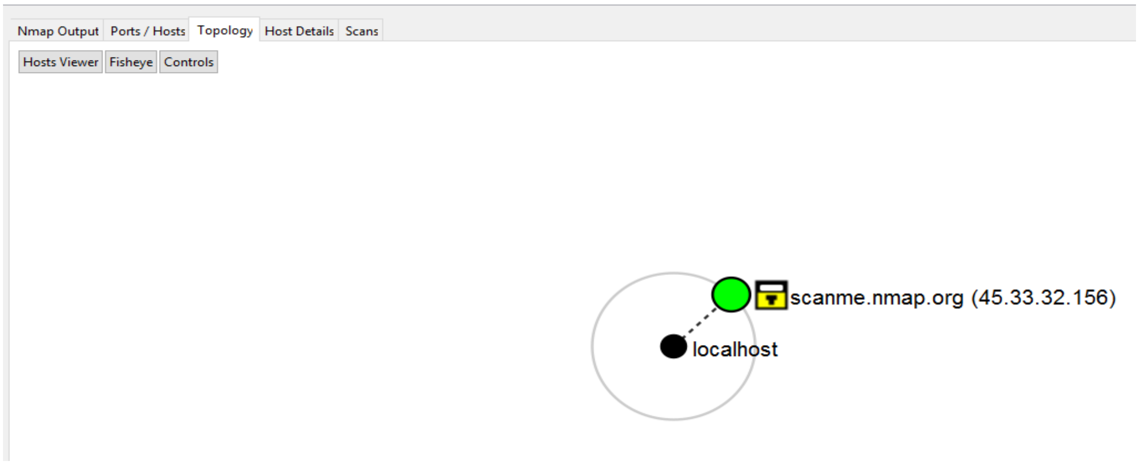
In the Screenshot above, we used Zenmap GUI to Scan the network with Quick scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. We observe Nmap output in which services are there ssh and http and also know the states and ports of each service.



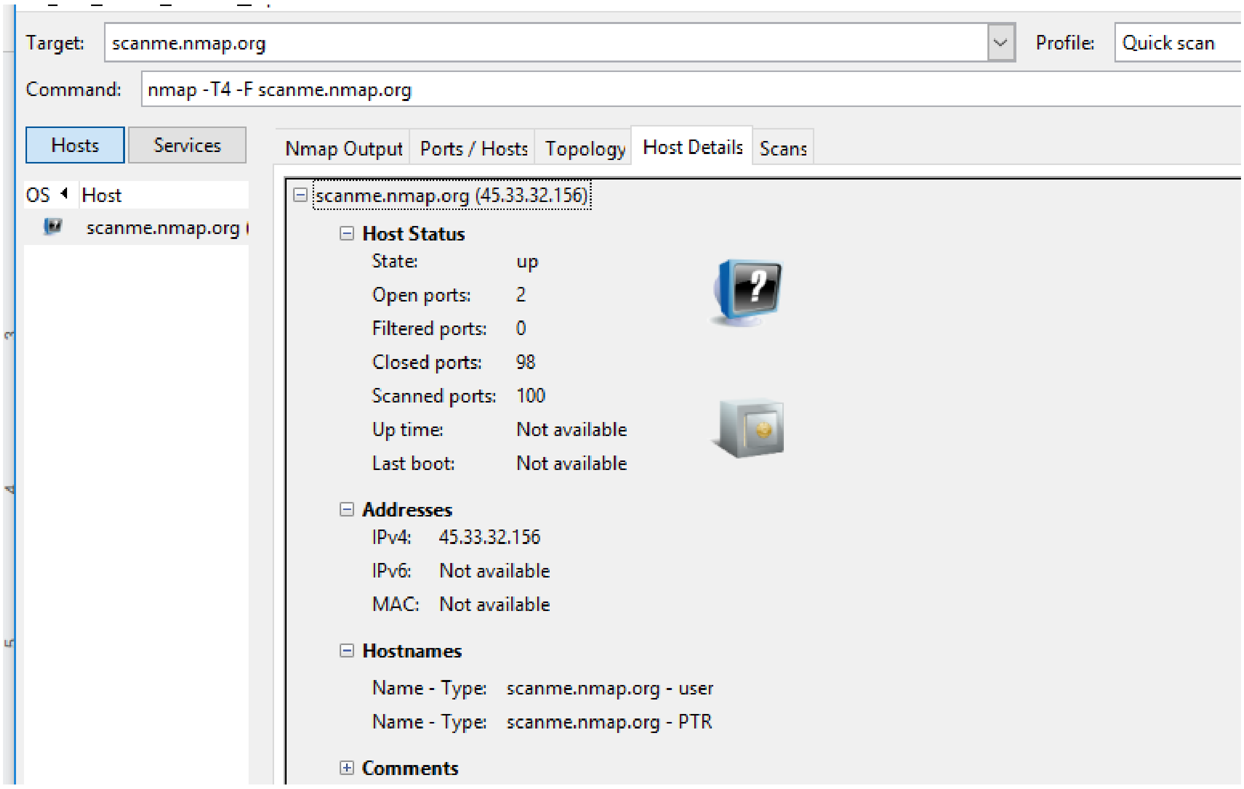
Target: scanme.nmap.org
Profile: Quick scan
Command: nmap -T4 -F scanme.nmap.org

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	
●	80	tcp	open	http	

In the Screenshot above, we used Zenmap GUI to Scan the network with Quick scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. As we can clearly see that green dots and states are open on their respective ports.



In the Screenshot above, we used Zenmap GUI to Scan the network with Quick scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. We observe the topology and find that there are less than 3 hosts at the given network.



Target: scanme.nmap.org
Profile: Quick scan
Command: nmap -T4 -F scanme.nmap.org

scanme.nmap.org (45.33.32.156)

Host Status

State:	up
Open ports:	2
Filtered ports:	0
Closed ports:	98
Scanned ports:	100
Up time:	Not available
Last boot:	Not available

