**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, analyse 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.
   1. Ping scan
   2. Quick scan
   3. Intense scan

Choose following targets,

1. scanme.nmap.org
2. Public IP address of SFIT website
3. Observe following features of Zenmap,
   1. Host
   2. Services
   3. Nmap output, Ports/Hosts, Topology, Host Details, Scans
4. 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:**

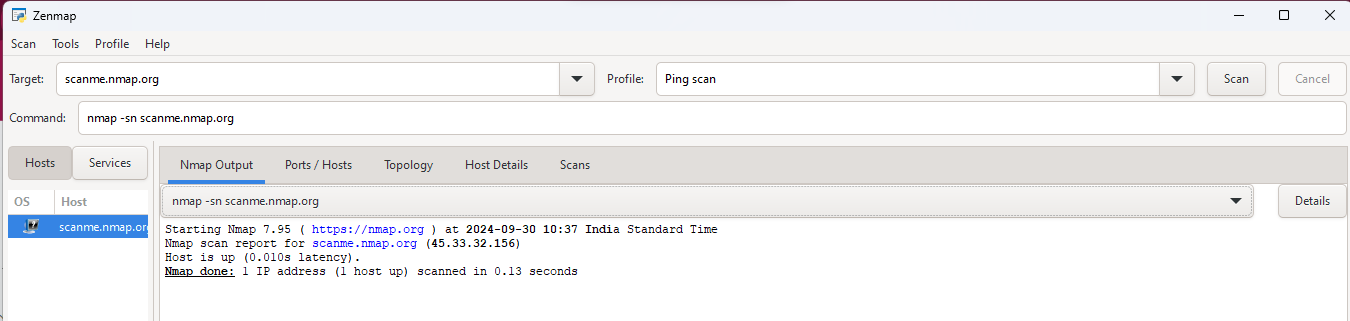
In this experiment Network mapping tool ‘Nmap’ was studied and different types of Nmap scans were used to gather host and network related information. We also learned that Nmap is an active reconnaissance tool which directly probes the target/victim for information gathering.

**References:** *(Mention your references here.)*

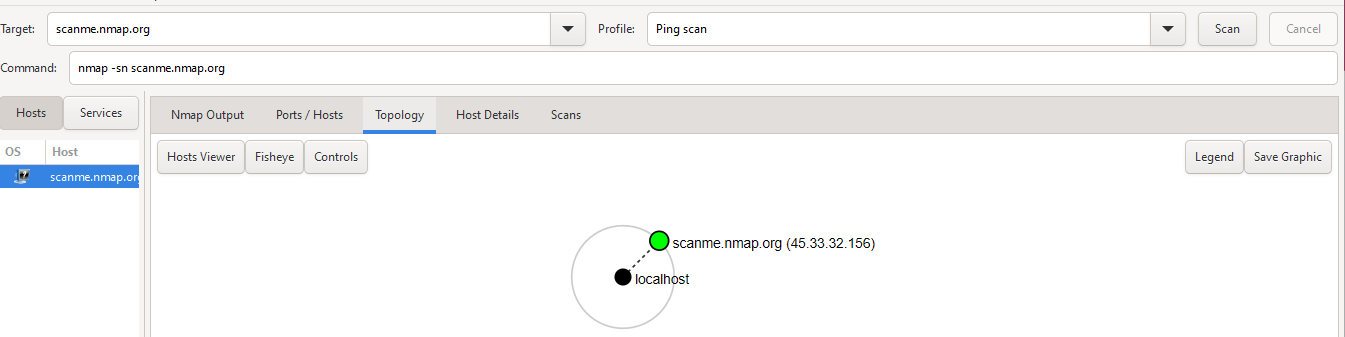
1. ‘Nmap official website’, <https://nmap.org/> *(Use for installation of Nmap)*
2. “Chapter 12. Zenmap GUI Users' Guide”, <https://nmap.org/book/zenmap.html>
3. <https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/>
4. https://www.kali.org/tools/nmap/

