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 the Zenmap tool on the system.
2) Study the Zenmap documentation for using its GUI.
3) Scan the network with the 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.

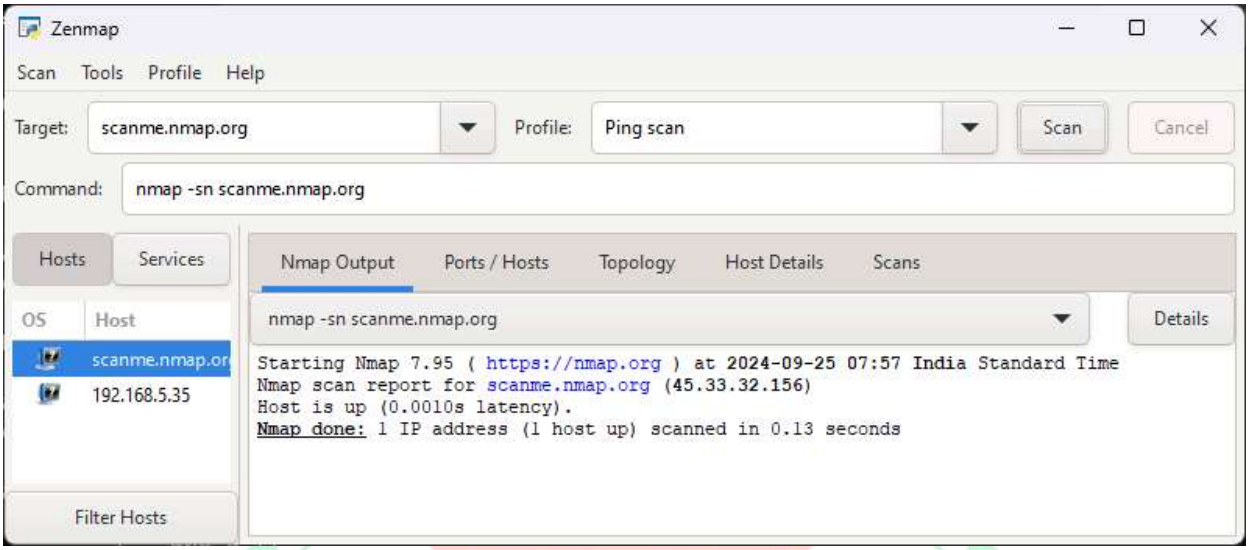
Conclusion:

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.

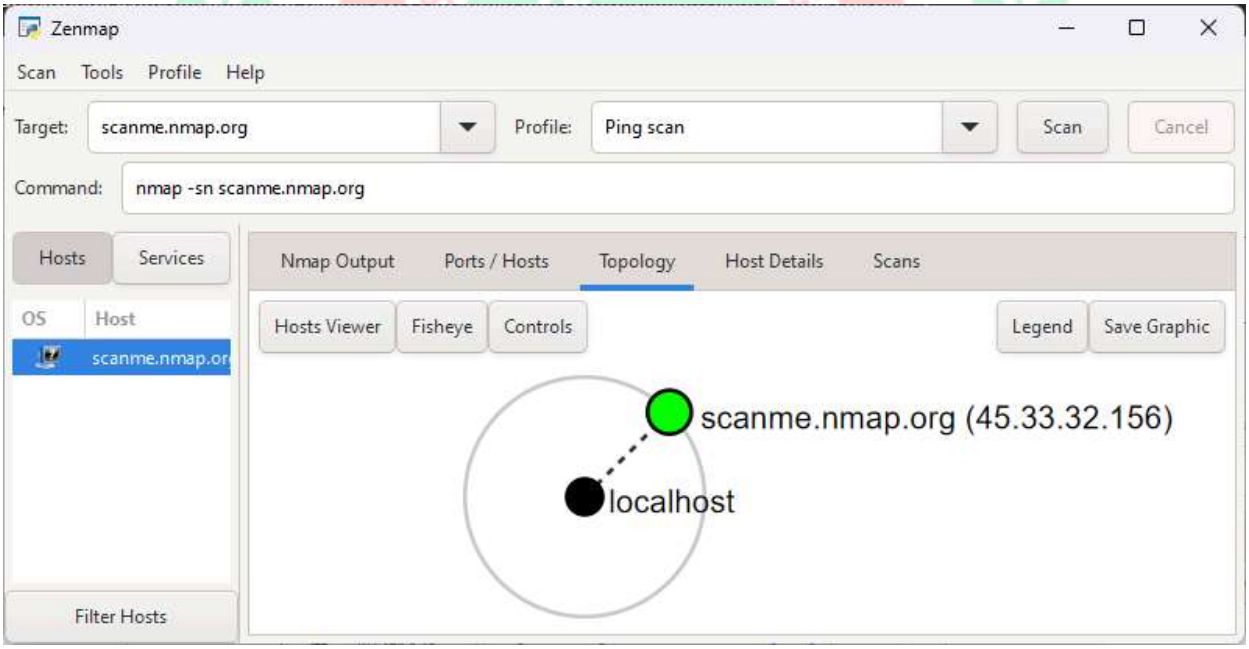
References: *(Mention your references here.)*