Addresses

IPv4:	45.33.32.156
IPv6:	Not available
MAC:	Not available

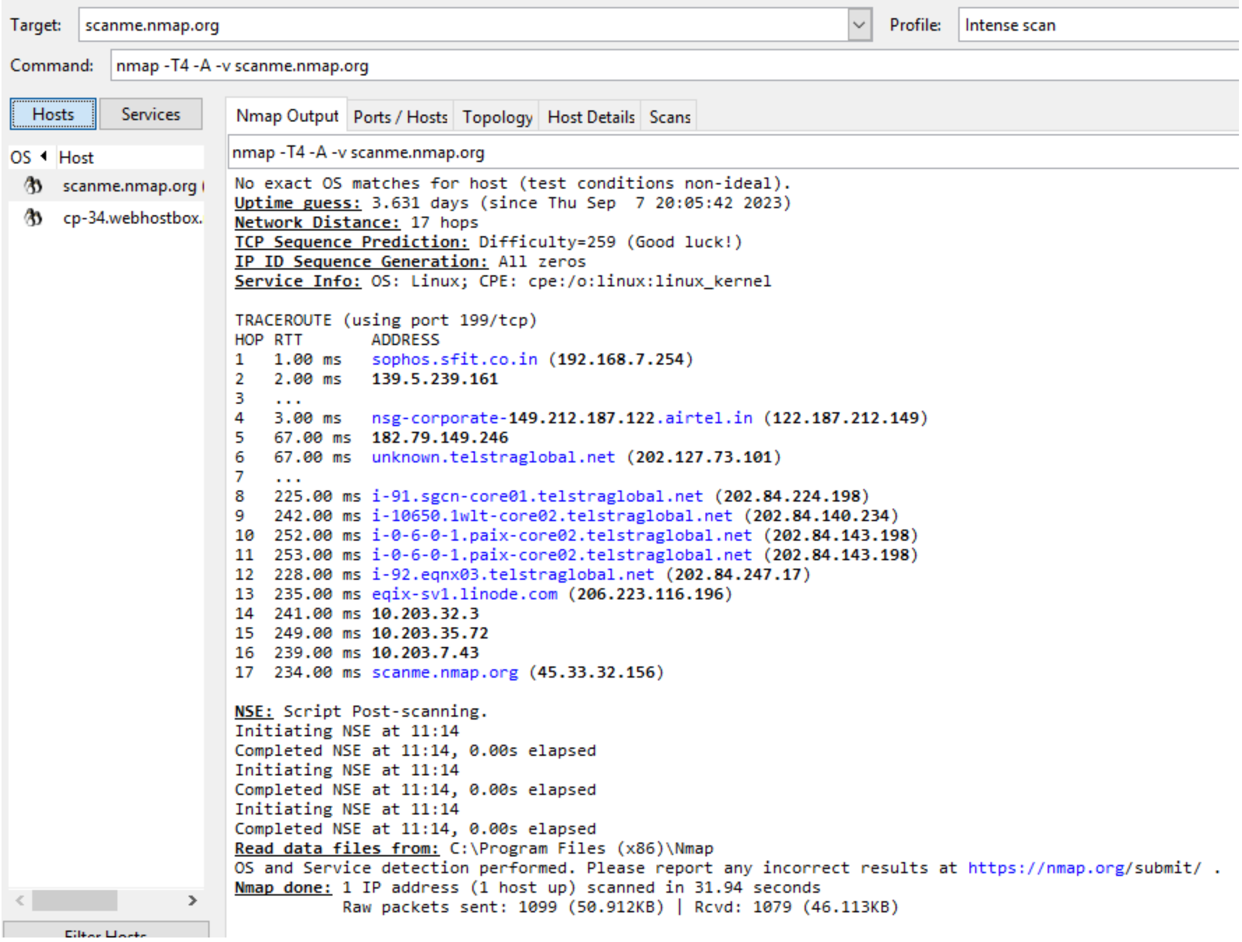
Hostnames

Name - Type:	scanme.nmap.org - user
Name - Type:	scanme.nmap.org - PTR

Comments

In the Screenshot above, we used Zenmap GUI to Scan the network with Quick scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. We observe that the state of the host is up which means the network is active right now and can see the ipv4 address. We also see the open ports, closed ports and Scanned ports numbers.

Scan: Intense Scan & Target: scanme.nmap.org



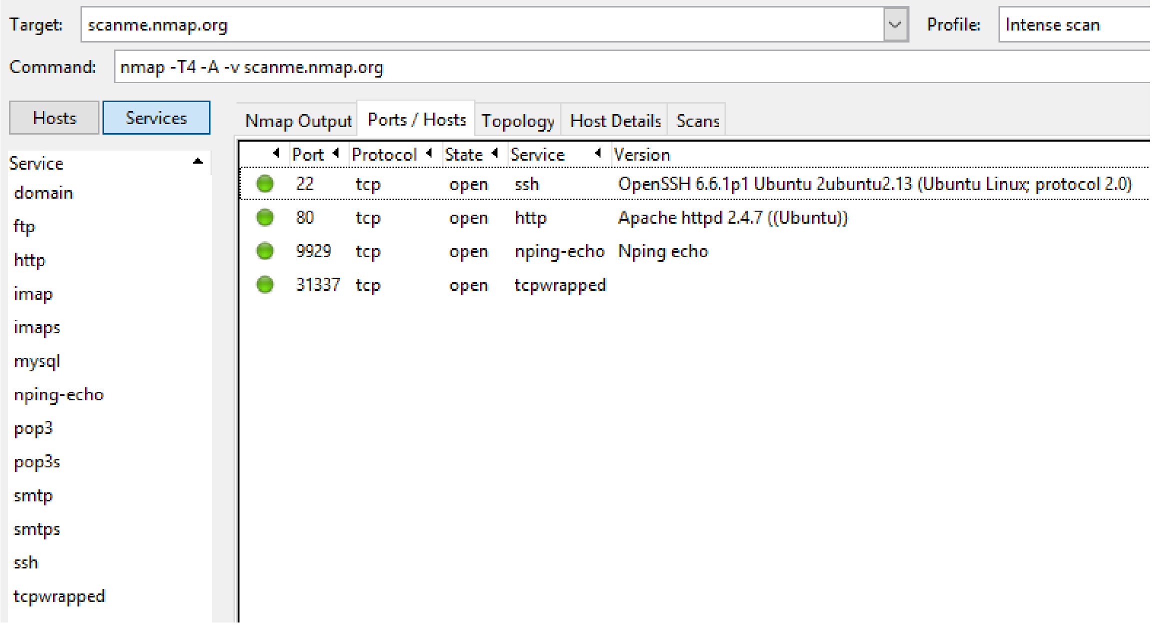
Target: scanme.nmap.org

Profile: Intense scan

Command: nmap -T4 -A -v scanme.nmap.org

```
nmap -T4 -A -v scanme.nmap.org

No exact OS matches for host (test conditions non-ideal).
Uptime guess: 3.631 days (since Thu Sep  7 20:05:42 2023)
Network Distance: 17 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 199/tcp)
HOP RTT       ADDRESS
1   1.00 ms   sophos.sfit.co.in (192.168.7.254)
2   2.00 ms   139.5.239.161
3   ...
4   3.00 ms   nsg-corporate-149.212.187.122.airtel.in (122.187.212.149)
5   67.00 ms  182.79.149.246
6   67.00 ms  unknown.telstraglobal.net (202.127.73.101)
7   ...
8   225.00 ms i-91.sgcn-core01.telstraglobal.net (202.84.224.198)
9   242.00 ms i-10650.1wlt-core02.telstraglobal.net (202.84.140.234)
10  252.00 ms i-0-6-0-1.paix-core02.telstraglobal.net (202.84.143.198)
11  253.00 ms i-0-6-0-1.paix-core02.telstraglobal.net (202.84.143.198)
12  228.00 ms i-92.eqnx03.telstraglobal.net (202.84.247.17)
13  235.00 ms eqix-sv1.linode.com (206.223.116.196)
14  241.00 ms 10.203.32.3
15  249.00 ms 10.203.35.72
16  239.00 ms 10.203.7.43
17  234.00 ms scanme.nmap.org (45.33.32.156)

NSE: Script Post-scanning.
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.94 seconds
           Raw packets sent: 1099 (50.912KB) | Rcvd: 1079 (46.113KB)
```

In the Screenshot above, we used Zenmap GUI to Scan the network with Intense scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. In this type of scan, it scans the vulnerable information in which a hacker can learn much more important things about the target which can observe in the Nmap output.



