**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.

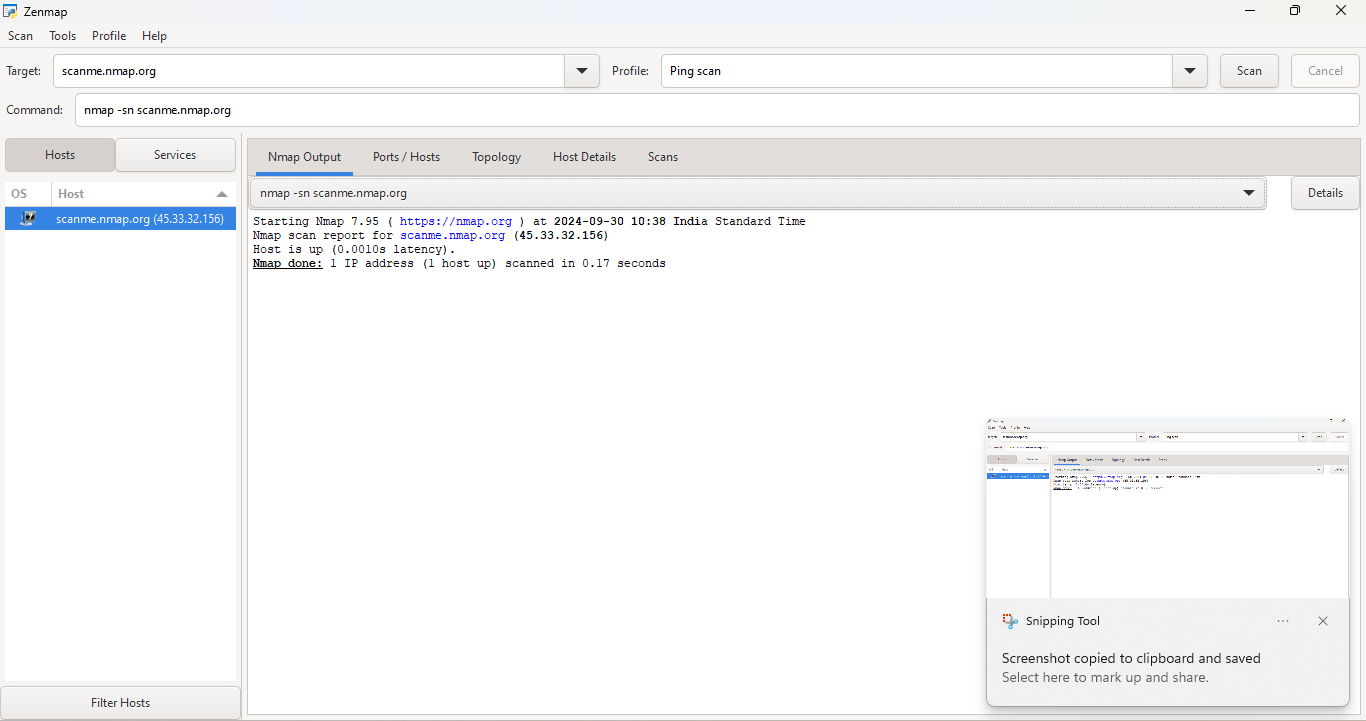
**References:** *(Mention your references here.)*

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.nitttrchd.ac.in/imee/Labmanuals/ZENMAP%20and%20HONEYBOT%20Manual.pdf>
4. <https://docs.oracle.com/cd/E86824_01/html/E54763/zenmap-1.html>
5. <https://www.geeksforgeeks.org/port-scan-in-ethical-hacking/>
6. **scanme.nmap.org:**

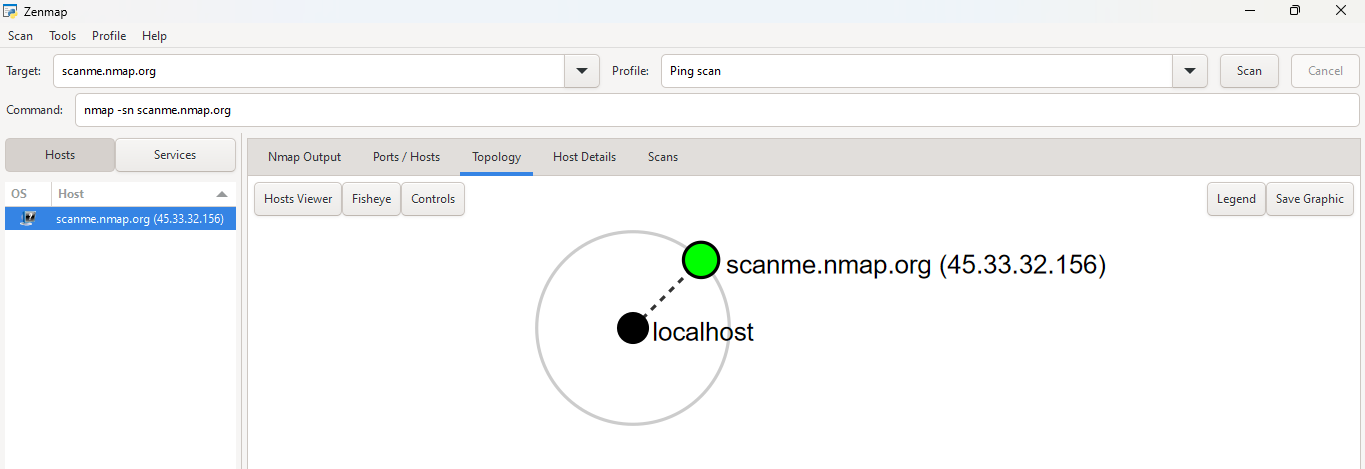
**PING SCAN**

In ping mode, Nmap can be used to check the reachability of scanme.nmap.org by sending ICMP echo requests, typically through the command nmap -sn scanme.nmap.org. This method determines whether the host is active on the network without conducting a full port scan, providing a quick assessment of its responsiveness.

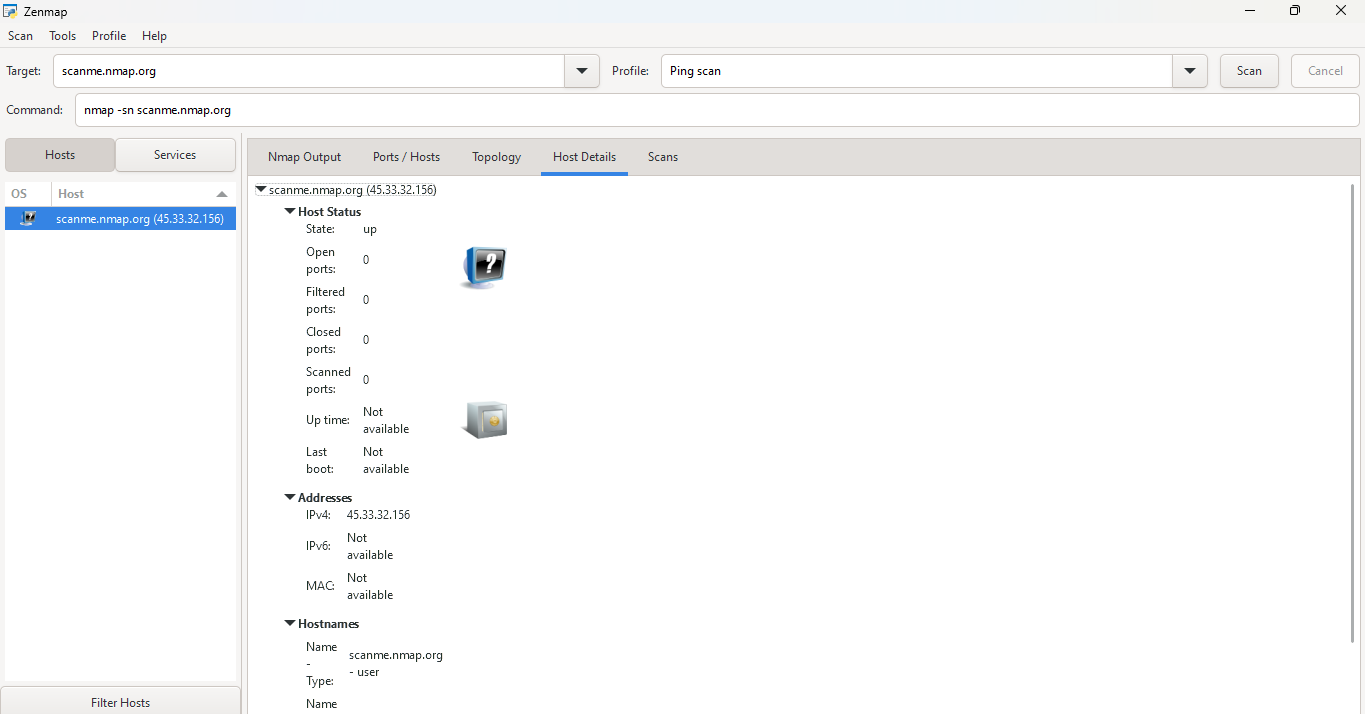
* **NMAP OUTPUT:** The output from Nmap during a ping scan is straightforward, typically showing the host's status (up or down) along with its IP address. When more comprehensive scans are executed, the output expands to include information on open ports, running services, and any vulnerabilities associated with those services.