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

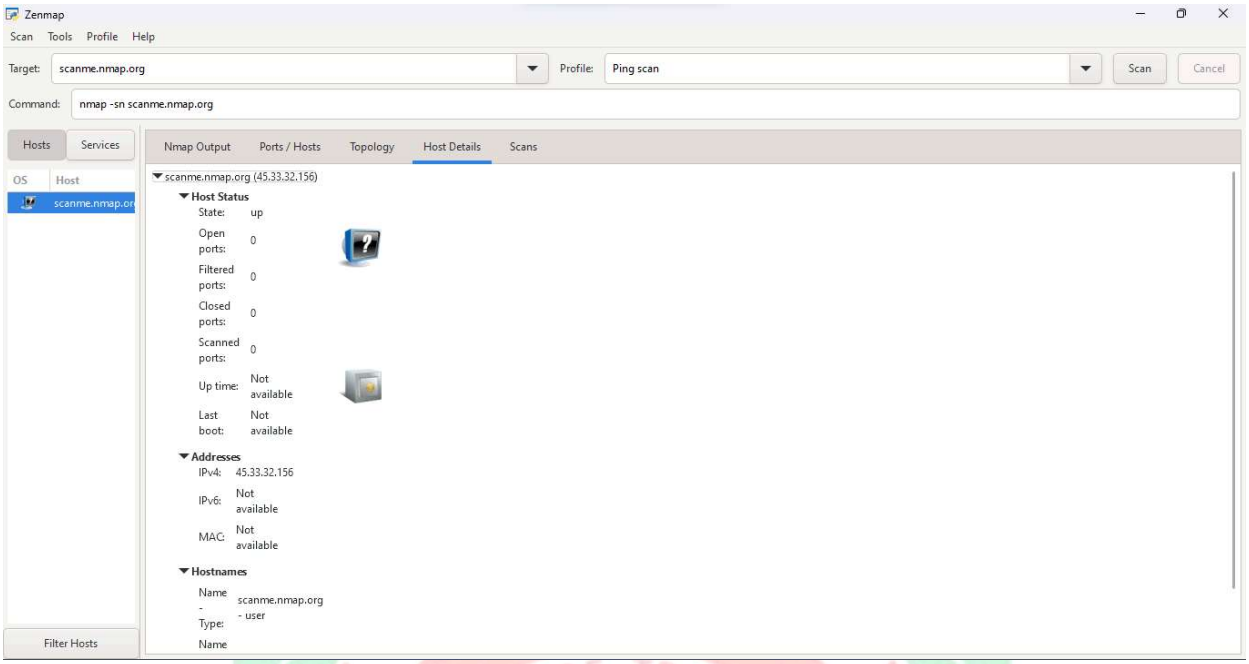
Ping Scan of scanme.nmap.org



Zenmap's ping scan on scanme.nmap.org (45.33.32.156) shows the host is up with 0.00108s latency. The scan completed in 0.13 seconds, confirming the host is reachable.