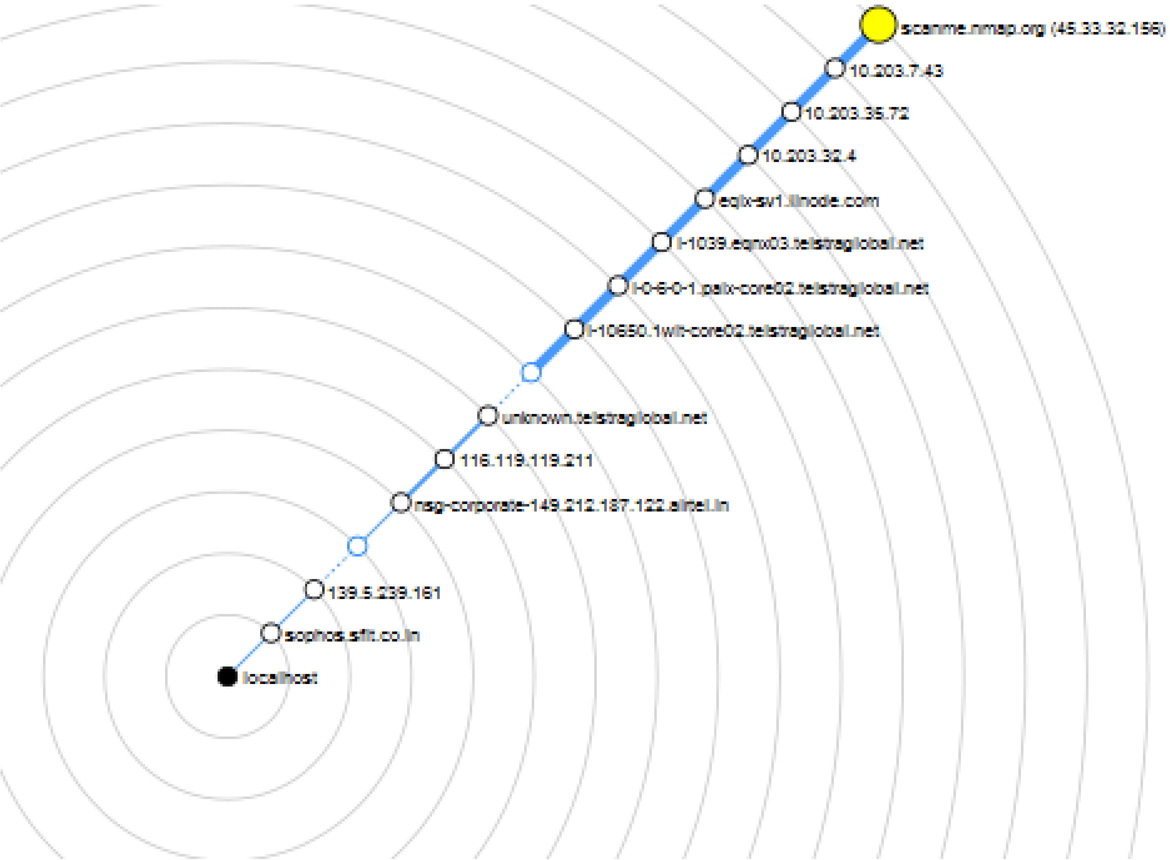
Target: scanme.nmap.org

Profile: Intense scan

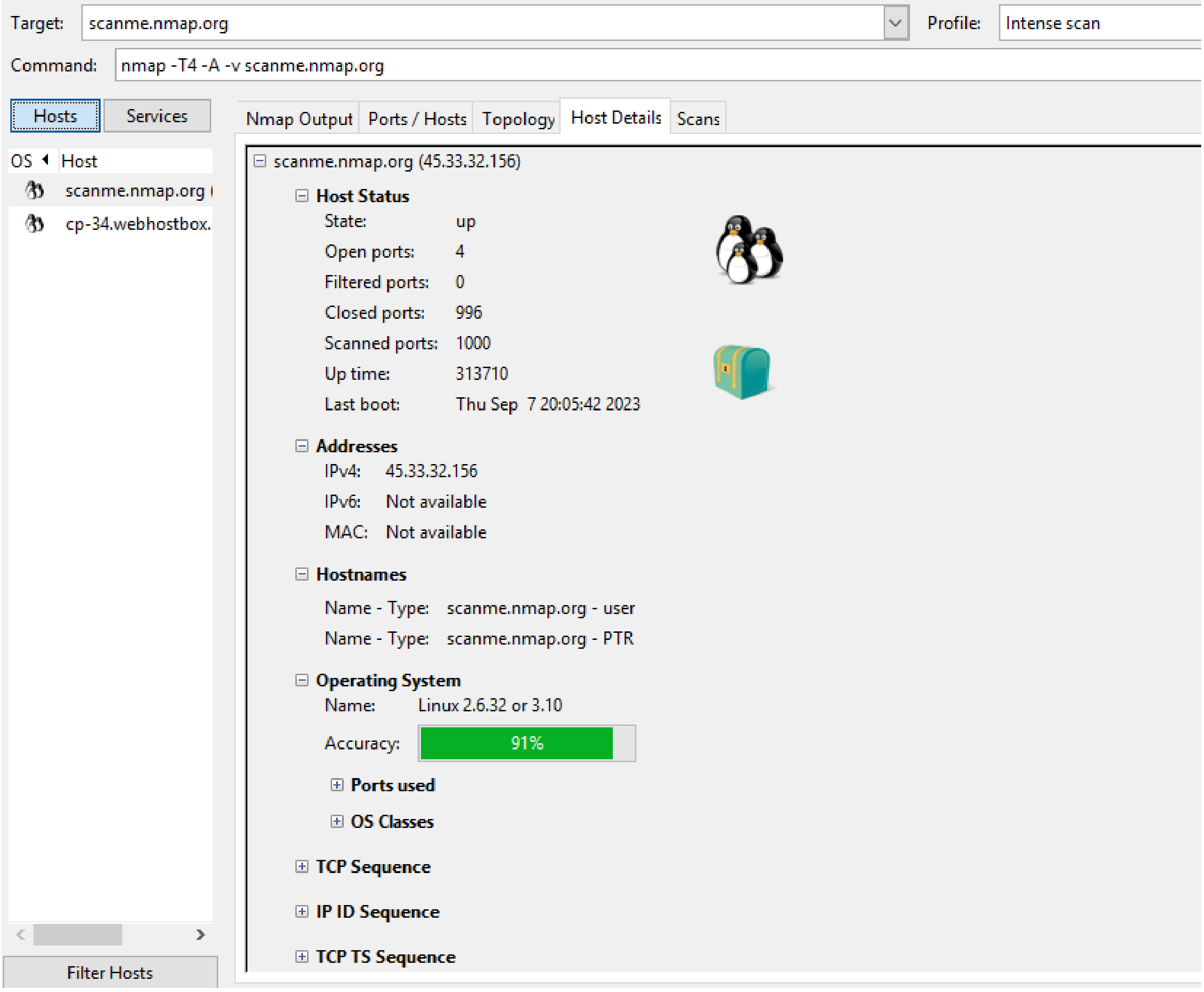
Command: nmap -T4 -A -v scanme.nmap.org

	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
●	80	tcp	open	http	Apache httpd 2.4.7 ((Ubuntu))
●	9929	tcp	open	nping-echo	Nping echo
●	31337	tcp	open	tcpwrapped	

In the Screenshot above, we used Zenmap GUI to Scan the network with Intense scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. In this screenshot we can see the services section in which there are multiple protocols like ftp, http, imap, mysql & etc. From the Ports and Host section we can observe the port, protocol, state, service and version respectively.


scanme.nmap.org (45.33.32.156)
10.203.7.43
10.203.35.72
10.203.32.4
eqix-sv1.linode.com
i-1039.eqnx03.telstraglobal.net
i-0-6-0-1.palx-core02.telstraglobal.net
i-10650.1wlt-core02.telstraglobal.net
unknown.telstraglobal.net
116.119.119.211
nsg-corporate-149.212.187.122.airtel.in
139.5.239.161
sophos.sfit.co.in
localhost

In the Screenshot above, we used Zenmap GUI to Scan the network with Intense scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. We observe the Topology which can show how complex it is. Shows us the entire connection of it from the starting to end.