* **NMAP TOPOLOGY**: Topology refers to the arrangement and connection of network devices. While a basic ping scan doesn't delve into topology details, advanced Nmap scans can illustrate how scanme.nmap.org connects with other devices, revealing the path taken by packets and the intermediate hops involved.



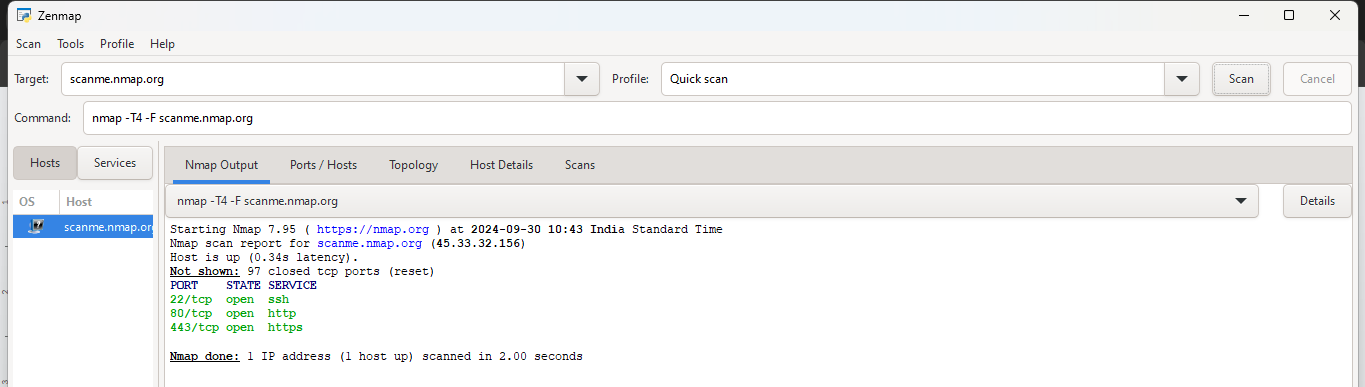
* **HOST DETAILS:** Host details encompass various attributes of the target system, such as hostname, IP address, and operating system. After performing a ping scan, additional queries can provide insights into the OS and the version of services running on scanme.nmap.org, aiding in vulnerability assessments and network profiling.



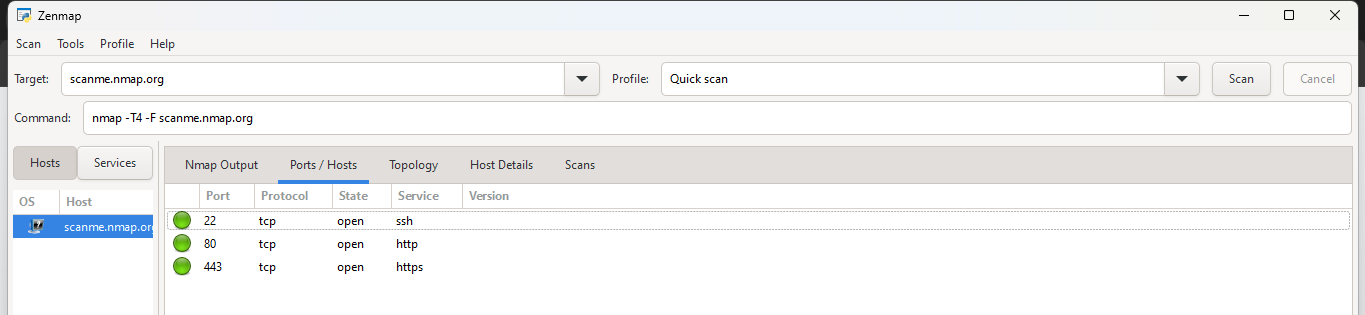
**QUICK SCAN:**

In quick scan mode, Nmap efficiently determines the status and open ports of scanme.nmap.org using the command. This mode prioritizes speed while providing a concise overview of the target, combining ping scans and port scanning in a single operation.

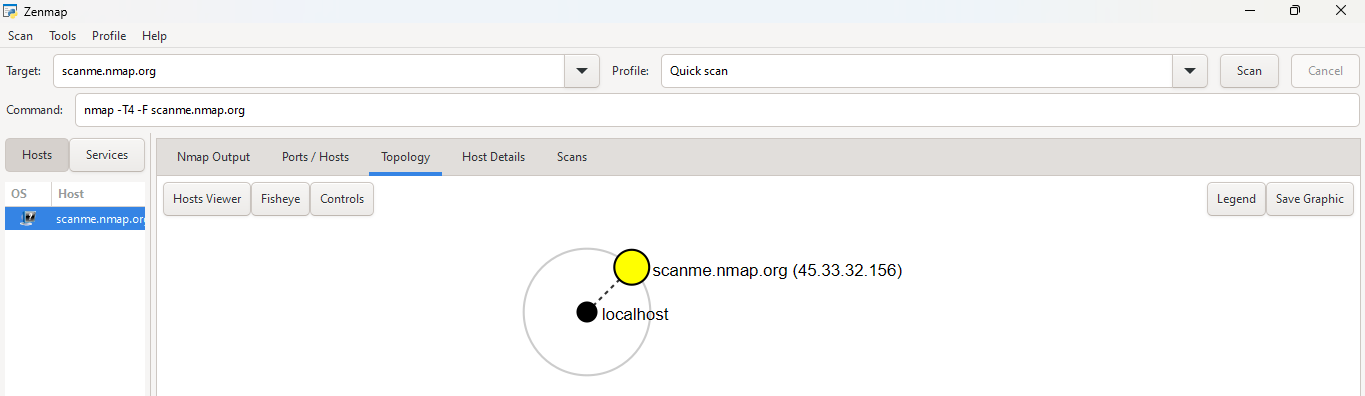
* **NMAP OUTPUT:** The output from a quick scan is straightforward, typically listing the status of the host alongside the open ports and their associated services. For scanme.nmap.org, this output provides a rapid assessment of the target's network configuration.