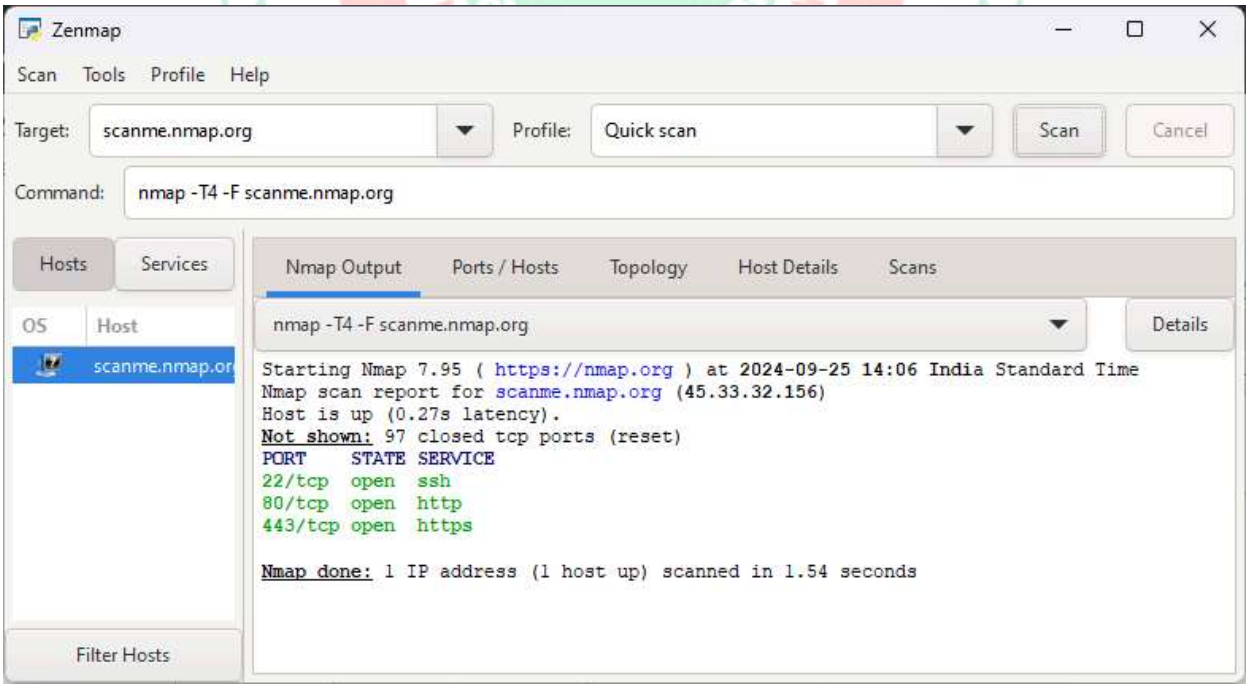


In Zenmap's Topology view, localhost (your machine) appears as a black dot, and scanme.nmap.org (45.33.32.156) as a green dot, indicating the host is up. A dashed line connects them, representing the network link between your system and the target.