Target: scanme.nmap.org

Profile: Intense scan

Command: nmap -T4 -A -v scanme.nmap.org

scanme.nmap.org (45.33.32.156)

Host Status

State: up
Open ports: 4
Filtered ports: 0
Closed ports: 996
Scanned ports: 1000
Up time: 313710
Last boot: Thu Sep 7 20:05:42 2023

Addresses

IPv4: 45.33.32.156
IPv6: Not available
MAC: Not available

Hostnames

Name - Type: scanme.nmap.org - user
Name - Type: scanme.nmap.org - PTR

Operating System

Name: Linux 2.6.32 or 3.10
Accuracy: 91%

Ports used

OS Classes

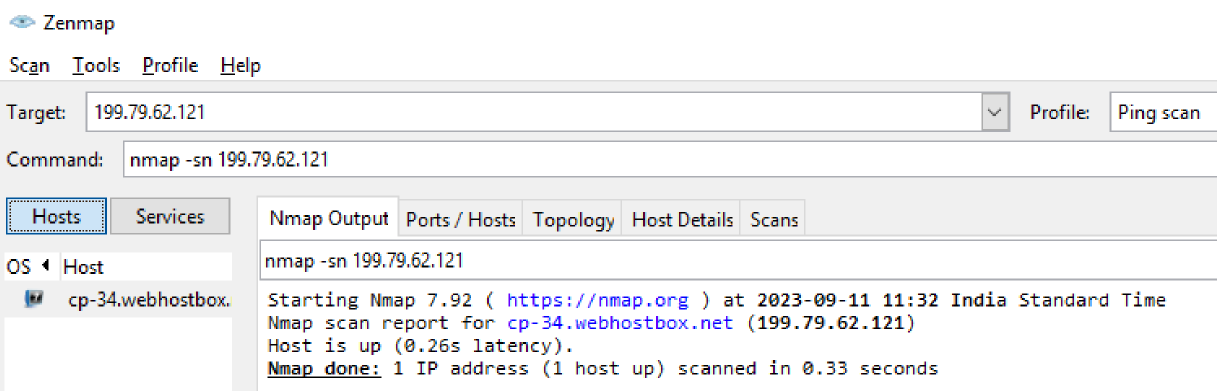
TCP Sequence

IP ID Sequence

TCP TS Sequence

In the Screenshot above, we used Zenmap GUI to Scan the network with Intense scan. In this we target the basic url provided by the Zenmap which is scanme.nmap.org. It shows us the extra information compared to ping, quick scan like operating system name, accuracy, up time, and last boot.