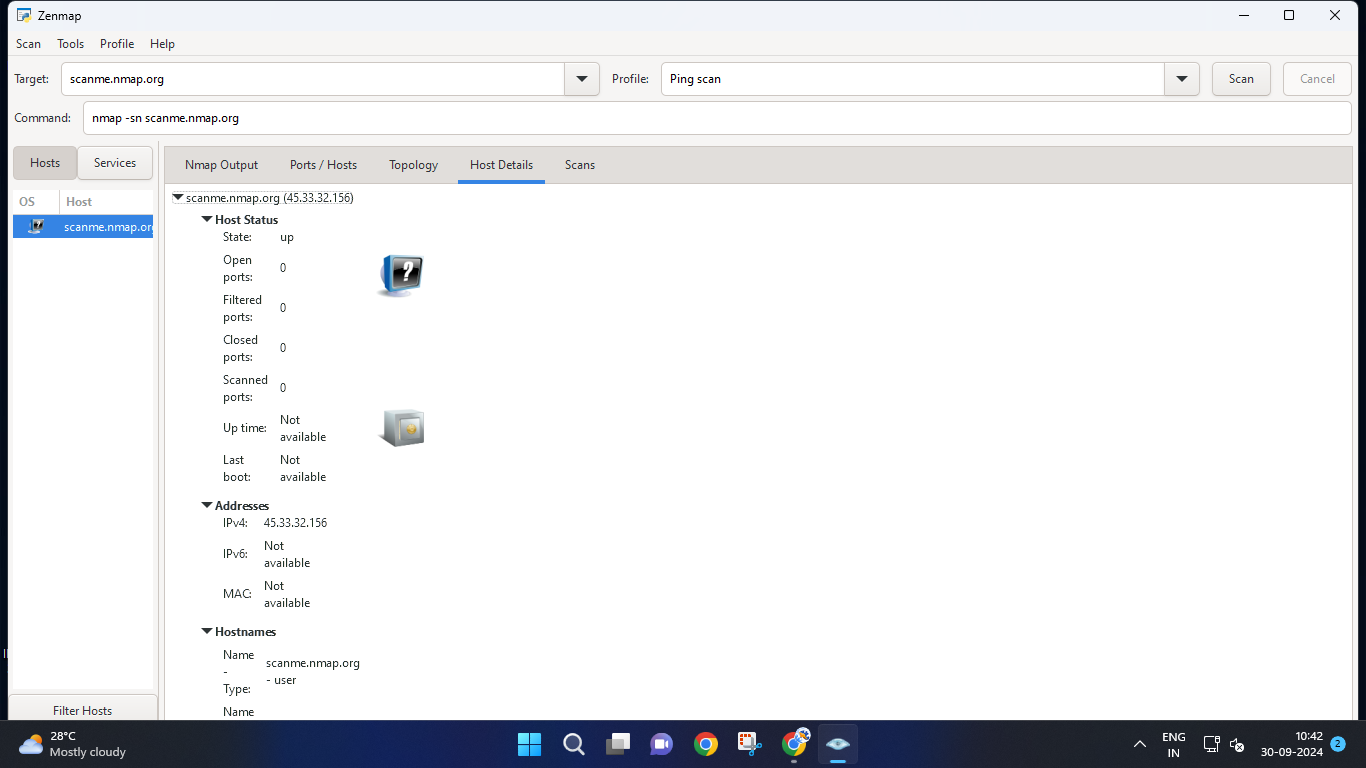
* **For scanme.nmap.org:**

-ping scan



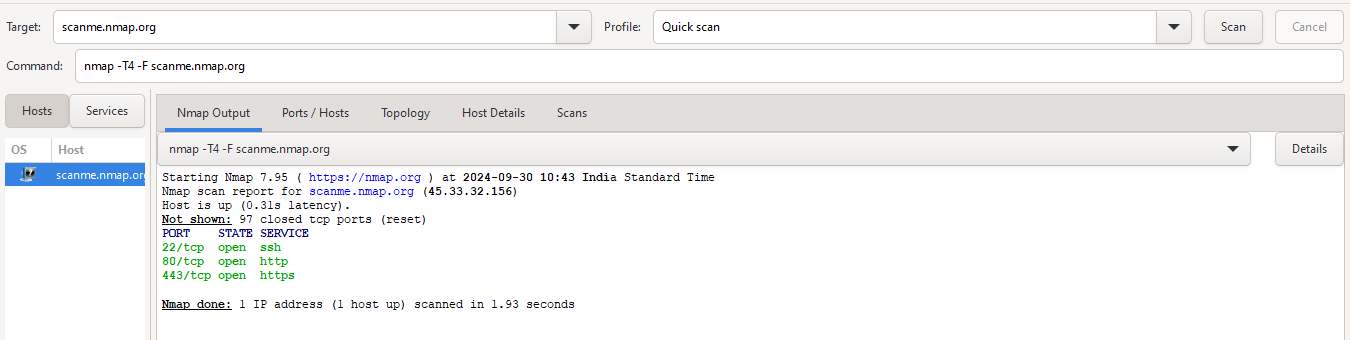
The Namp output section above for ping type of scan gives information only about of the number of host that at up without scanning for open ports.In case of scanme.nmap.org 1 host is up there.



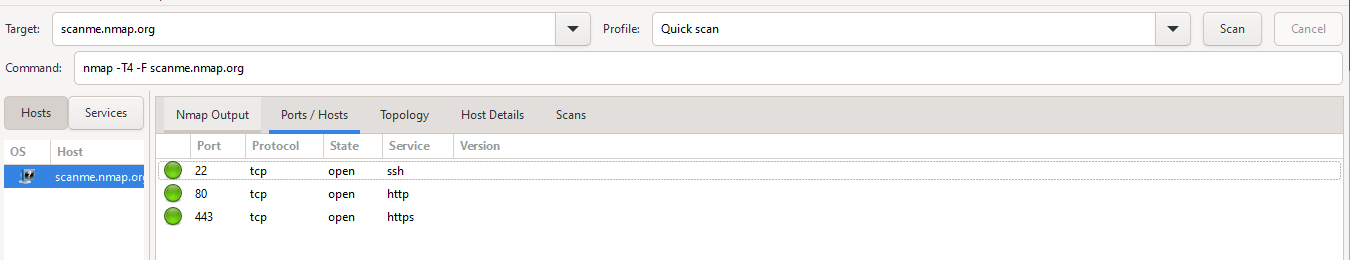
Each **host** (device) that responded to the ping scan is represented as a node in the topology..Here the target device(scanme.namp.org) is represented by green circle and local machine(localhost) by black circle.

The host details includes the information like status,addresses and names of the hosts.Here as the ping scan gives only number of hosts that are up that is displayed and since it dont scan for ports the port related information is nil.

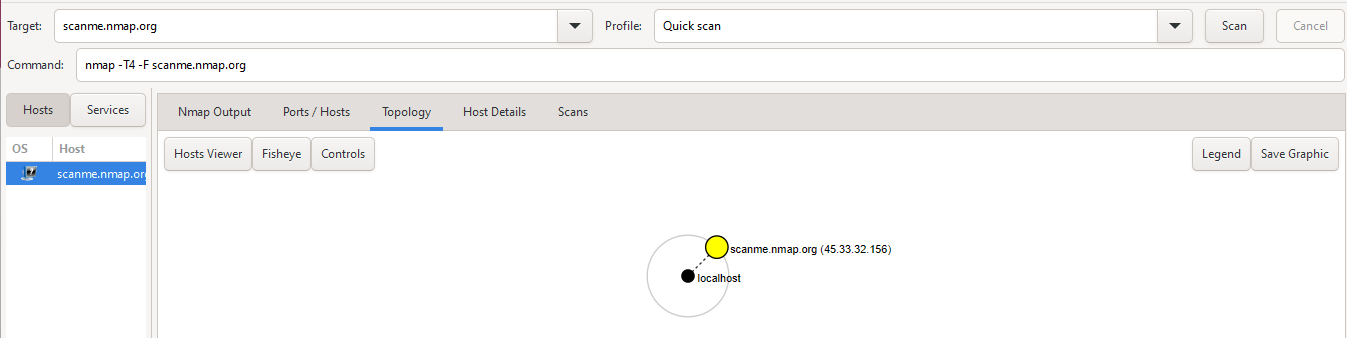
-quick scan



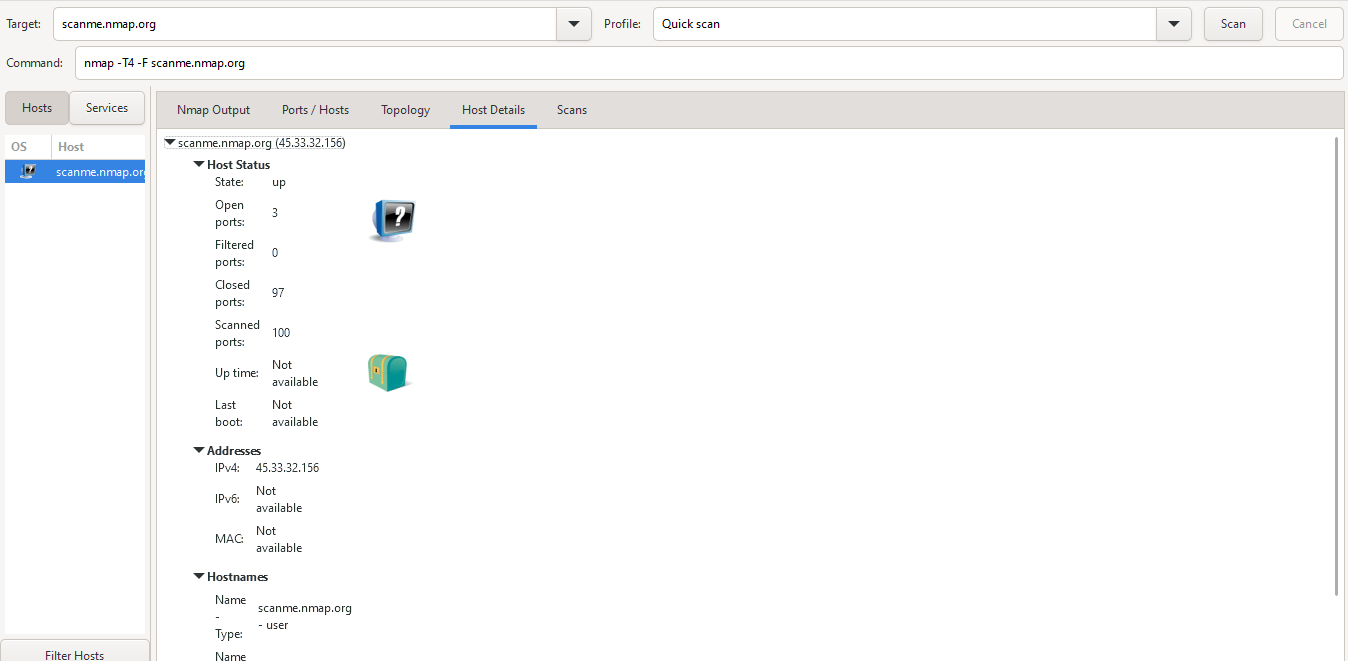
For the quick scan the information related to host as well as ports is available.The Nmap output above is showing that 1 host is up with 3 ports on ,which are 22/tcp for ssh,80/tcp for http and 443/tcp for https.