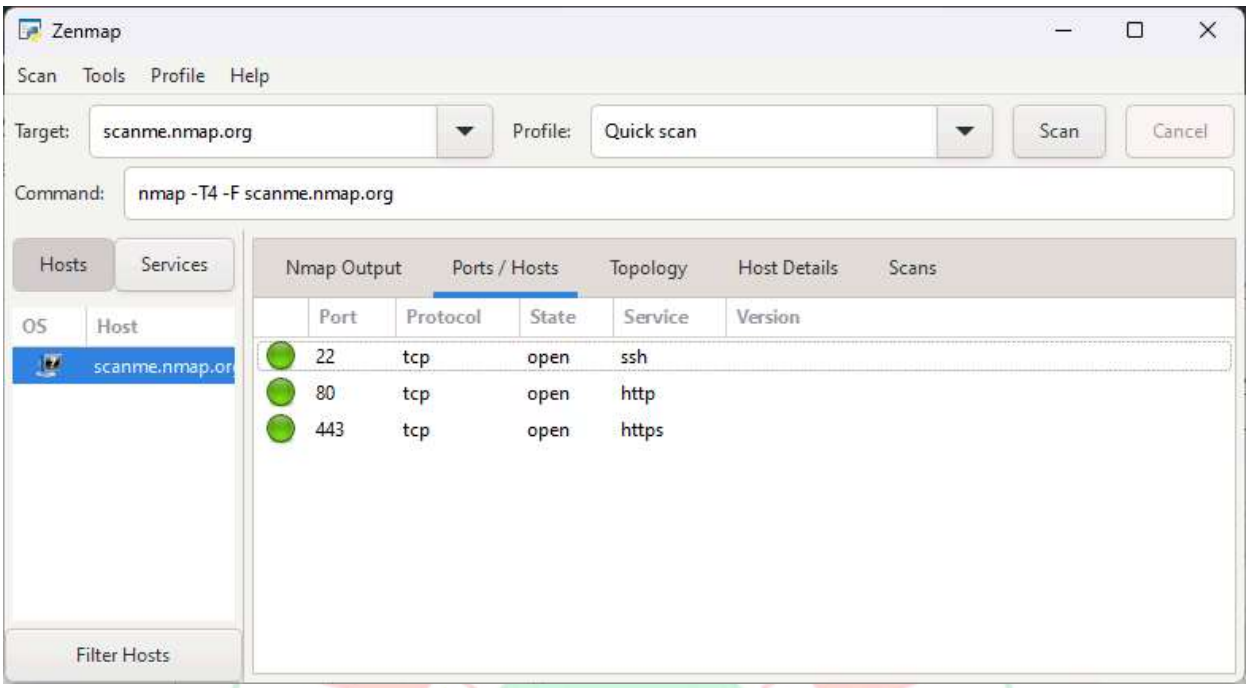


In Zenmap's "Host Details" tab, the target scanme.nmap.org (45.33.32.156) is shown as up. The scan reveals the IP address, hostname, and basic network details, confirming the host's active status and network connection.