Scan: Ping Scan & Target: sfit.ac.in Or Ip: 199.79.62.121



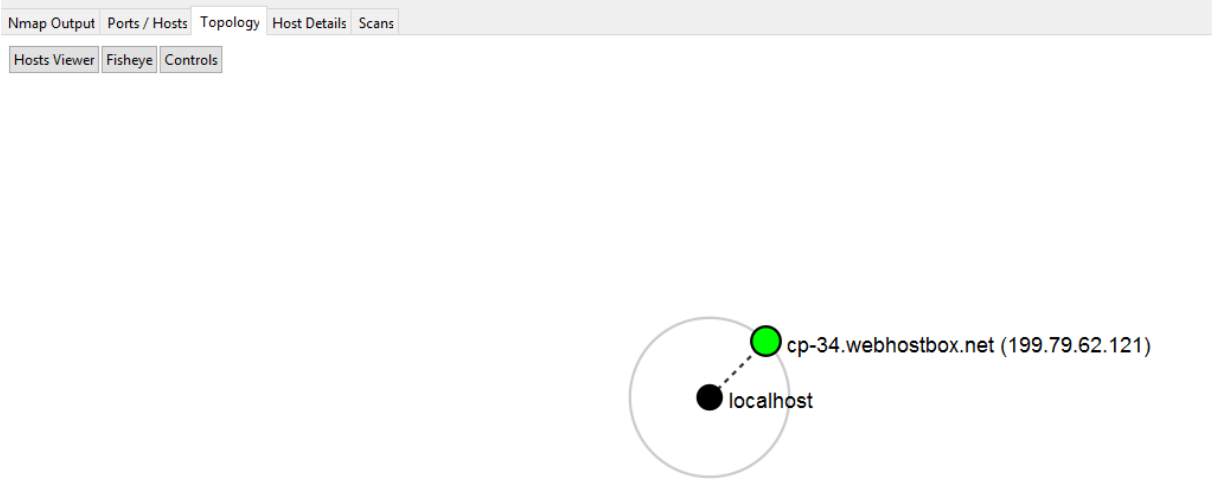
Target: 199.79.62.121

Profile: Ping scan

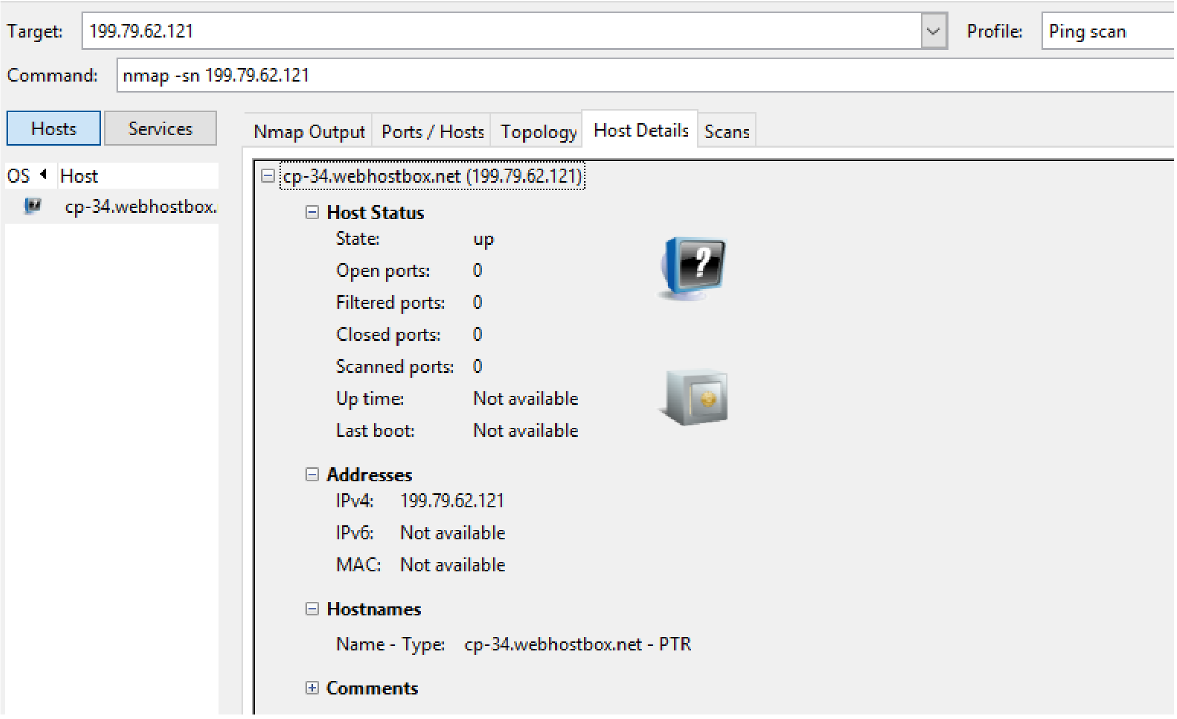
Command: nmap -sn 199.79.62.121

```
nmap -sn 199.79.62.121

Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-11 11:32 India Standard Time
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up (0.26s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

In the Screenshot above, we used Zenmap GUI to Scan the network with ping scan. In this we target the basic url provided by the Zenmap which is sfit.ac.in. We observe that the state of the host is up which means the network is active right now and can see the ipv4 address.



In the Screenshot above, we used Zenmap GUI to Scan the network with ping scan. In this we target the basic url provided by the Zenmap which is sfit.ac.in. We observe the topology and find that there are less than 3 hosts at the given network.



Target: 199.79.62.121 Profile: Ping scan

Command: nmap -sn 199.79.62.121

cp-34.webhostbox.

cp-34.webhostbox.net (199.79.62.121)

Host Status

State: up

Open ports: 0

Filtered ports: 0

Closed ports: 0

Scanned ports: 0

Up time: Not available

Last boot: Not available

Addresses

IPv4: 199.79.62.121

IPv6: Not available

MAC: Not available

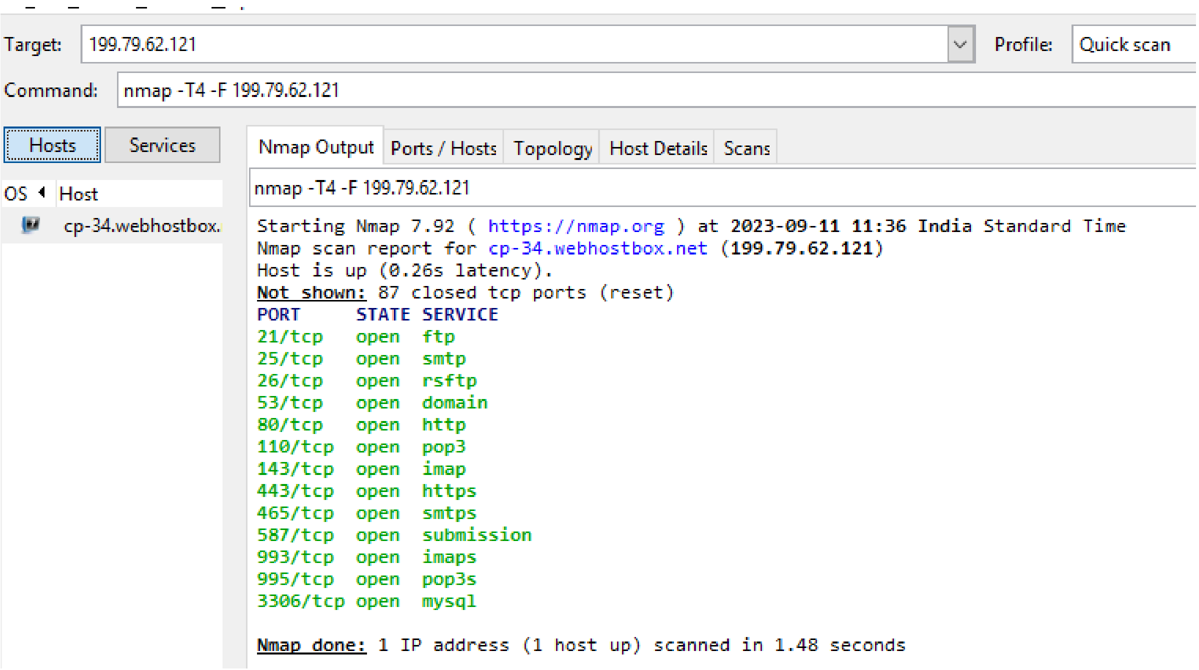
Hostnames

Name - Type: cp-34.webhostbox.net - PTR

Comments

In the Screenshot above, we used Zenmap GUI to Scan the network with ping scan. In this we target the basic url provided by the Zenmap which is sfit.ac.in. In the host details section we observe that the state of the host is up which means the network is active right now and can see the ipv4 address.

Scan: Quick Scan   &   Target: sfit.ac.in Or   ip: 199.79.62.121



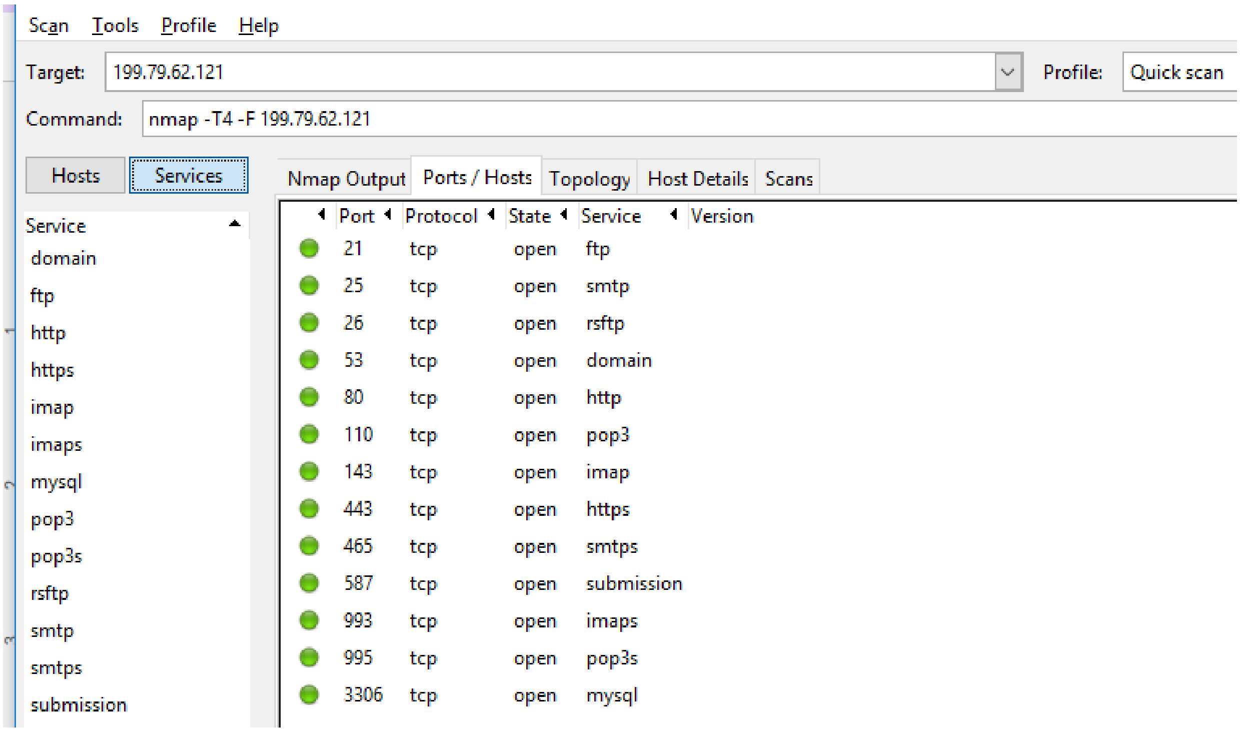
Target: 199.79.62.121

Profile: Quick scan

Command: nmap -T4 -F 199.79.62.121

```
nmap -T4 -F 199.79.62.121

Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-11 11:36 India Standard Time
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up (0.26s latency).
Not shown: 87 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
26/tcp   open  rsftp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

In the Screenshot above, we used Zenmap GUI to Scan the network with Quick scan. In this we target the basic url provided by the Zenmap which is sfit.ac.in. In the Nmap Output section we observe the port, state and of different services.