The ports/hosts section for quick scan is representing the ports with the protocol they are using also there state if open or closed and finally the services being used by these ports.Currently all the three ports are open.

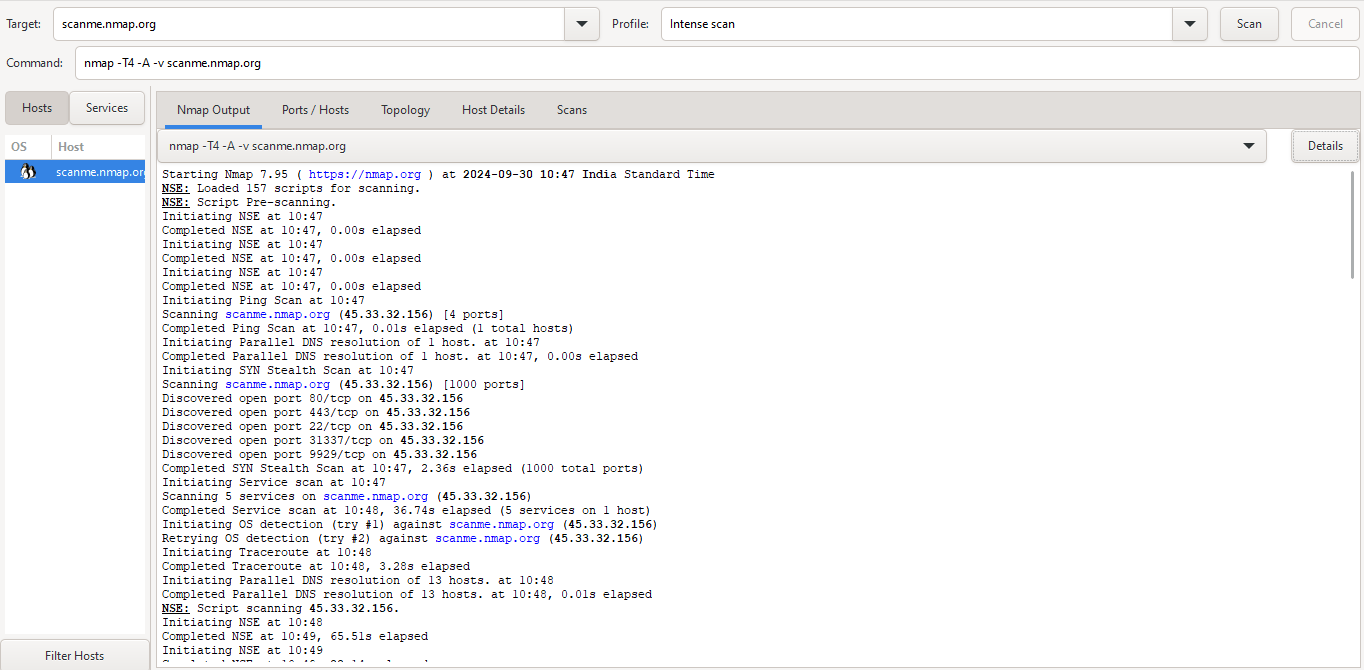


The topology section is just showing the target with a yellow circle and the local machine with a black circle.

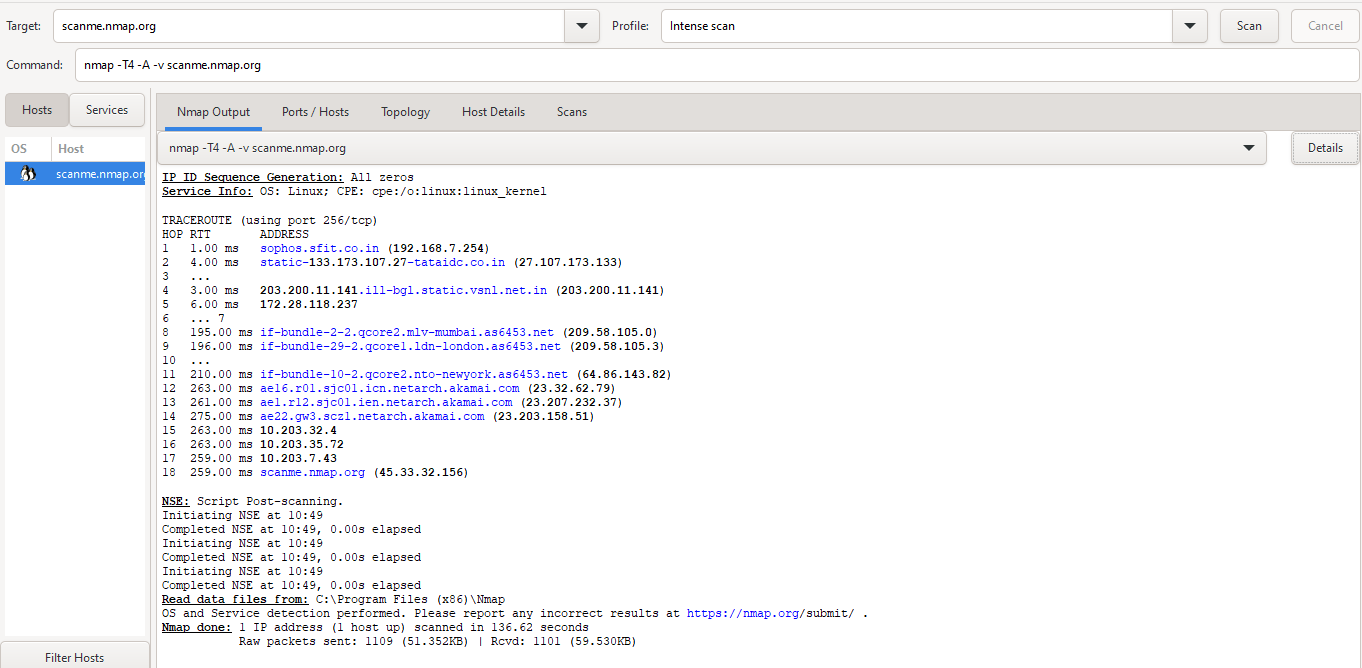


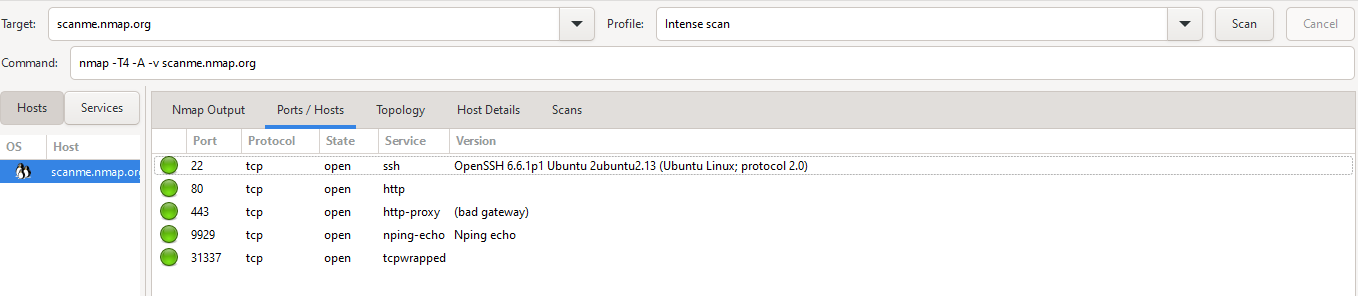
The host details section for quick scan is showing above ports related info along with the host status ,i.e open ports as 3,scanned ports 100,the IPv4 address of the target as 45.33.32.156 and closed ports as 97.