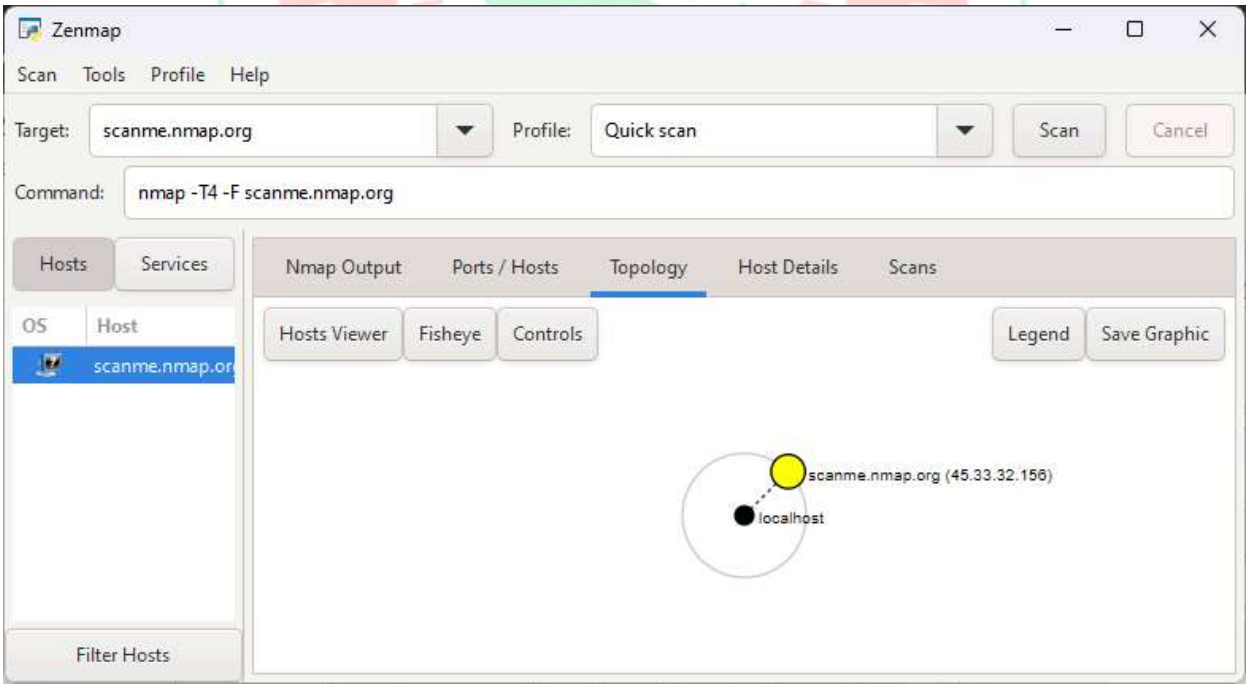
Quick Scan of scanme.nmap.org



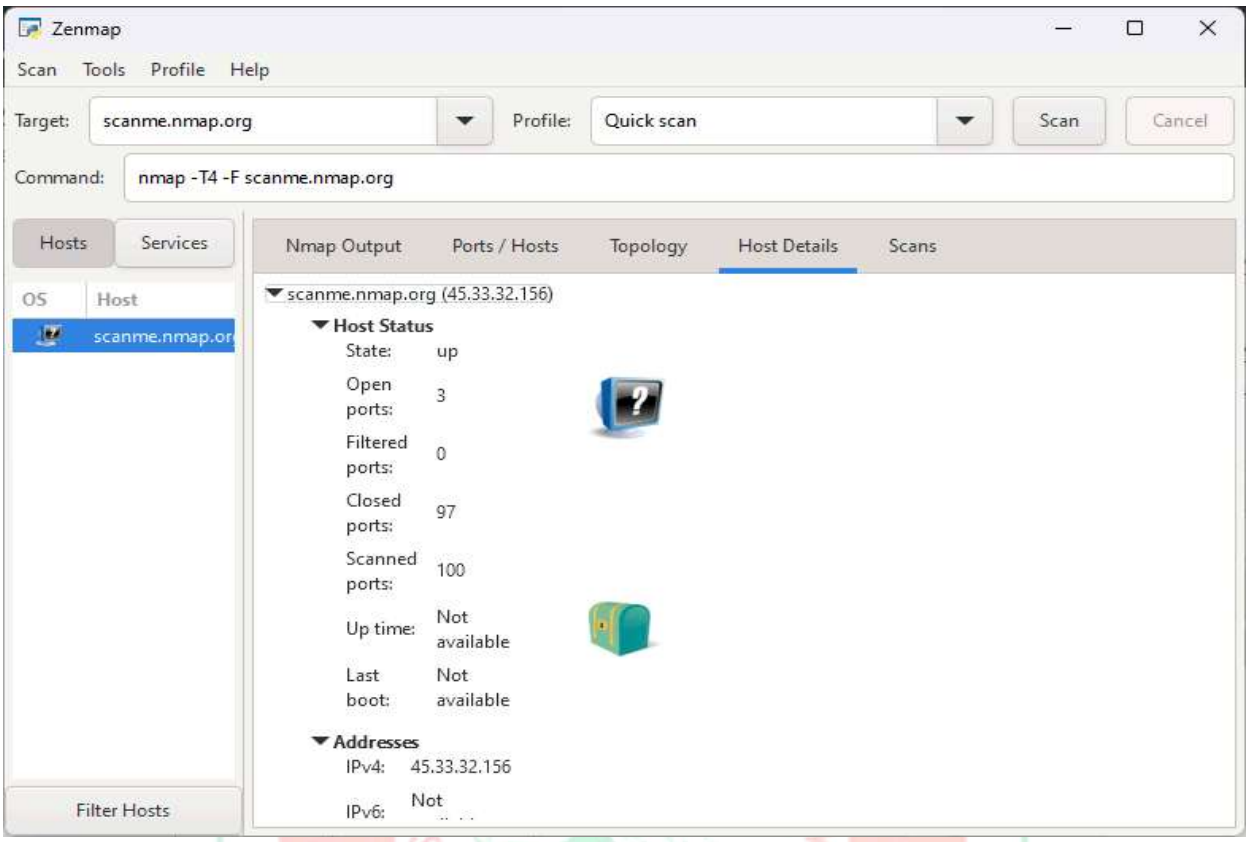
In Zenmap's Quick Scan of scanme.nmap.org (45.33.32.156), the host is up with 0.217s latency. It shows three open ports: SSH (22), HTTP (80), and HTTPS (443). The scan completed in 1.54 seconds.



In Zenmap's "Ports/Hosts" tab, a Quick Scan of scanme.nmap.org (45.33.32.156) shows three open ports: 22/tcp (SSH), 80/tcp (HTTP), and 443/tcp (HTTPS). All services are active and reachable.