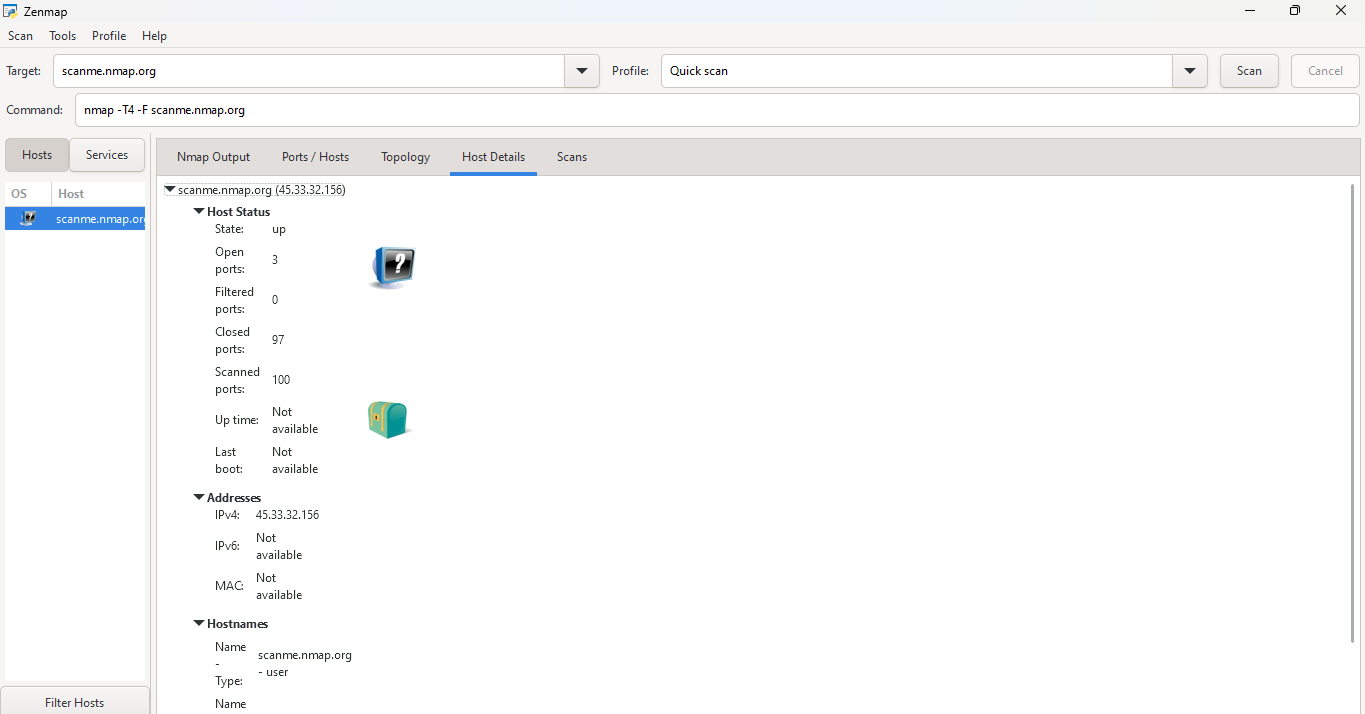
* **PORTS/HOSTS:** The port/hosts section in quick scan mode reveals which ports on scanme.nmap.org are open. It generally focuses on the most commonly used ports, offering insights into the services that might be running and their potential vulnerabilities.



* **TOPOLOGY:** While quick scans do not deeply explore network topology, they can provide basic information about how scanme.nmap.org interacts with the network. More advanced scans would be necessary to illustrate the connections and paths taken by packets to reach the host.

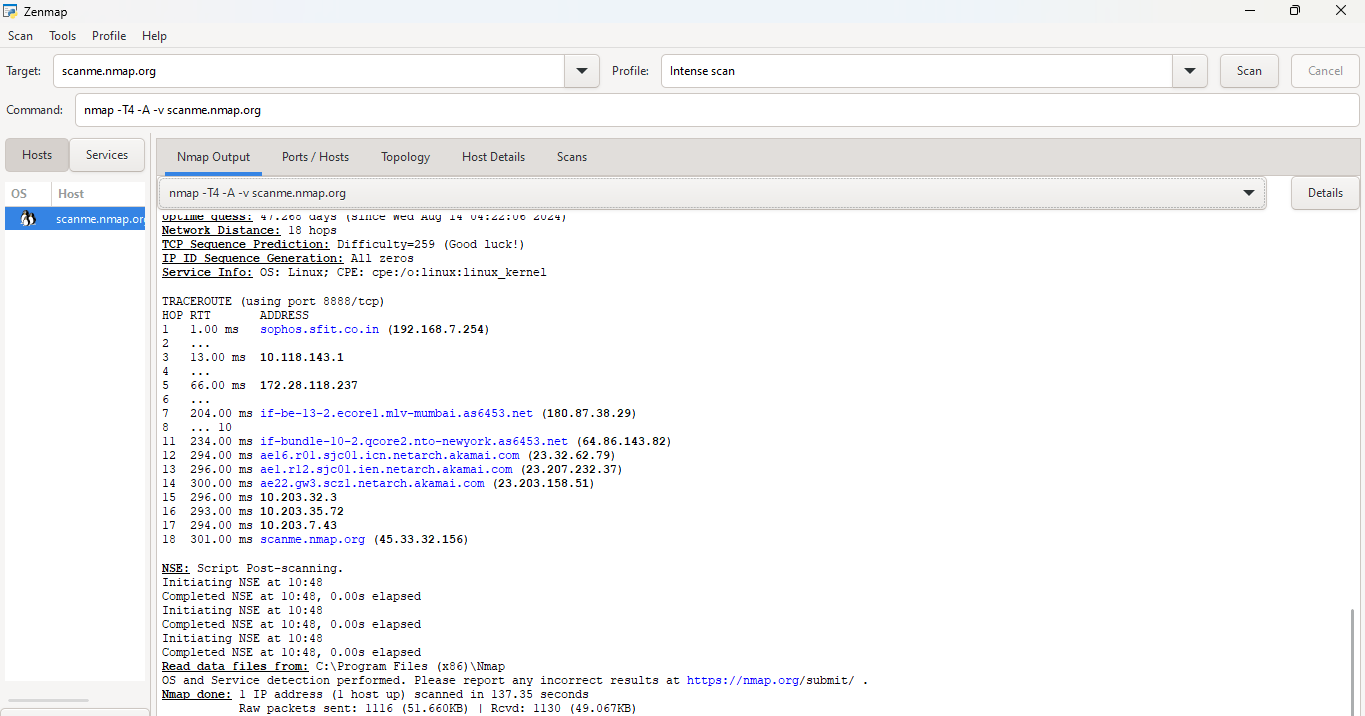
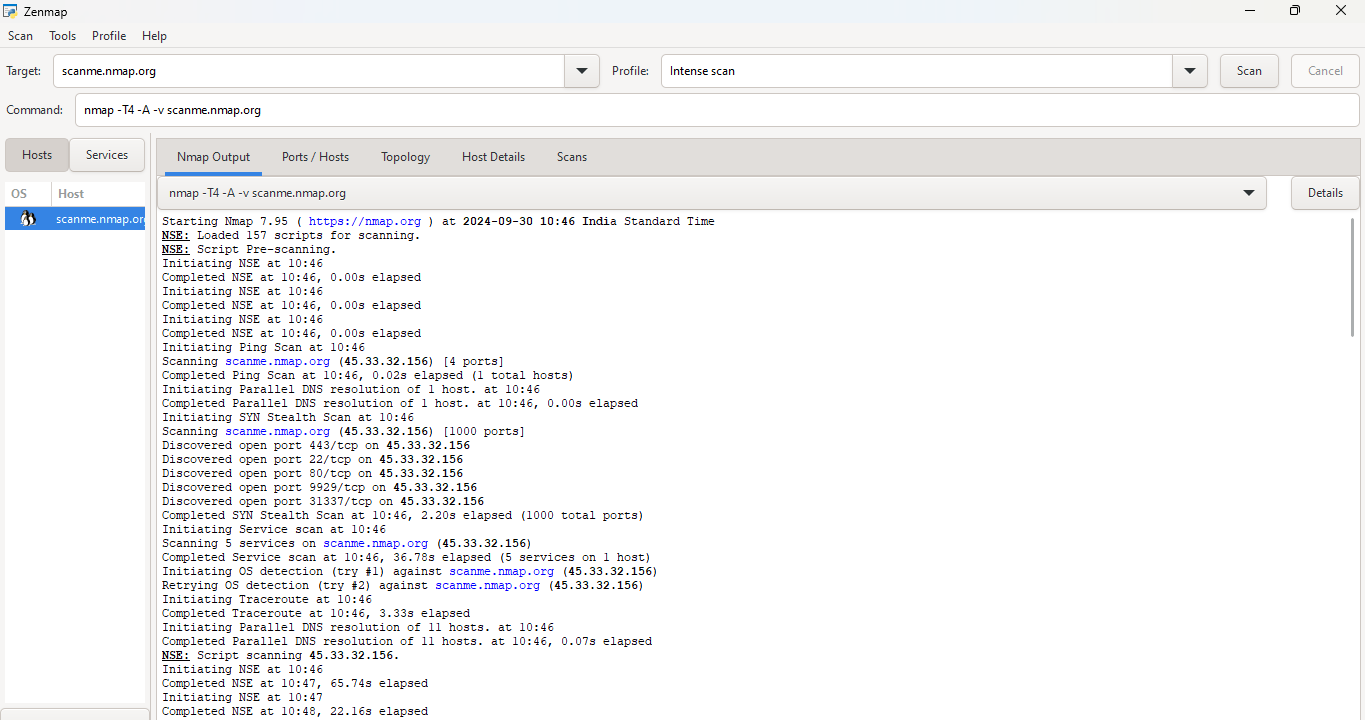