~Intense scan

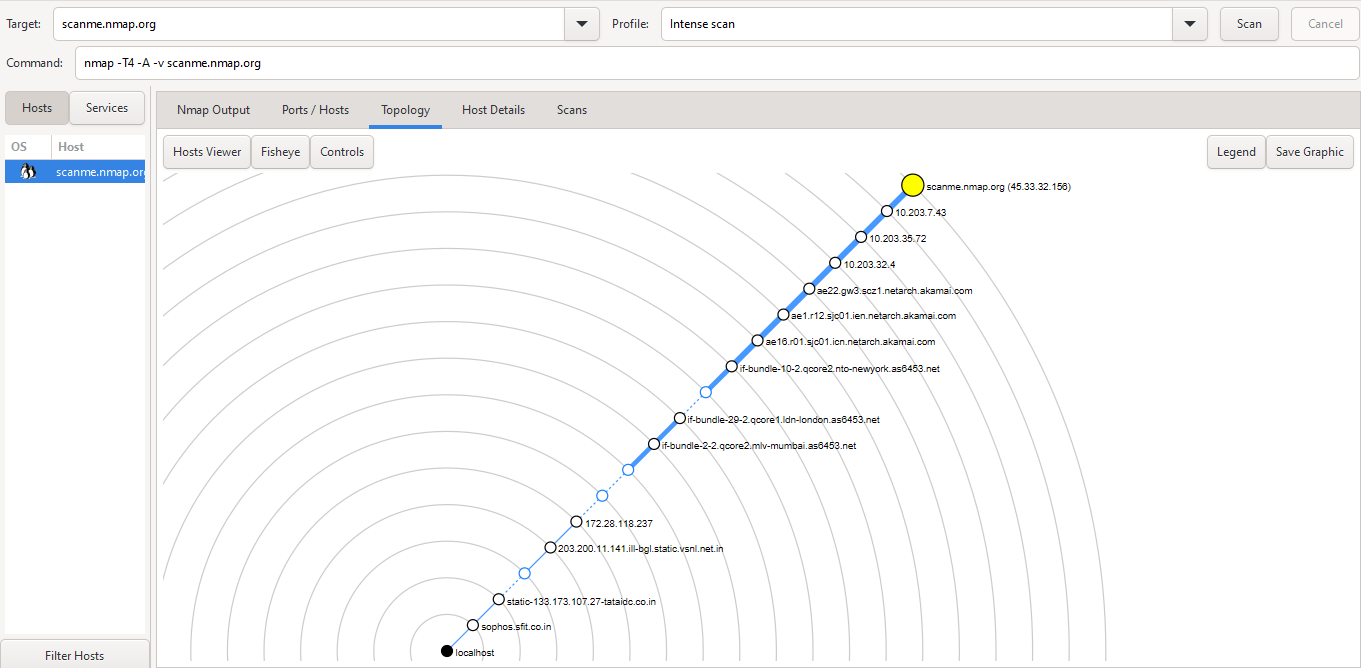


**….**

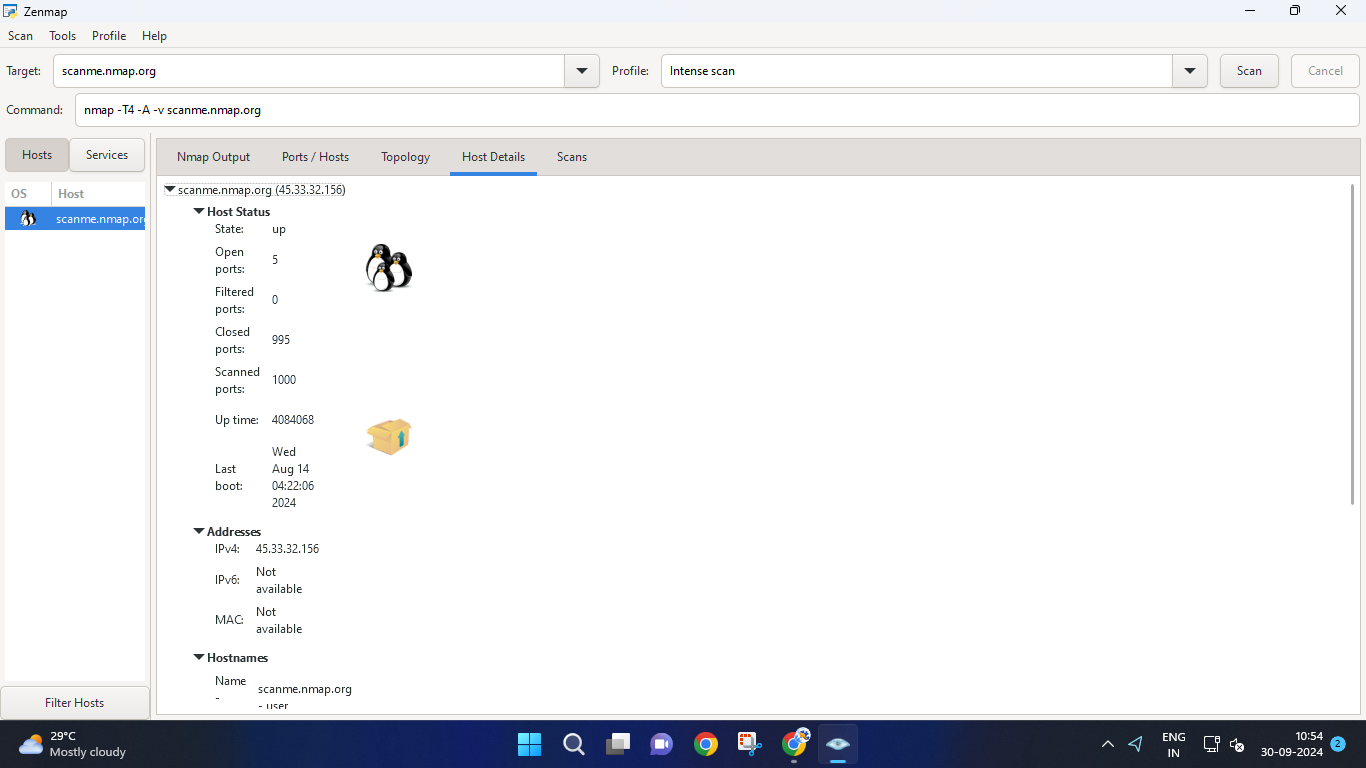


The above screenshot shows that for intense type of scan there are 157 scripts for scanning and at the end of this scan its is sequencing IP IDs that are generated and the Nmap done message says 1 IP address found.