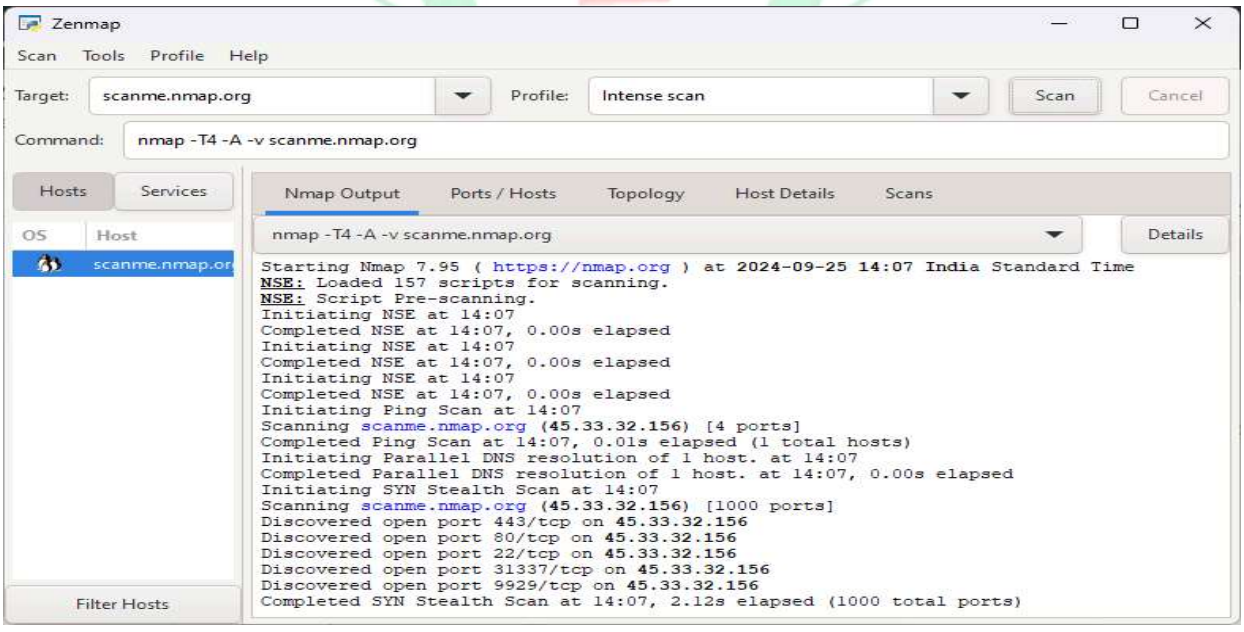


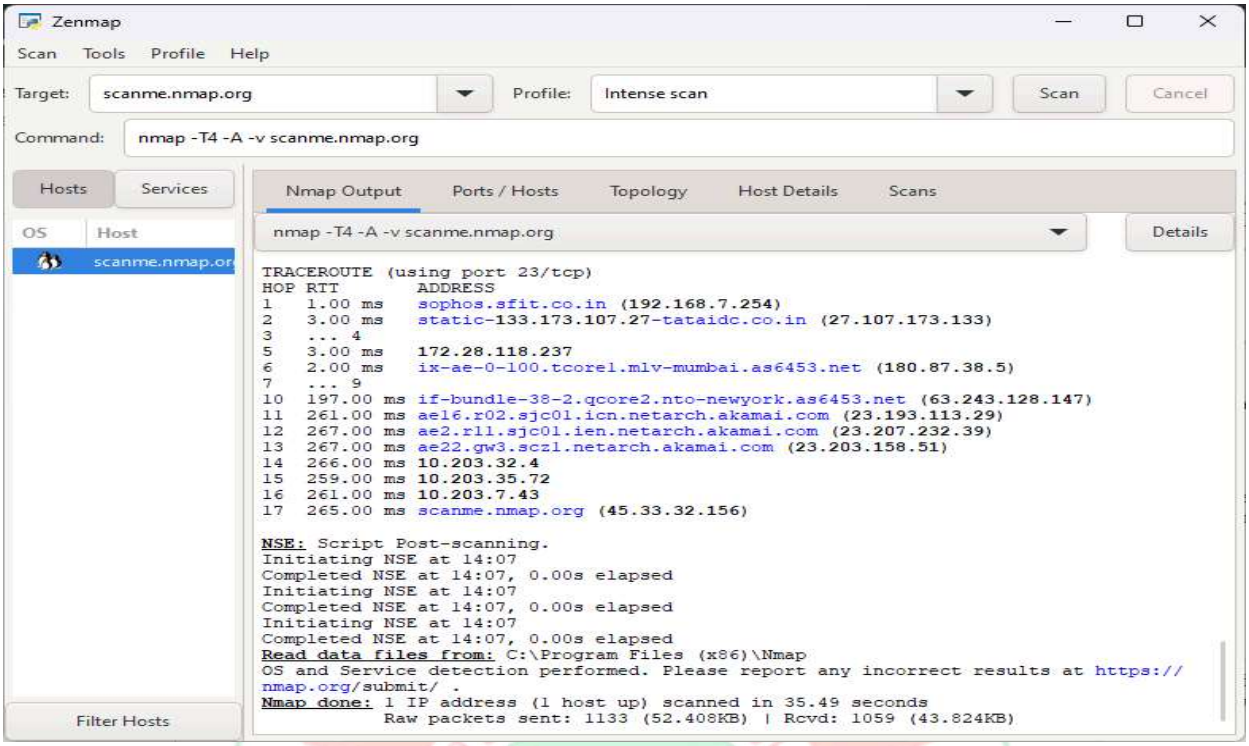
In Zenmap's topology view, localhost (your machine) is represented as a black dot, while scanme.nmap.org (45.33.32.156) is shown as a yellow dot, indicating that the host is up but not responding to pings. A dashed line connects the two, visually representing the network connection between your system and the target host.