* **HOST DETAILS:** Host details include the essential characteristics of scanme.nmap.org, such as its IP address and potentially its operating system. Quick scans offer limited detail, but subsequent, more thorough scans can reveal more about the system's configuration and service versions.



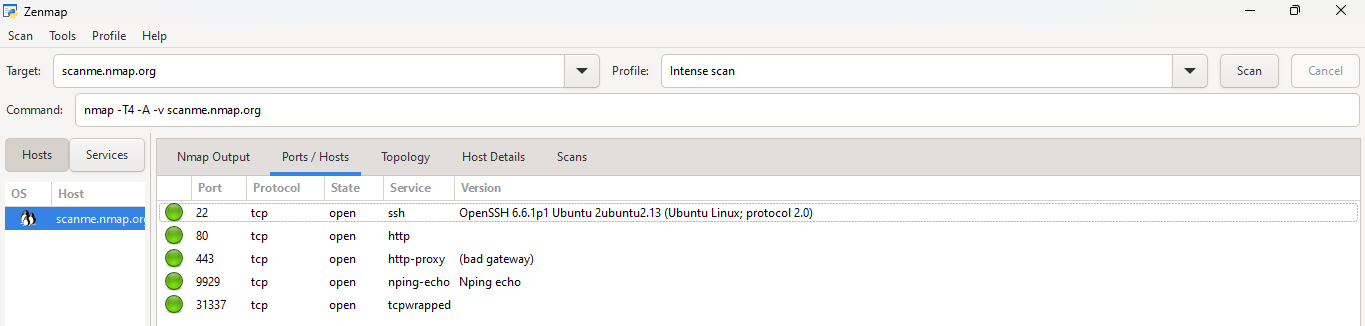
**INTENSE SCAN:**

In intense scan mode, Nmap conducts a comprehensive examination of scanme.nmap.org using the command. This mode performs an in-depth scan that not only identifies open ports but also probes services, OS details, and performs script scanning for vulnerabilities, offering a thorough assessment of the target's network.

* **NMAP OUTPUT:**

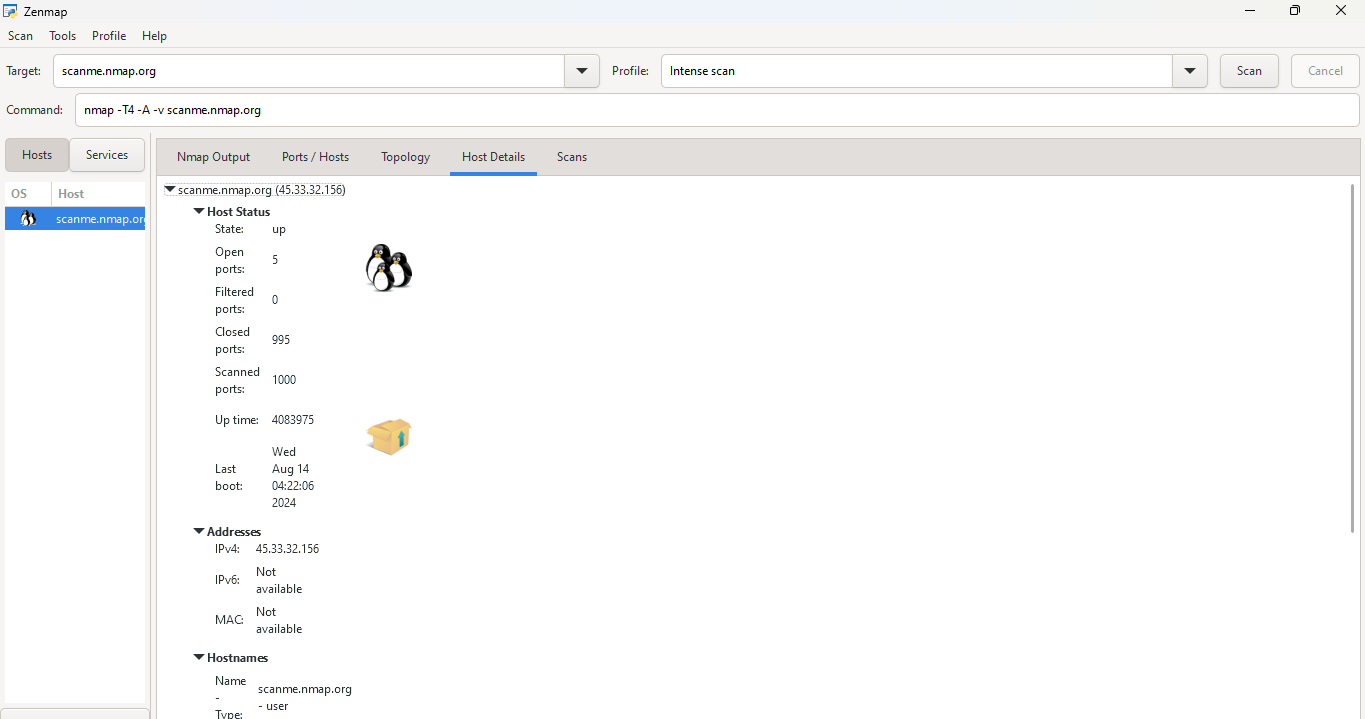
This output is a connected view of the output where we see detailed and comprehensive, listing the status of the host, open ports, services, and their versions. It also includes additional information such as script results, potential vulnerabilities, and OS detection, offering a full picture of the target.