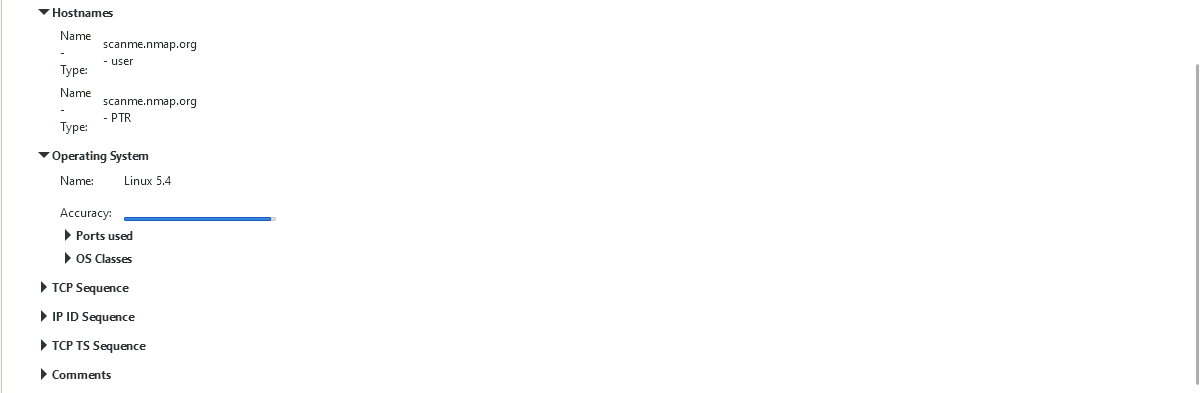
The ports/hosts section is showing the ports 22,80,443,9929 & 31337 are open for ssh, http, http-proxy ,nping-echo and tcpwrapped services respectively.



The above screenshot of intense scan for topology section shows all the hops performed before reaching to the target in detail along with there IP addresses.

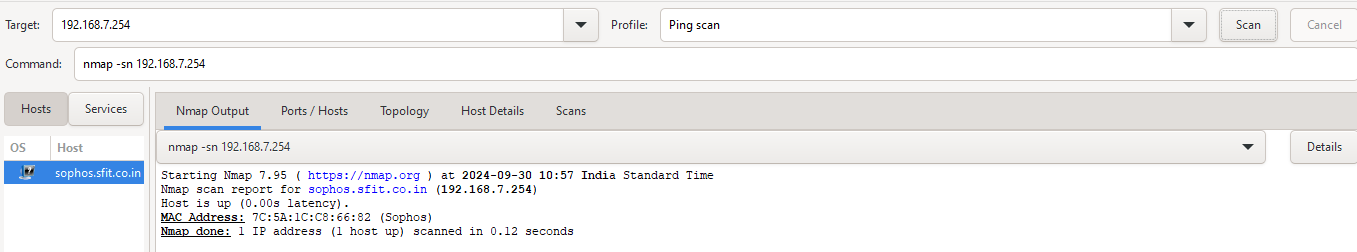


The screenshot of host details section for intense scan is showing 5 open ports ,995 closed and 1000 scanned ports.The IPv4 address of the target being 45.33.32.156.The host are scanme.nmap.org one with user and one with PTR type of user.The operating system used is Linux 5.4 with maximum accuracy.