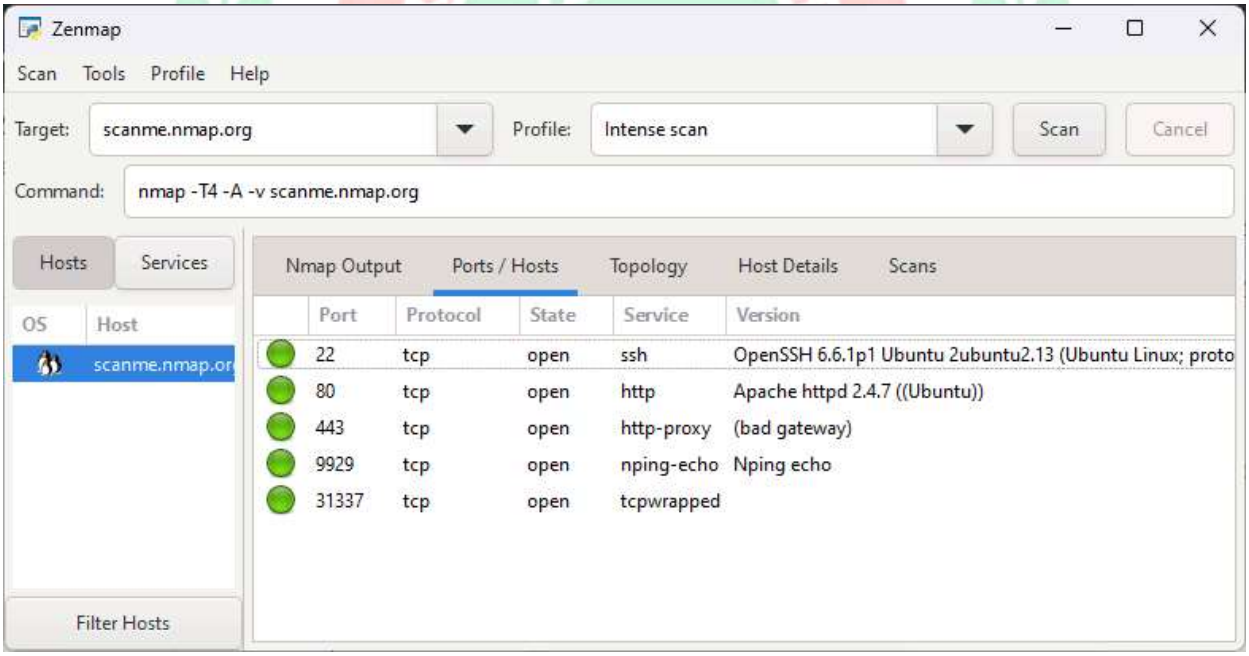


In Zenmap's "Host Details," the target scanme.nmap.org (45.33.32.156) shows that three ports are open (22, 80, and 443) while 93 ports are closed. The IP address is confirmed as 45.33.32.156, indicating the host's active status and its network connectivity.