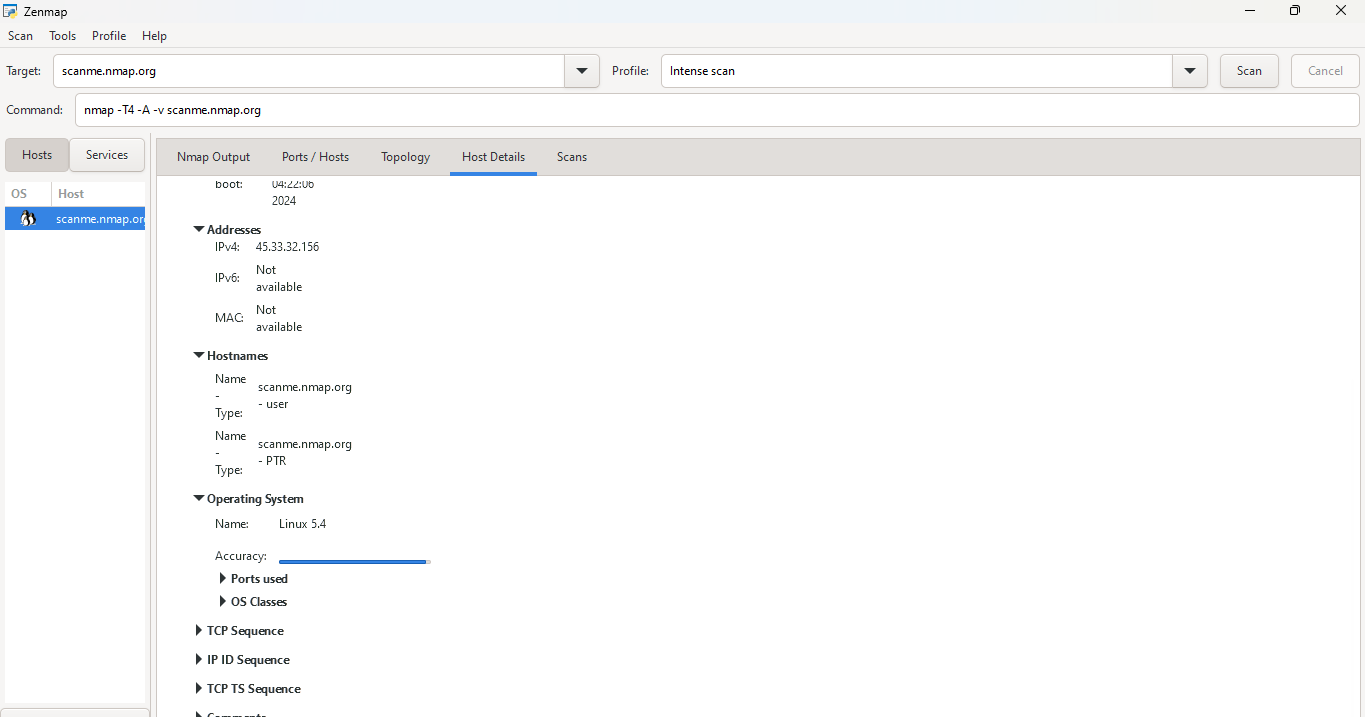
The initial section of the output indicates whether the target host is online or offline. This is shown with a status message, typically “Nmap scan report for scanme.nmap.org (IP address)” followed by “Host is up” or “Host is down,” depending on the results of the ping and other probe attempts.

* **PORTS/HOSTS:**  In intense scan mode, the port/hosts section highlights all open ports on scanme.nmap.org, including both common and less frequently used ports. This extensive listing aids in assessing which services may be exposed and the potential attack vectors that can be exploited.
* **TOPOLOGY:** The intense scan can provide insights into the network topology surrounding scanme.nmap.org. By analyzing responses from various ports and service interactions, it offers a better understanding of how the host is integrated into the broader network, although detailed topology mapping would require additional tools.



* **HOST DETAILS:** Host details in an intense scan encompass a wide range of information, including the operating system, device type, and even details about running applications. This information is critical for security assessments, enabling the identification of possible weaknesses based on the system's configuration.

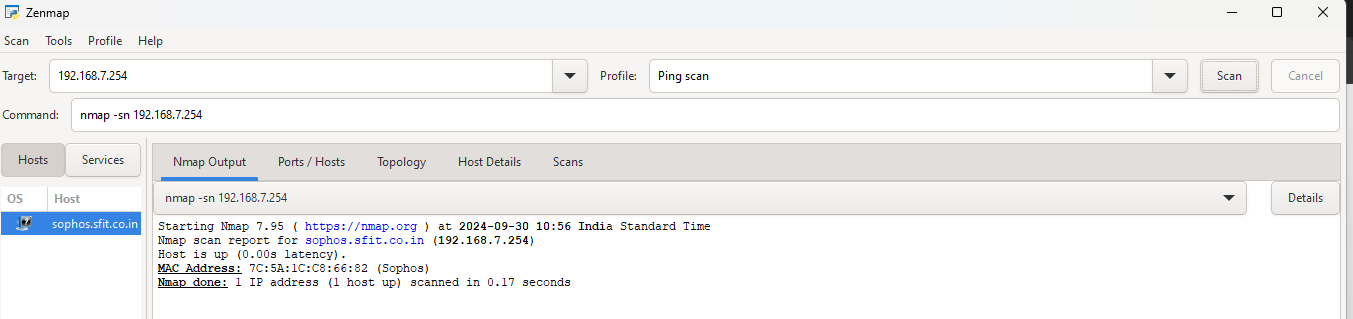




1. **URL OF SFIT.AC.In(use nsloookup) 192.168.7.254**

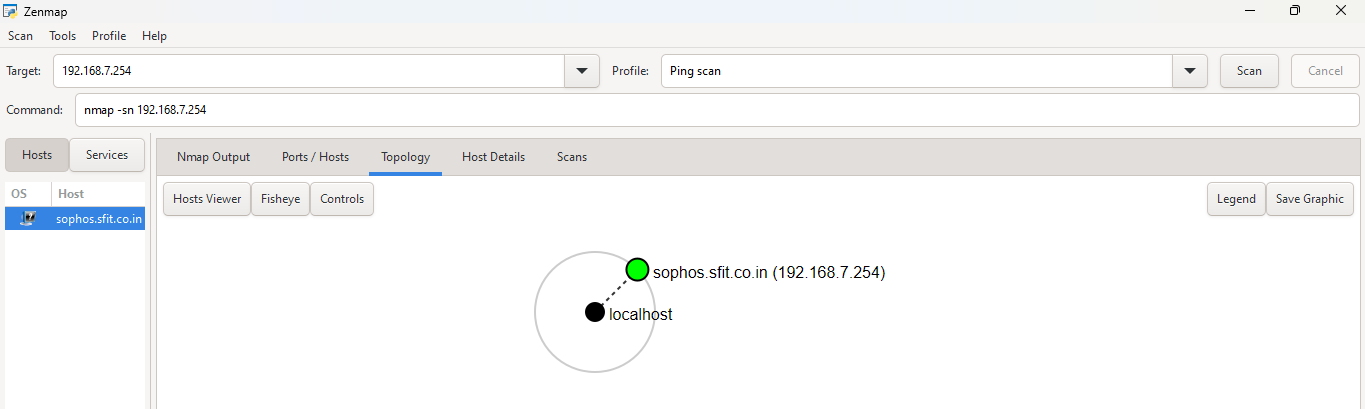
**PING SCAN**

* **NMAP OUTPUT:** A Ping scan using Nmap checks the reachability of a specified host on a network. This scan is executed with the command nmap -sn 192.168.7.254, which sends ICMP echo requests to the target. The output confirms whether the host is online and responsive without scanning any ports, providing a quick way to ascertain network connectivity.