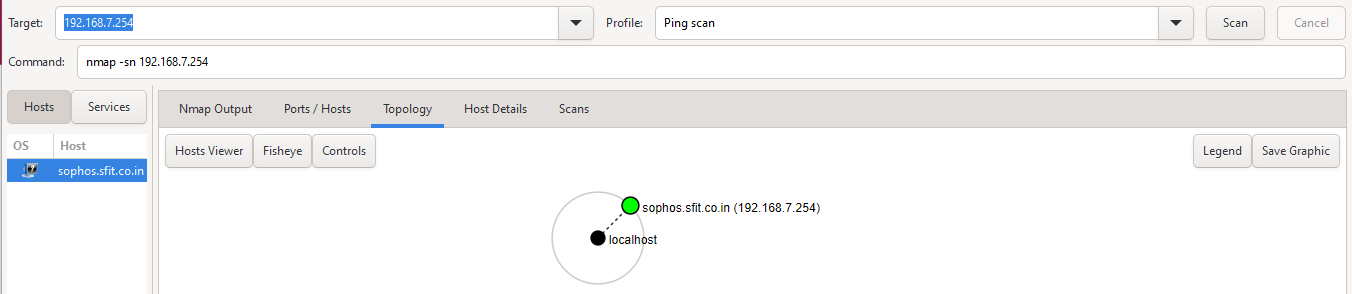


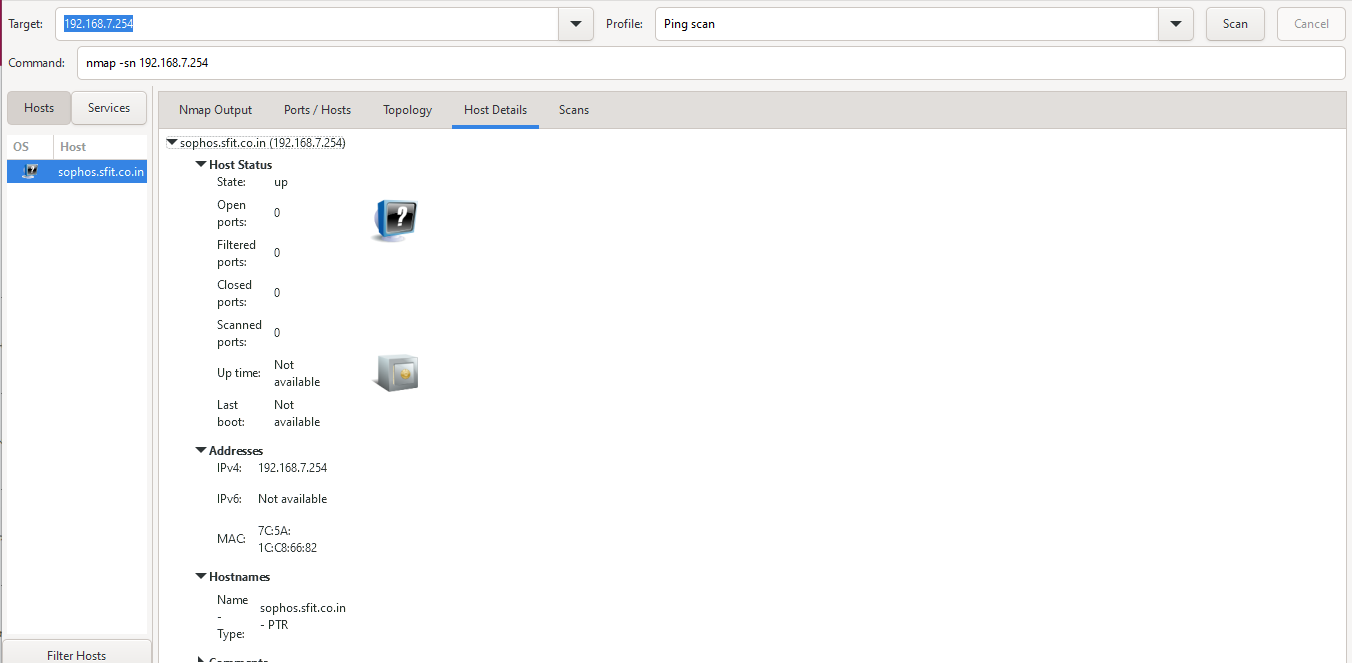
* **For sfit.ac.in(192.168.7.254)**

~ping scan



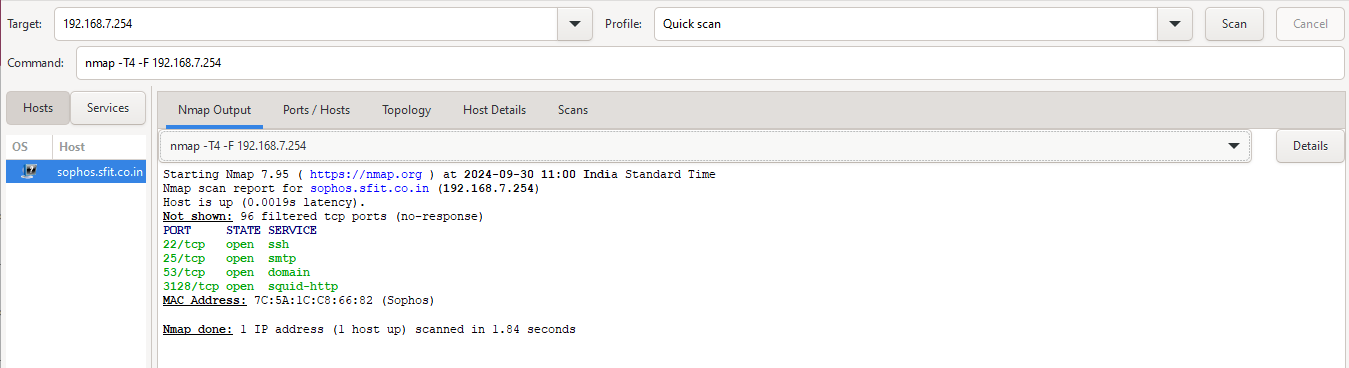
The Namp output section above for ping type of scan gives information only about of the number of host that at up without scanning for open ports.In case of scanme.nmap.org 1 host is up there.



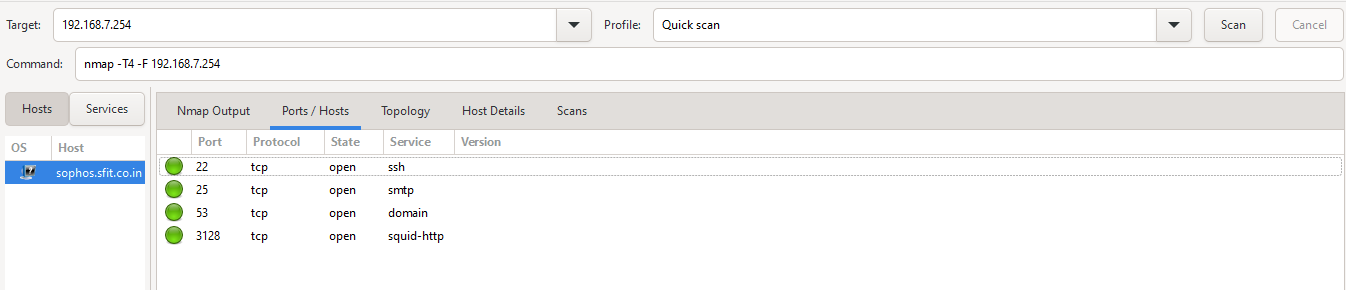
Each **host** (device) that responded to the ping scan is represented as a node in the topology..Here the target device(sophos.sfit.co.in) is represented by green circle and local machine(localhost) by black circle.

The host details includes the information like status,addresses and names of the hosts.Here as the ping scan gives only number of hosts that are up that is displayed and since it dont scan for ports the port related information is nil.

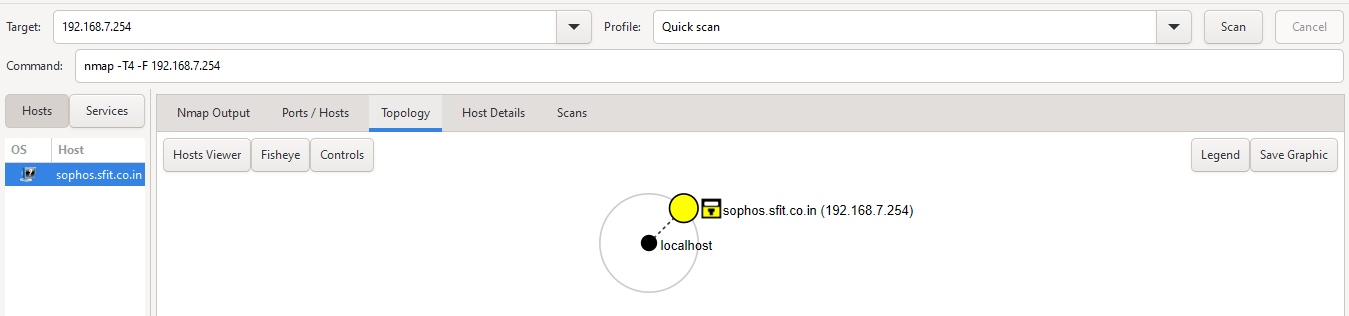
~quick scan

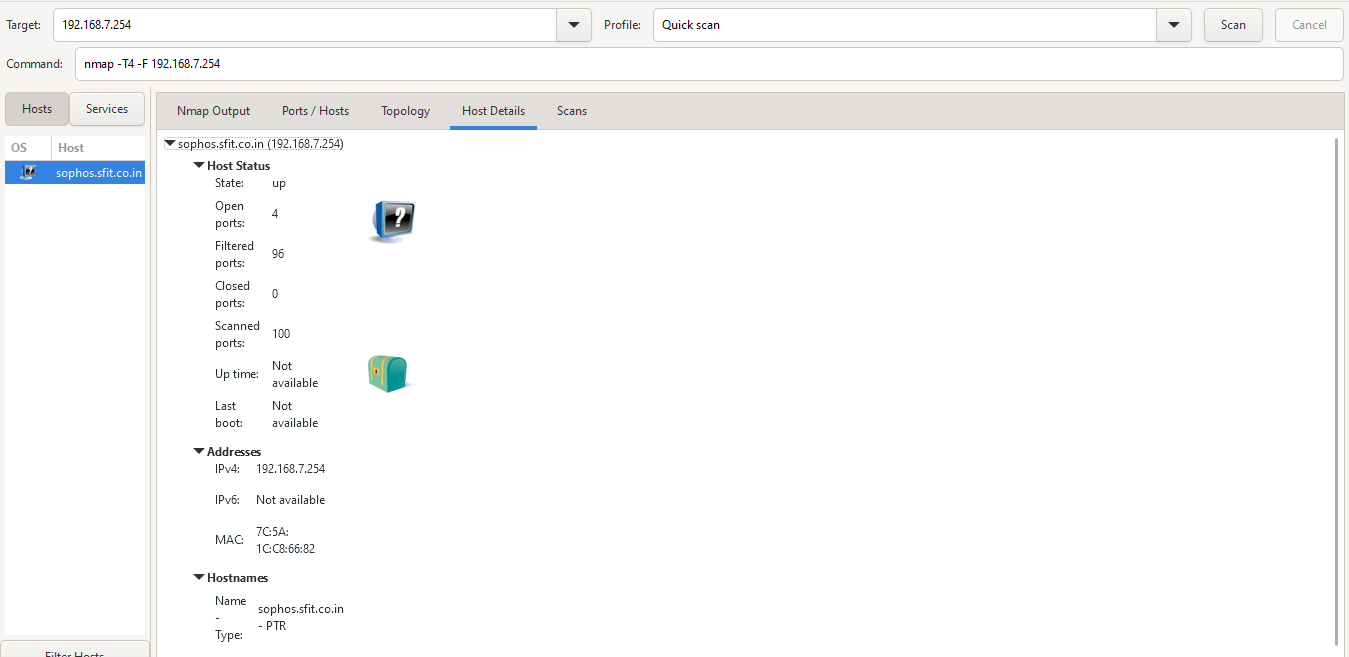


For the quick scan the information related to host as well as ports is available.The Nmap output above is showing that 1 host is up with 3 ports on ,which are 22/tcp for ssh,25/tcp for smtp ,53/tcp for domain and 3128/tcp for squid-http.