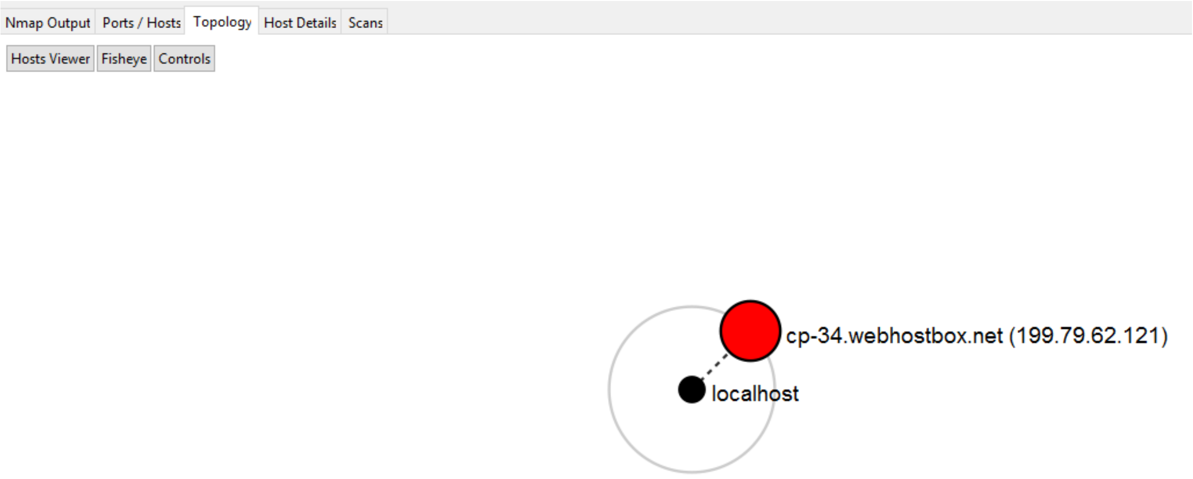
Target: 199.79.62.121

Profile: Quick scan

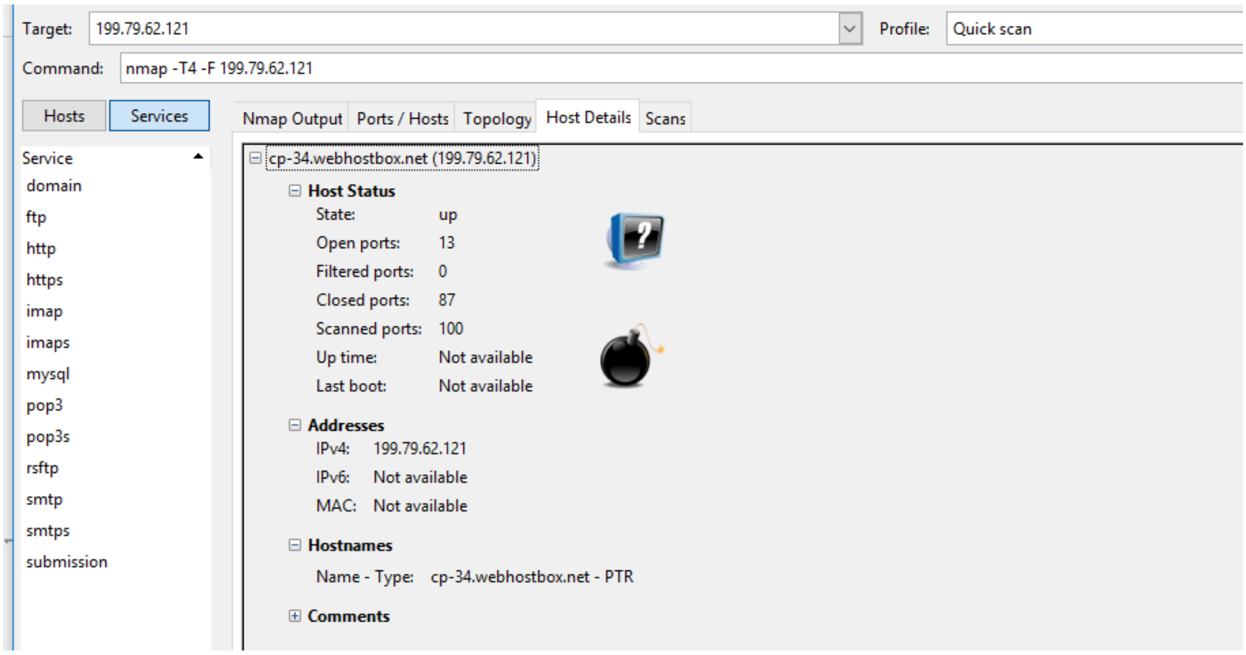
Command: nmap -T4 -F 199.79.62.121

	Port	Protocol	State	Service	Version
●	21	tcp	open	ftp	
●	25	tcp	open	smtp	
●	26	tcp	open	rsftp	
●	53	tcp	open	domain	
●	80	tcp	open	http	
●	110	tcp	open	pop3	
●	143	tcp	open	imap	
●	443	tcp	open	https	
●	465	tcp	open	smtps	
●	587	tcp	open	submission	
●	993	tcp	open	imaps	
●	995	tcp	open	pop3s	
●	3306	tcp	open	mysql	

In the Screenshot above, we used Zenmap GUI to Scan the network with Quick scan. In this we target the basic url provided by the Zenmap which is sfit.ac.in. In the Ports/Hosts section we see multiple protocols with its respective port, state, Service and version.



In the Screenshot above, we used Zenmap GUI to Scan the network with ping scan. In this we target the basic url provided by the Zenmap which is sfit.ac.in. We observe the topology and find that there is red circle which denote that there are more than 3 hosts at the given network.



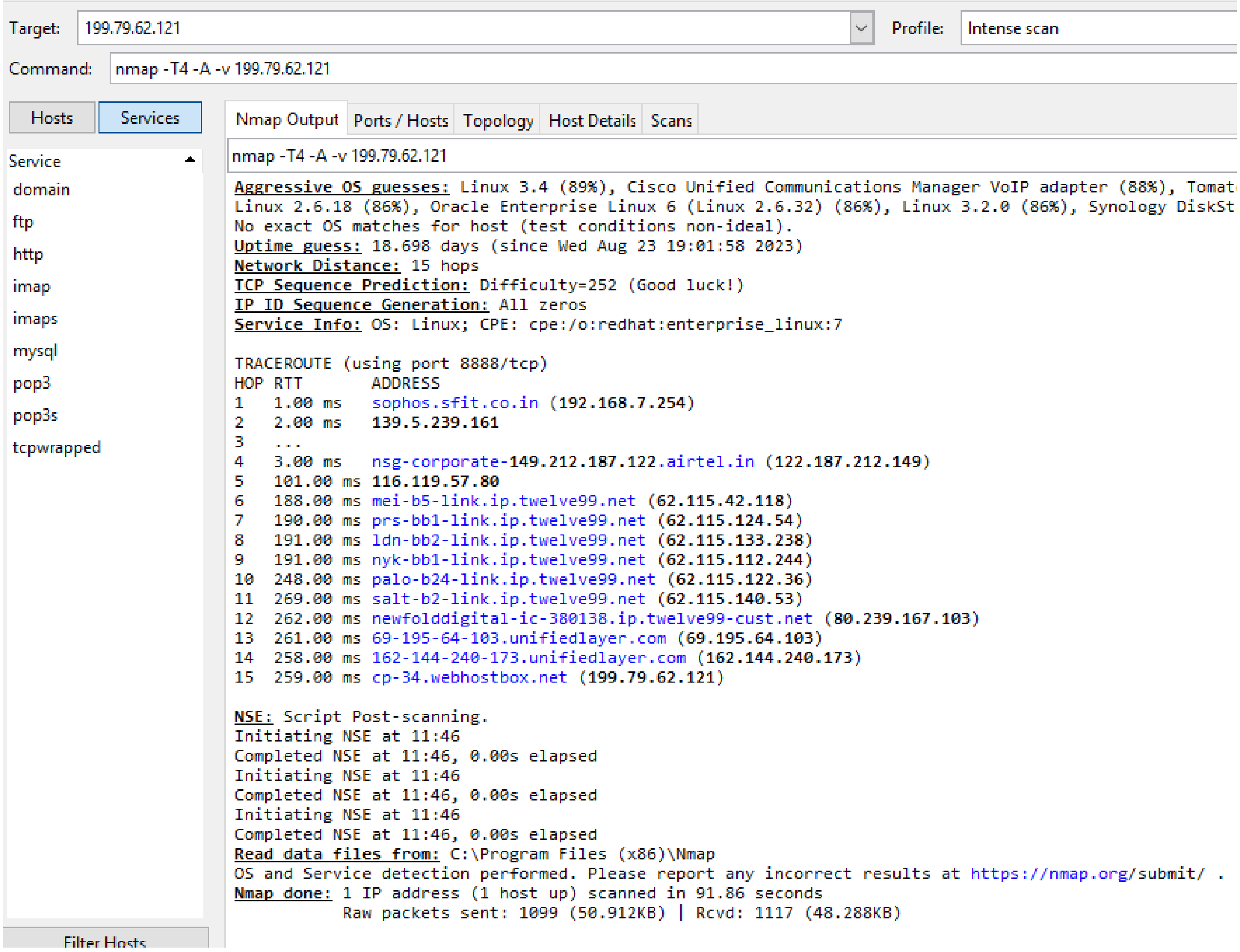
Target: 199.79.62.121
Profile: Quick scan
Command: nmap -T4 -F 199.79.62.121

```
Service
 domain
 ftp
 http
 https
 imap
 imaps
 mysql
 pop3
 pop3s
 rsftp
 smtp
 smtps
 submission
```

```
⊟ cp-34.webhostbox.net (199.79.62.121)
  ⊟ Host Status
     State:          up
     Open ports:     13
     Filtered ports: 0
     Closed ports:   87
     Scanned ports:  100
     Up time:        Not available
     Last boot:      Not available
  ⊟ Addresses
     IPv4:   199.79.62.121
     IPv6:   Not available
     MAC:    Not available
  ⊟ Hostnames
     Name - Type:   cp-34.webhostbox.net - PTR
  ⊞ Comments
```