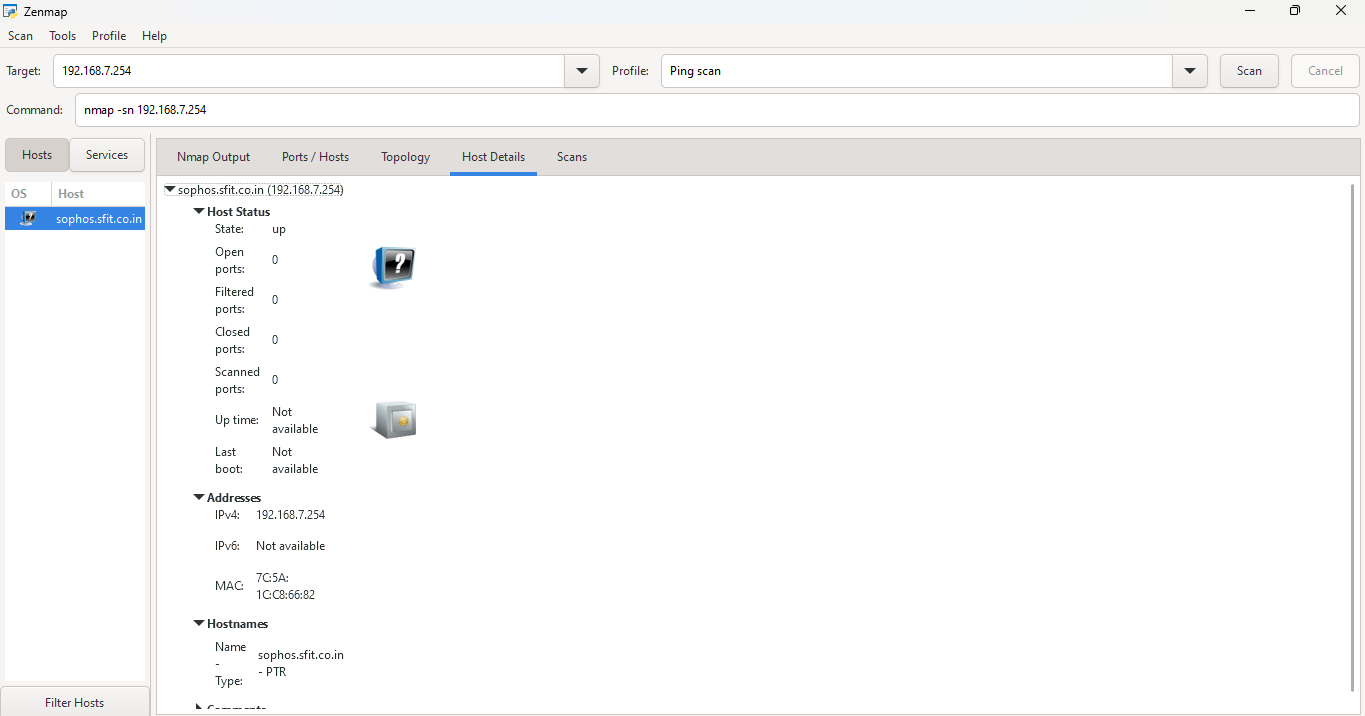


* **TOPOLOGY:**  Here we see the circle where we see how localhost connects to sophos sfit.ac.in

The scan helps map out live hosts within a network segment, indicating which devices are reachable. However, for a comprehensive topology analysis, additional scans and tools would be needed to visualize the connections and layout of the network.

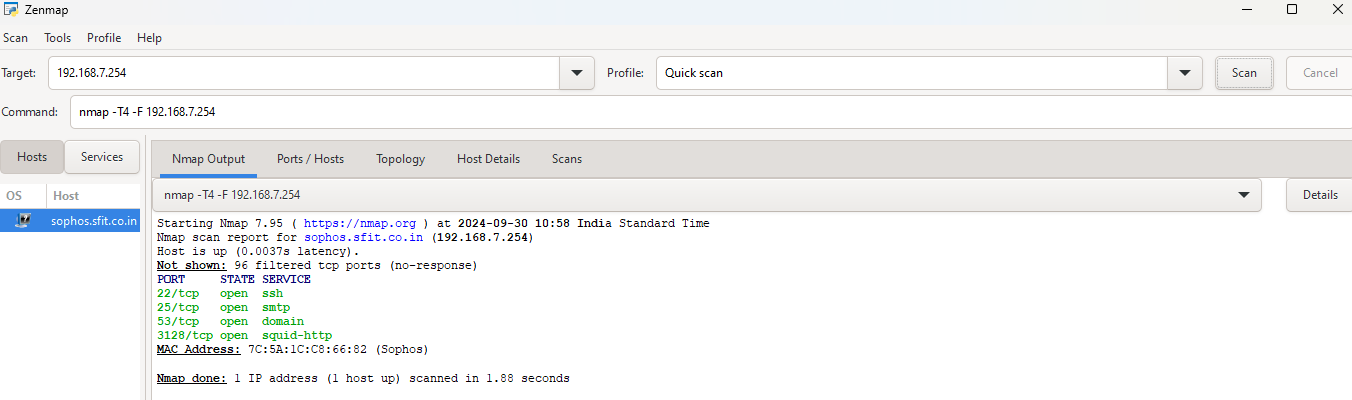


* **HOST DETAILS:** Host details obtained from a Ping scan typically include the IP address (192.168.7.254), status (online or offline), and response time (latency). This response time indicates how quickly the host reacted to the ICMP echo request, allowing for insights into network performance. Additional details, such as MAC addresses or hostname resolution, may require more advanced scans beyond a simple Ping.

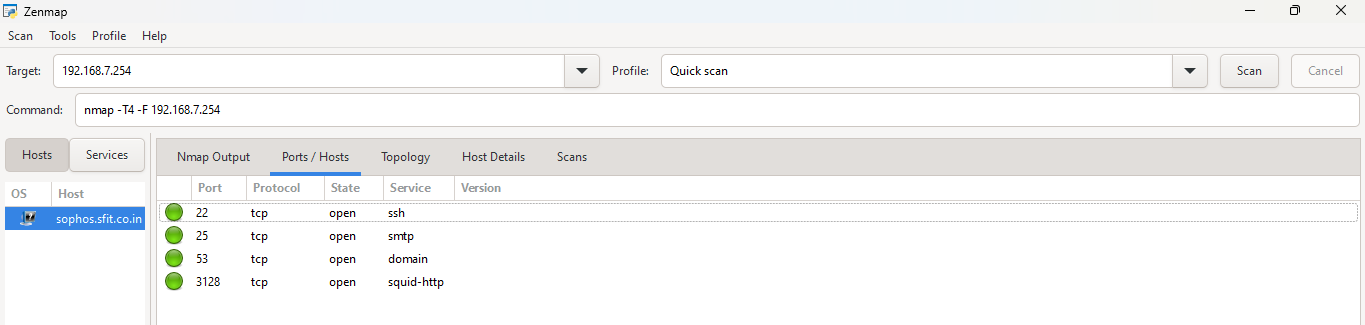


**QUICK SCAN:**

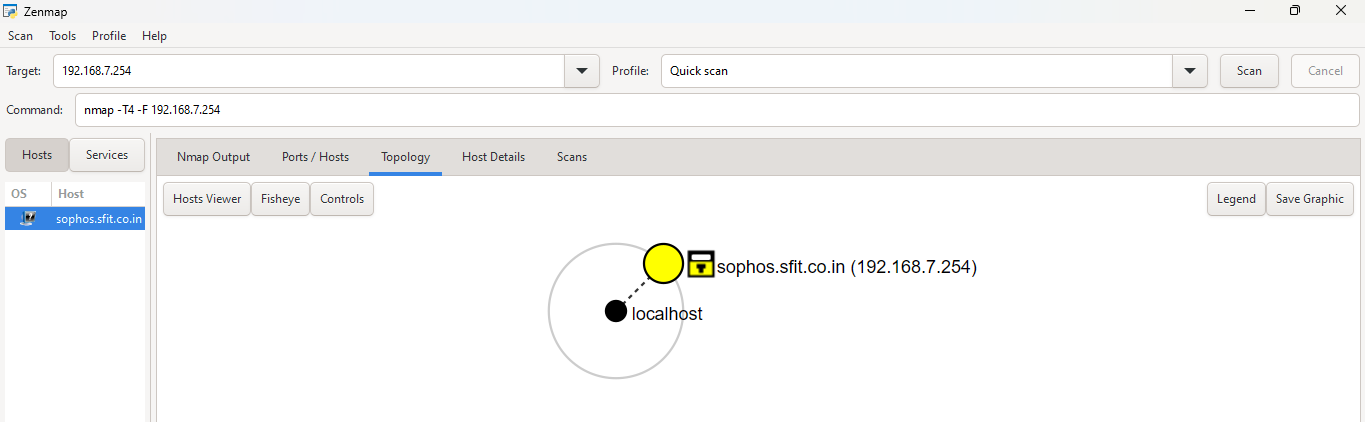
* **NMAP OUTPUT:** Focuses on quickly identifying open ports and services on the target host. This scan employs the -F option to perform a fast scan, checking only the most common 100 ports. The -T4 timing template speeds up the scan process while balancing performance and accuracy.