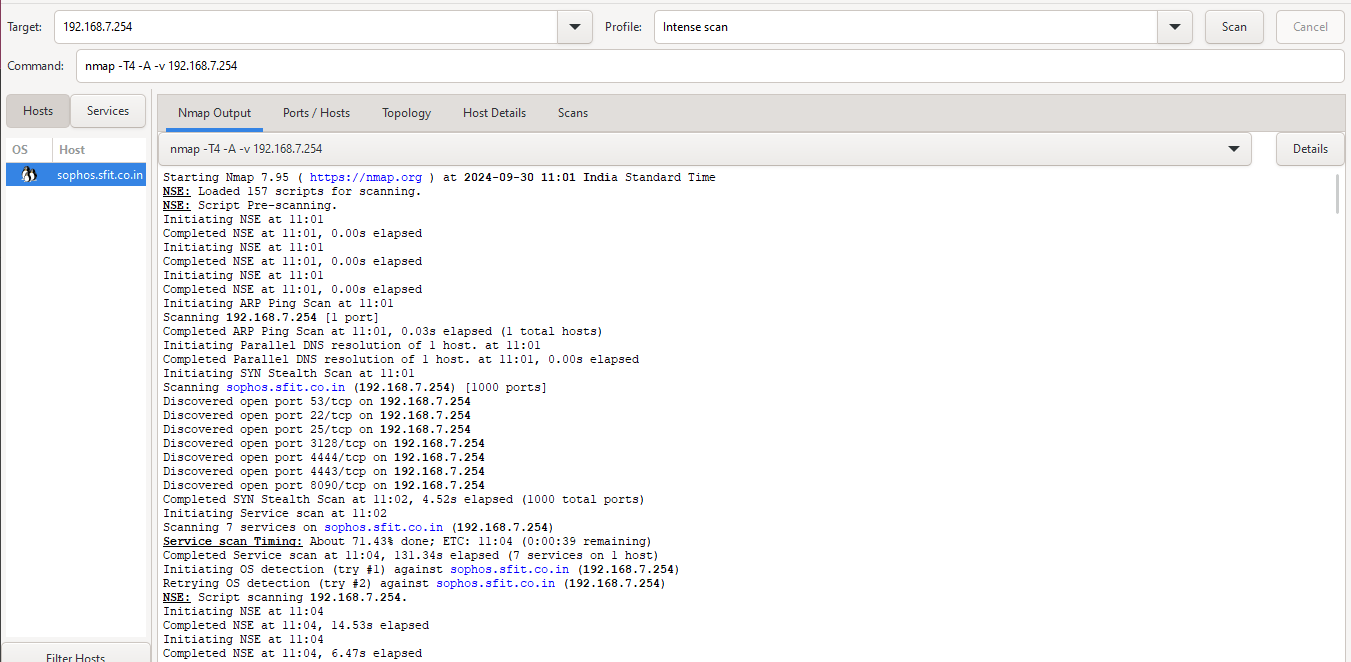
The ports/hosts section for quick scan is representing the ports with the protocol they are using also there state if open or closed and finally the services being used by these ports.Currently all the four ports are open.



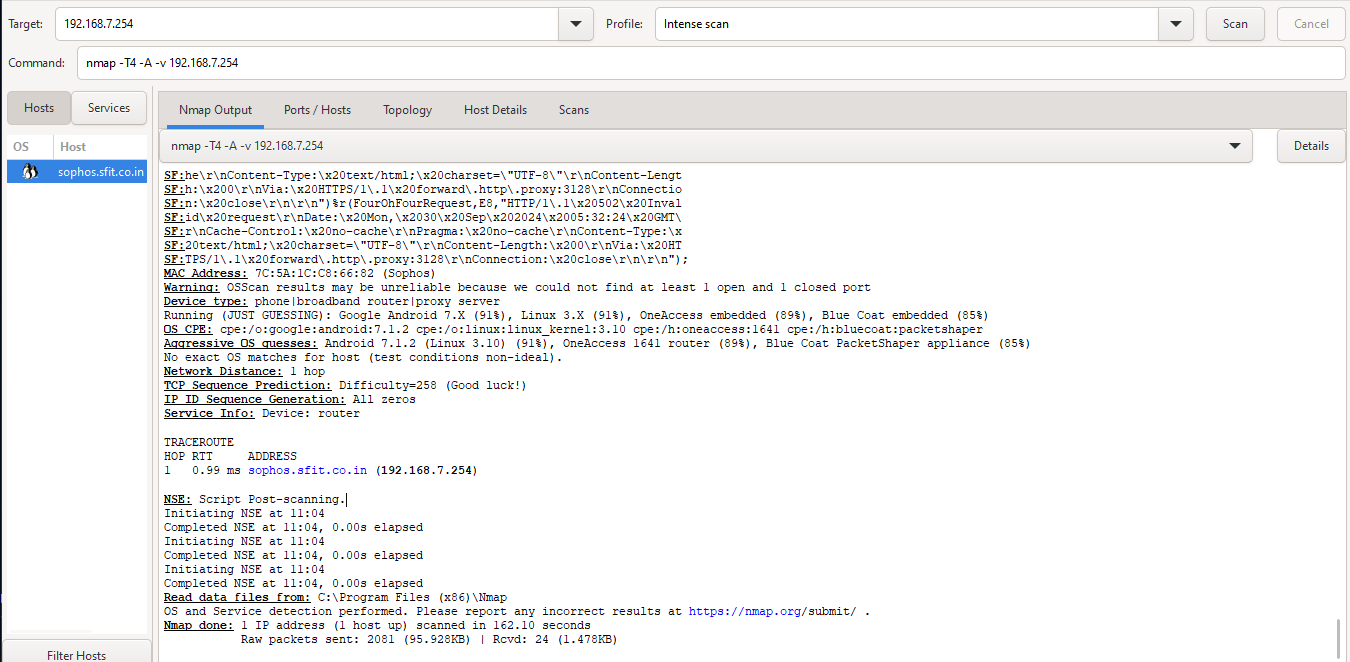
The topology section is just showing the target(sophos.sfit.co.in(192.168.7.254)) with a yellow circle and the local machine with a black circle.