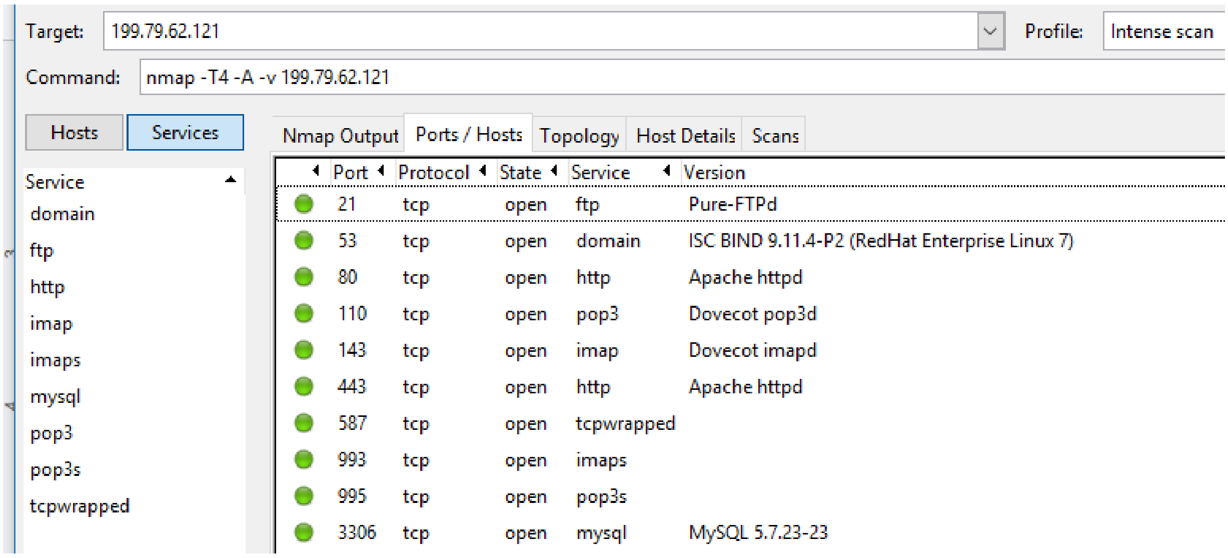
In the Screenshot above, we used Zenmap GUI to Scan the network with ping scan. In this we target the basic url provided by the Zenmap which is sfit.ac.in. In the host details section we observe that the state of the host is up which means the network is active right now and can see the ipv4 address with open ports, closed ports and scanned ports.

Scan: Intense Scan   &   Target: sfit.ac.in Or ip: 199.79.62.121



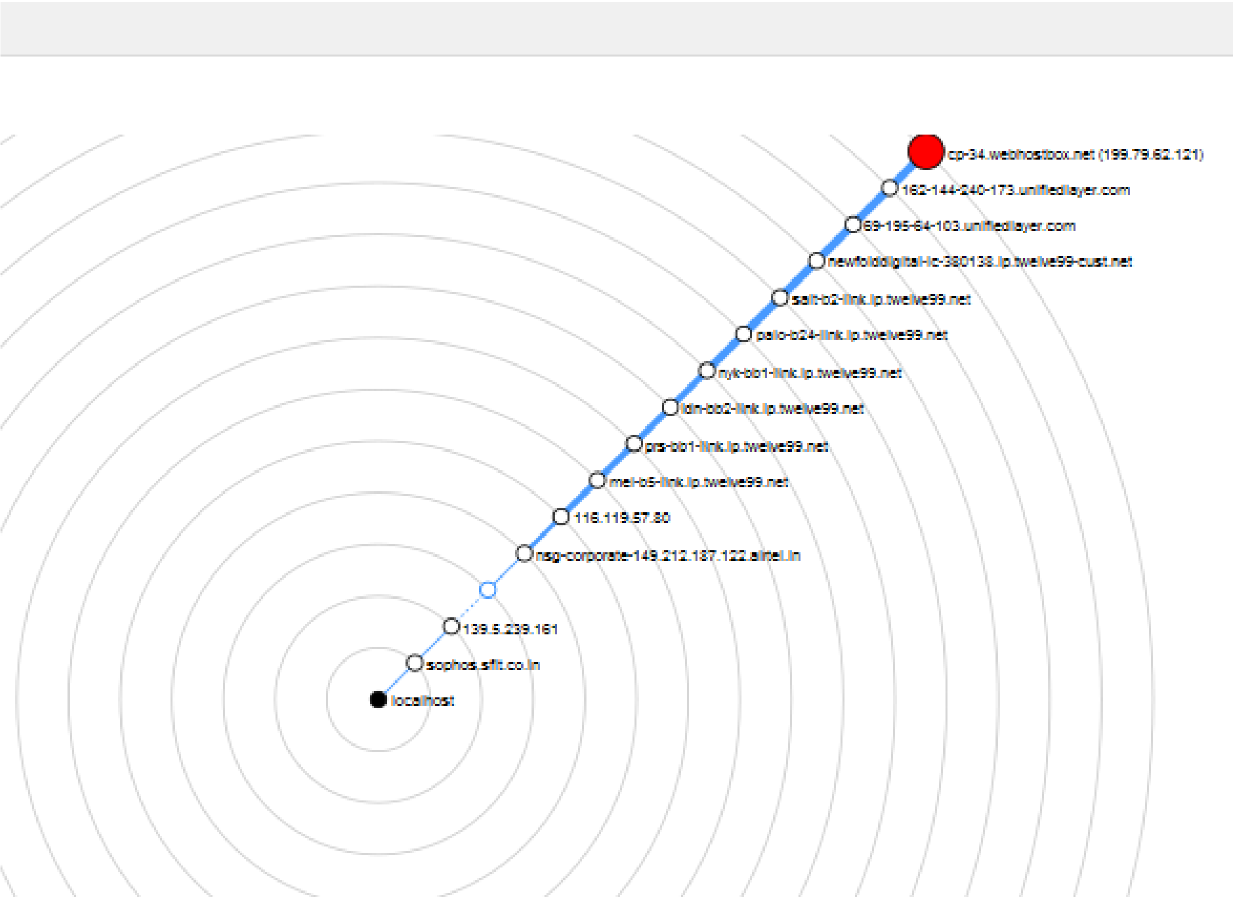
```
nmap -T4 -A -v 199.79.62.121
Aggressive OS guesses: Linux 3.4 (89%), Cisco Unified Communications Manager VoIP adapter (88%), Tomat
Linux 2.6.18 (86%), Oracle Enterprise Linux 6 (Linux 2.6.32) (86%), Linux 3.2.0 (86%), Synology DiskSt
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 18.698 days (since Wed Aug 23 19:01:58 2023)
Network Distance: 15 hops
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

TRACEROUTE (using port 8888/tcp)
HOP RTT       ADDRESS
1   1.00 ms   sophos.sfit.co.in (192.168.7.254)
2   2.00 ms   139.5.239.161
3   ...
4   3.00 ms   nsg-corporate-149.212.187.122.airtel.in (122.187.212.149)
5   101.00 ms 116.119.57.80
6   188.00 ms mei-b5-link.ip.twelve99.net (62.115.42.118)
7   190.00 ms prs-bb1-link.ip.twelve99.net (62.115.124.54)
8   191.00 ms ldn-bb2-link.ip.twelve99.net (62.115.133.238)
9   191.00 ms nyk-bb1-link.ip.twelve99.net (62.115.112.244)
10  248.00 ms palo-b24-link.ip.twelve99.net (62.115.122.36)
11  269.00 ms salt-b2-link.ip.twelve99.net (62.115.140.53)
12  262.00 ms newfolddigital-ic-380138.ip.twelve99-cust.net (80.239.167.103)
13  261.00 ms 69-195-64-103.unifiedlayer.com (69.195.64.103)
14  258.00 ms 162-144-240-173.unifiedlayer.com (162.144.240.173)
15  259.00 ms cp-34.webhostbox.net (199.79.62.121)

NSE: Script Post-scanning.
Initiating NSE at 11:46
Completed NSE at 11:46, 0.00s elapsed
Initiating NSE at 11:46
Completed NSE at 11:46, 0.00s elapsed
Initiating NSE at 11:46
Completed NSE at 11:46, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 91.86 seconds
           Raw packets sent: 1099 (50.912KB) | Rcvd: 1117 (48.288KB)
```