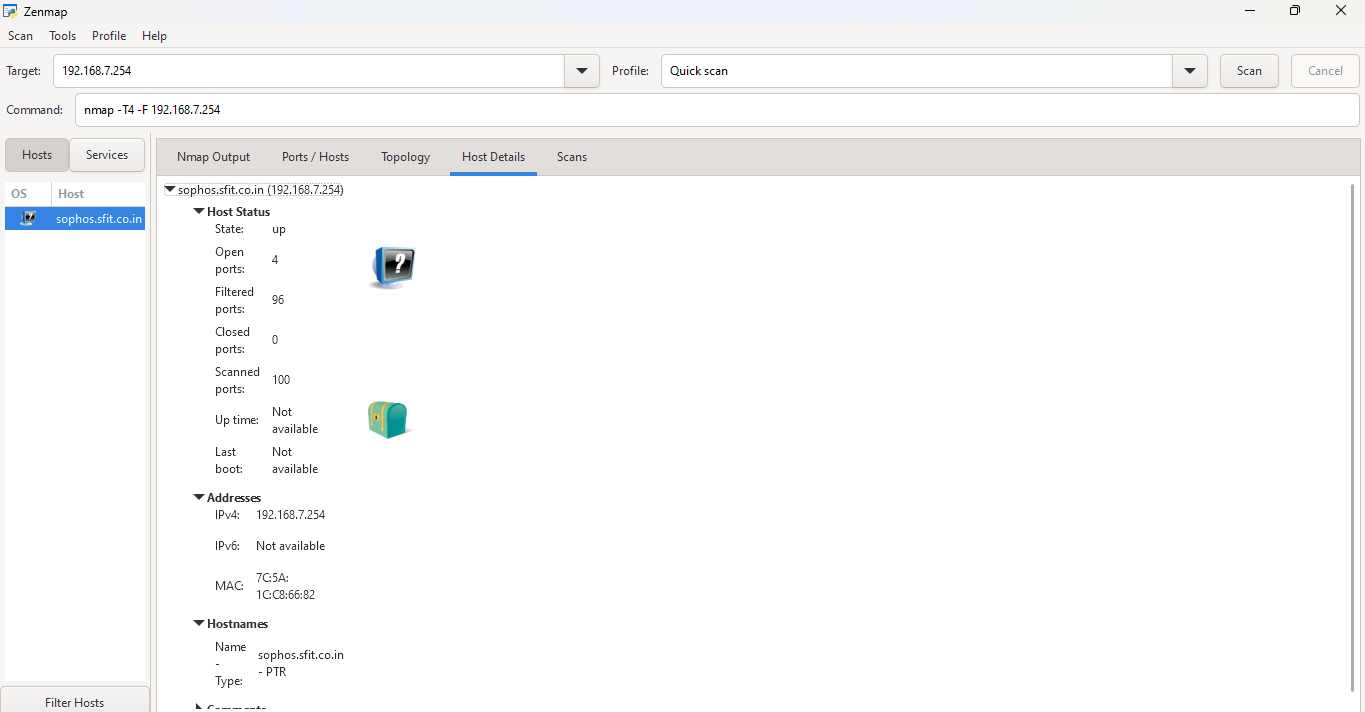
* **PORTS/HOSTS:** This indicates that the SSH service is running on port 22 and a web server is active on port 80, which could potentially be a vulnerable point for attackers if not properly secured. The quick scan focuses on essential ports, providing immediate insights into which services are available.



* **TOPOLOGY:** The Quick Scan doesn’t inherently provide a detailed topology view but gives an understanding of the host's network context. By confirming the open ports, administrators can infer the roles of devices within the network.

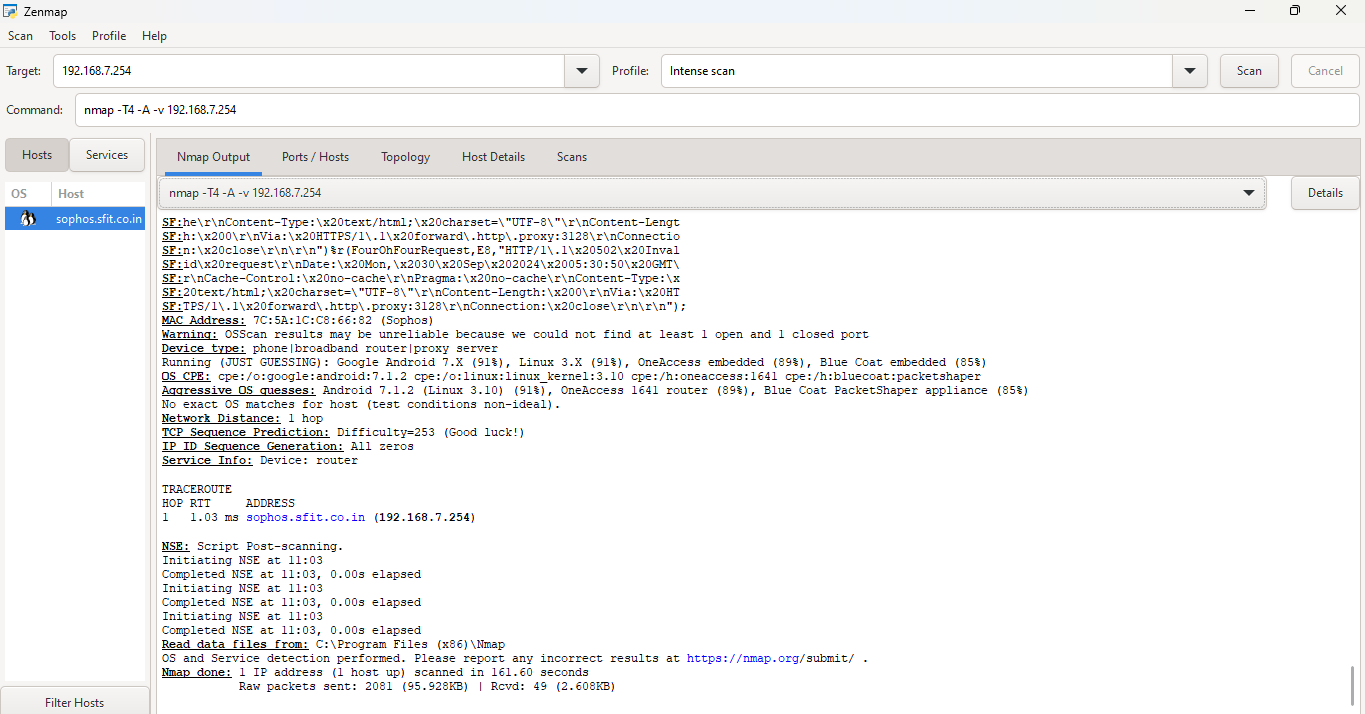
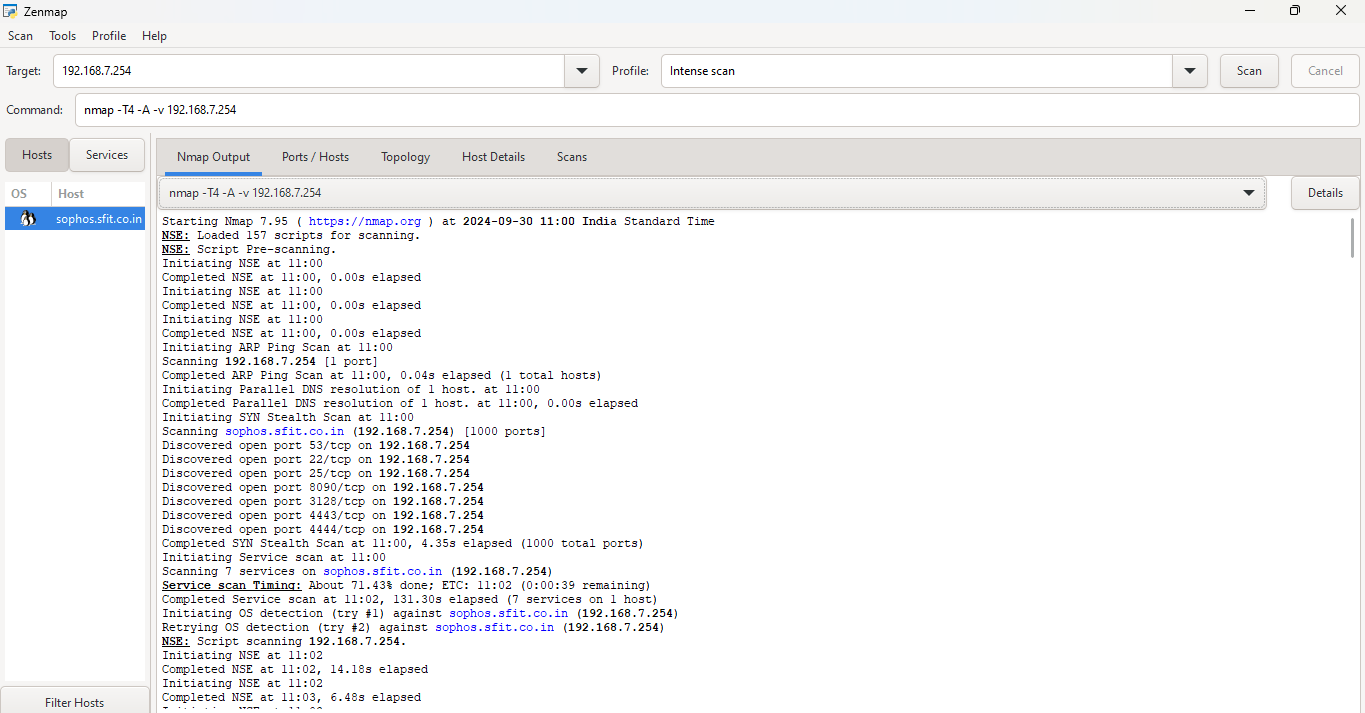