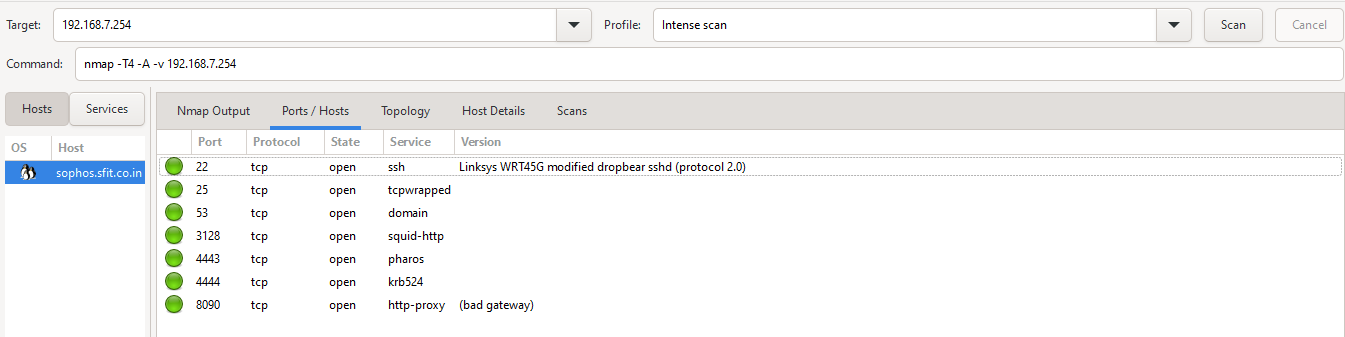
The host details section for quick scan is showing above ports related info along with the host status ,i.e open ports as 4,scanned ports 100,the IPv4 address of the target as 192.168.7.254 and closed ports as 0.

~Intense scan

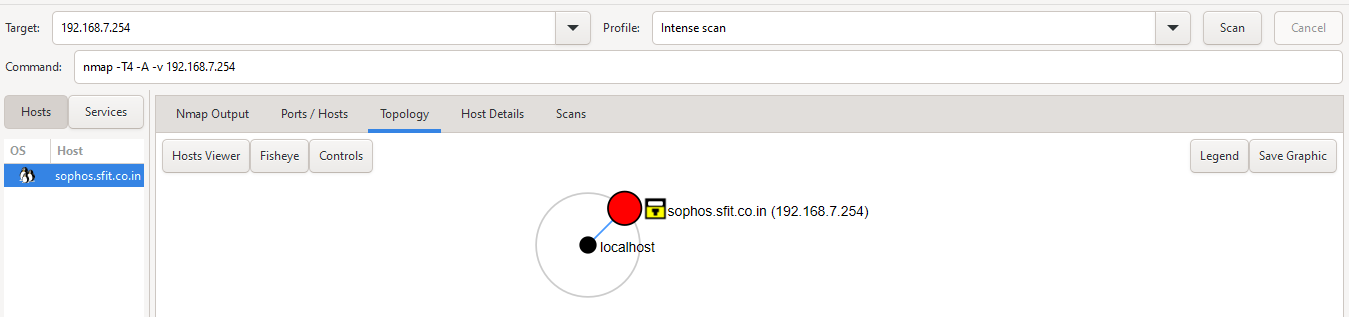


**…**

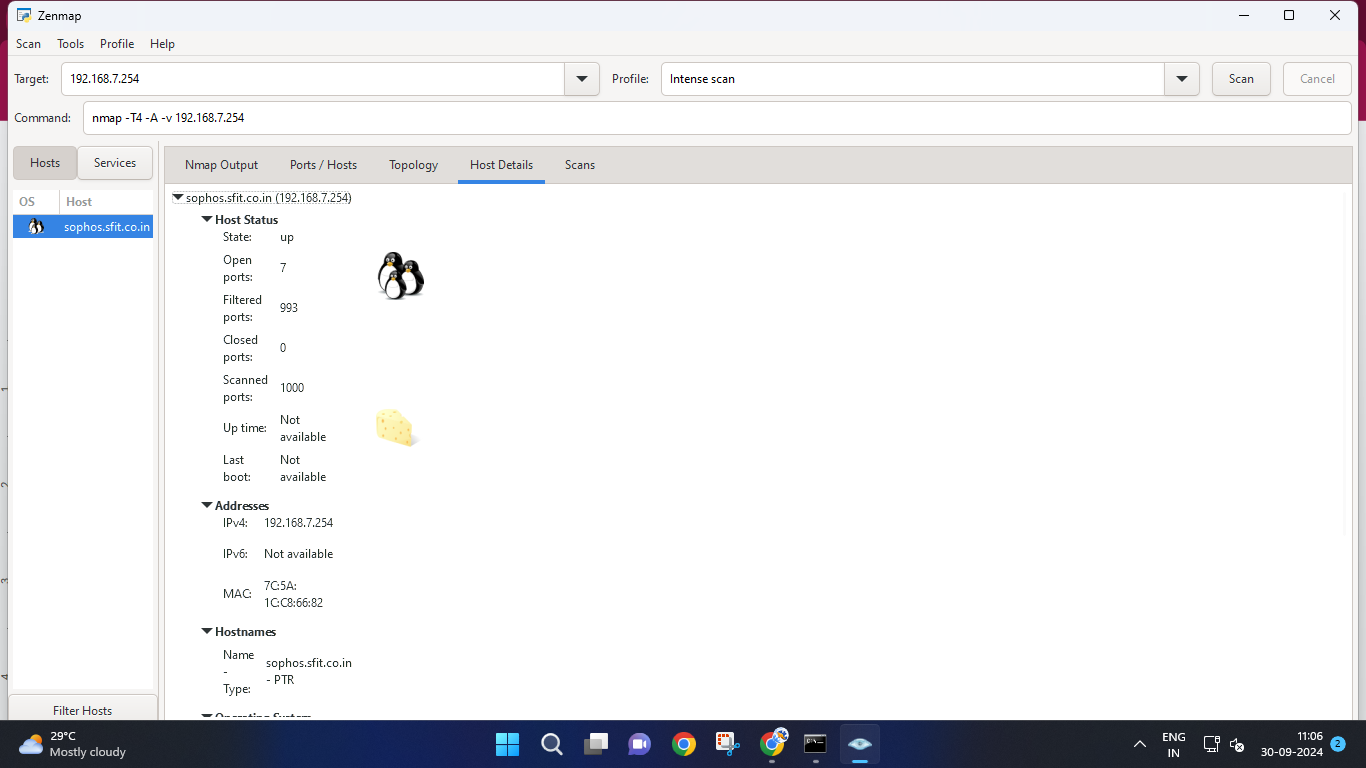


The above screenshot shows that for intense type of scan there are 157 scripts for scanning and at the end of this scan its is sequencing IP IDs that are generated and the Nmap done message says 1 IP address found.

The ports/hosts section is showing the ports 22,25,53,3128,4443,4444,8090 are open for ssh, tcpwrapped, domain ,squid-http,pharos,krb524 and http-proxy services respectively.



The above screenshot of intense scan for topology section shows all the hops performed before reaching to the target in detail along with there IP addresses. Here there are only two hops as we are accessing the college’s server through college’s PC.



The screenshot of host details section for intense scan is showing 7 open ports ,993 closed and 1000 scanned ports.The IPv4 address of the target being 192.168.5.254.The host is scanme.nmap.org with PTR type of user.The operating system used is Android 7.1.2(Linux 3.10) with maximum accuracy.