In the Screenshot above, we used Zenmap GUI to Scan the network with Intense scan. In this we target the basic url provided by the Zenmap which is sfit.ac.in. In this type of scan, it scans the vulnerable information in which a hacker can learn much more important things about the target which can be observed in the Nmap output.

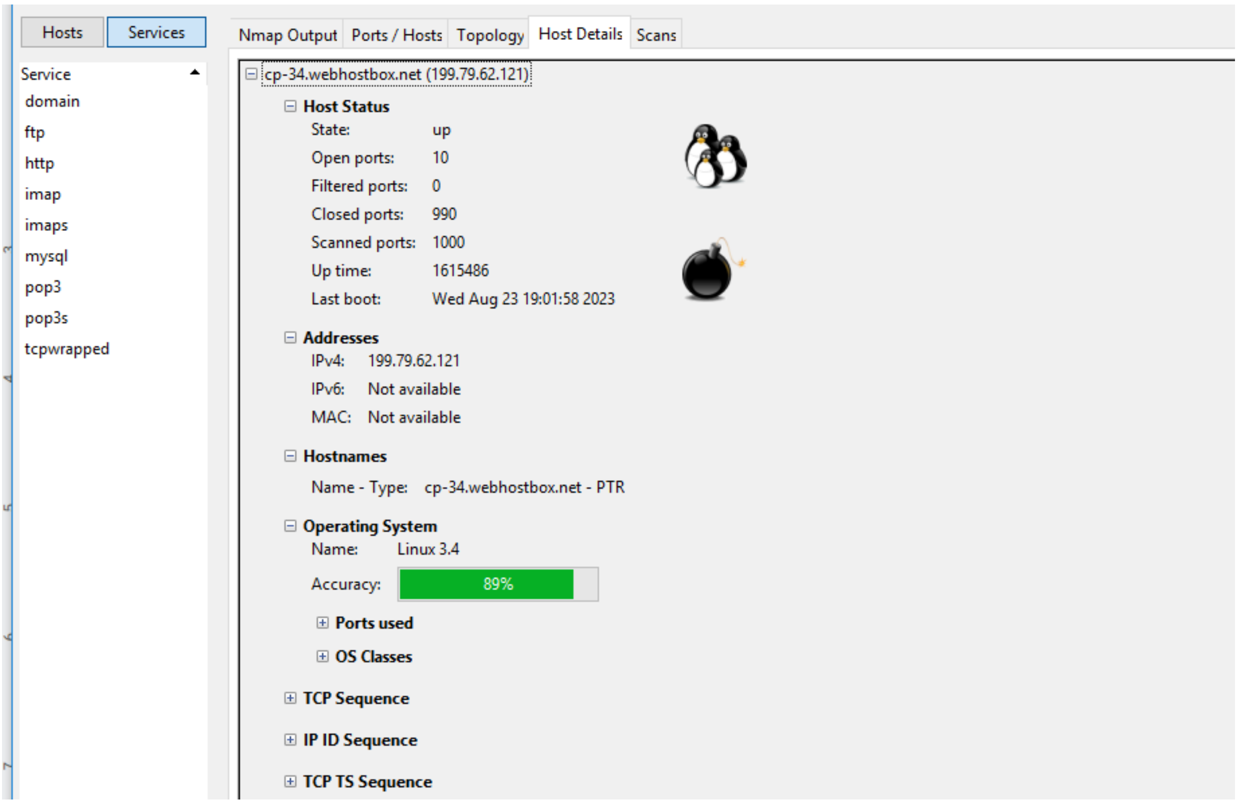


	Port	Protocol	State	Service	Version
●	21	tcp	open	ftp	Pure-FTPd
●	53	tcp	open	domain	ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
●	80	tcp	open	http	Apache httpd
●	110	tcp	open	pop3	Dovecot pop3d
●	143	tcp	open	imap	Dovecot imapd
●	443	tcp	open	http	Apache httpd
●	587	tcp	open	tcpwrapped	
●	993	tcp	open	imaps	
●	995	tcp	open	pop3s	
●	3306	tcp	open	mysql	MySQL 5.7.23-23

In the Screenshot above, we used Zenmap GUI to Scan the network with Intense scan. In this we target the basic url provided by the Zenmap which is sfit.ac.in. In the Ports/Hosts section we see multiple protocols with its respective port, state, Service and version.


cp-34.webhostbox.net (199.79.62.121)
162-144-240-173.unifiedlayer.com
69-195-64-103.unifiedlayer.com
newfolddigital-ic-380138.ip.twelve99-cust.net
salt-b2-link.ip.twelve99.net
palo-b24-link.ip.twelve99.net
nyk-bb1-link.ip.twelve99.net
ldn-bb2-link.ip.twelve99.net
prs-bb1-link.ip.twelve99.net
mei-b5-link.ip.twelve99.net
116.119.57.80
nsg-corporate-149.212.187.122.airtel.in
139.5.239.161
sophos.sfit.co.in
localhost

In the Screenshot above, we used Zenmap GUI to Scan the network with Intense scan. In this we target the basic url provided by the Zenmap which is sfit.ac.in. We observe the Topology which can show how complex it is. Shows us the entire connection of it from the starting to end.



cp-34.webhostbox.net (199.79.62.121)

Host Status

State: up
Open ports: 10
Filtered ports: 0
Closed ports: 990
Scanned ports: 1000
Up time: 1615486
Last boot: Wed Aug 23 19:01:58 2023

Addresses

IPv4: 199.79.62.121
IPv6: Not available
MAC: Not available

Hostnames

Name - Type: cp-34.webhostbox.net - PTR

Operating System

Name: Linux 3.4
Accuracy: 89%

⊞ **Ports used**
⊞ **OS Classes**

⊞ **TCP Sequence**
⊞ **IP ID Sequence**
⊞ **TCP TS Sequence**

In the Screenshot above, we used Zenmap GUI to Scan the network with Intense scan. In this we target the basic url provided by the Zenmap which is sfit.ac.in. It shows us the extra information compared to ping, quick scan like operating system name, accuracy, up time, and last boot.