* **HOST DETAILS:** This line confirms that the host is online and provides latency information, which indicates the response time for packets sent to the target. Additional details may include hostname resolution if available, like hostname.example.com, allowing for better identification of the host within the network.

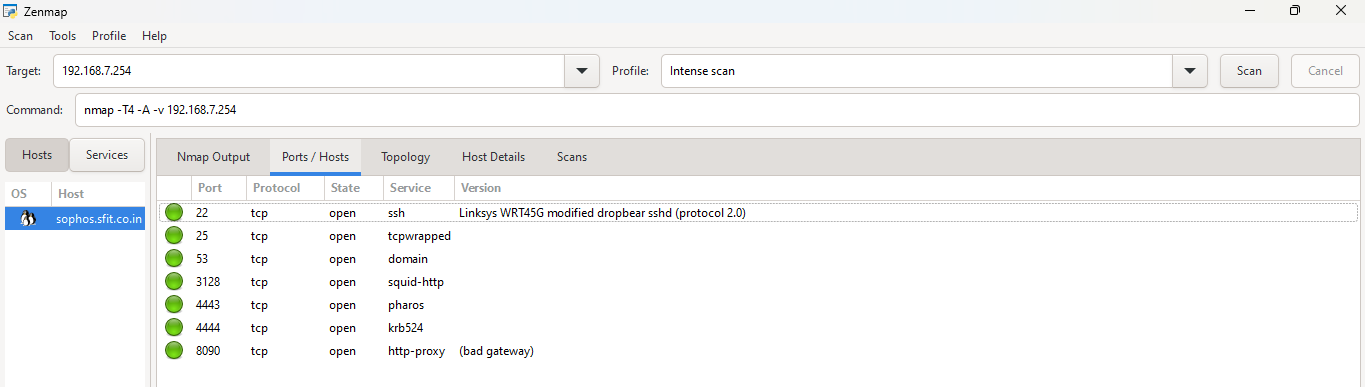


**INTENSE SCAN:**

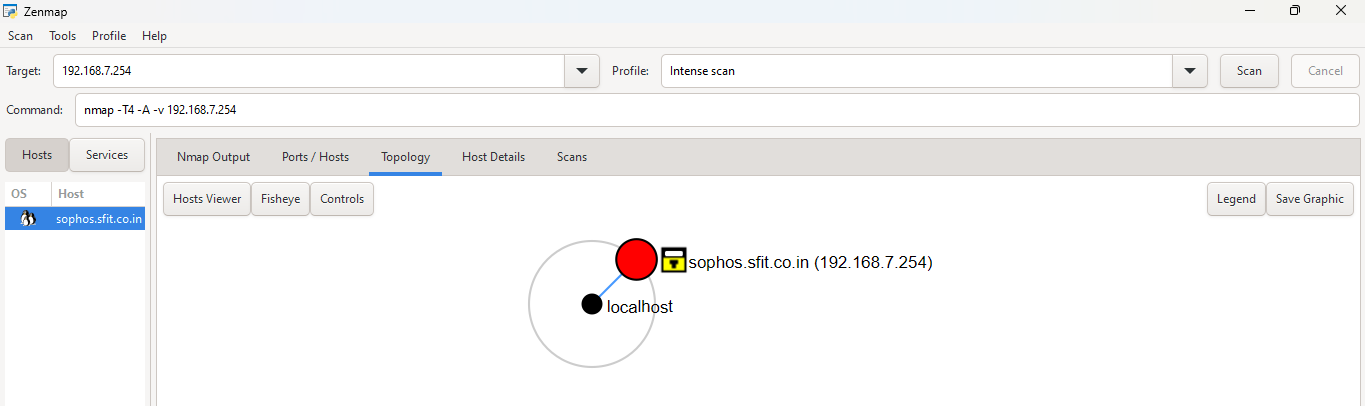
* **NMAP OUTPUT:** An Intense Scan using Nmap, executed with the commanddetection, version detection, script scanning, and traceroute, and the -p- option scans all 65535 TCP ports. The -T4 timing template optimizes the scan speed while maintaining accuracy.



* **PORTS/HOSTS:** This output indicates not only the state of each port (open) but also the specific services running and their versions. Such detailed information is crucial for vulnerability assessment, as it allows administrators to identify outdated software that may be susceptible to attacks.



* **TOPOLOGY:** While the Intense Scan itself does not produce a graphical topology map, the comprehensive data it provides can aid in understanding the network structure. The scan identifies the roles of various services on the target host, allowing administrators to infer how this device interacts within the network.



* **HOST DETAILS:** Begins with a scan report, providing the IP address of the host being analyzed, along with its status. For instance, it typically indicates whether the host is up or down, often including latency information that reflects the responsiveness of the server.