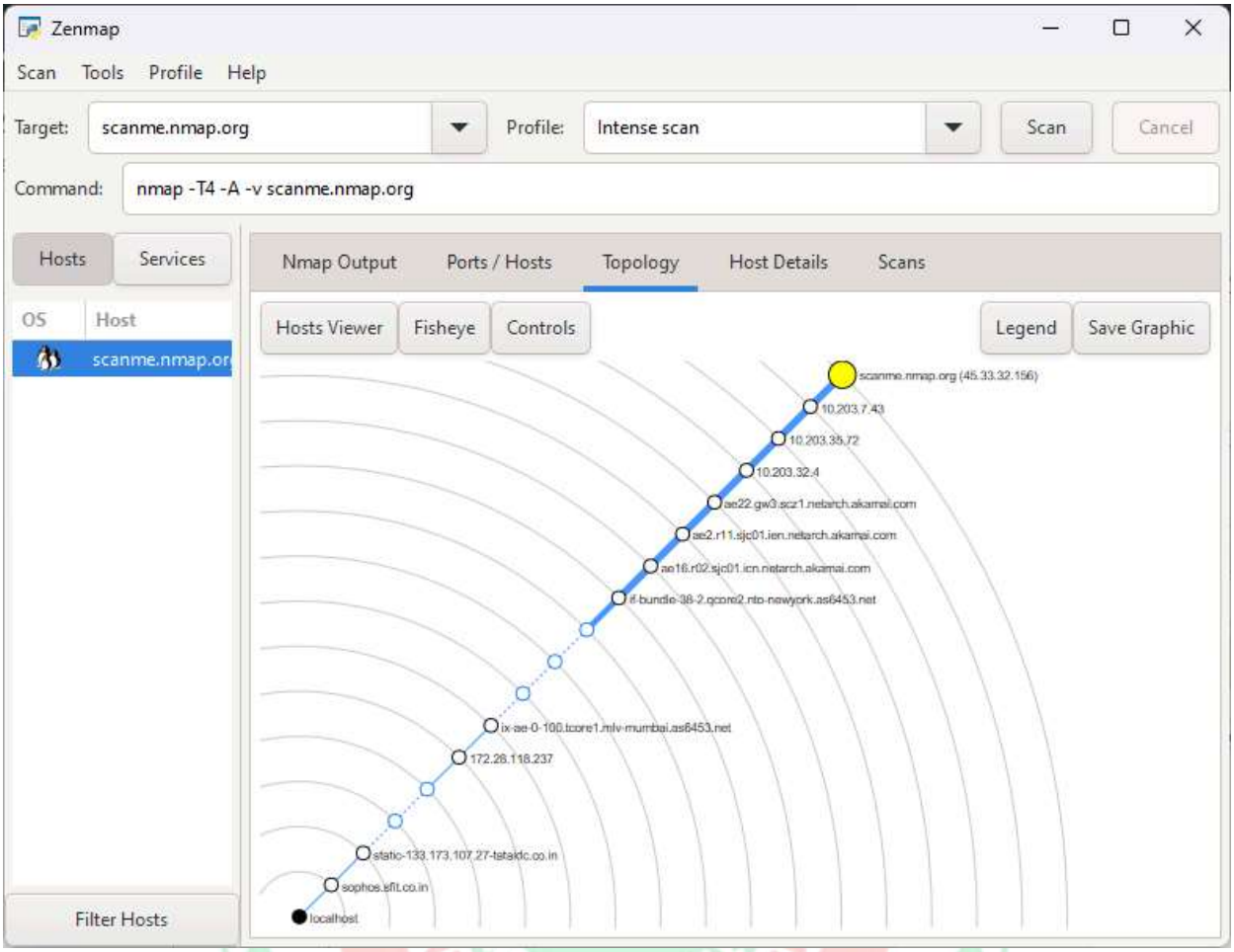
Intense Scan of scanme.nmap.org



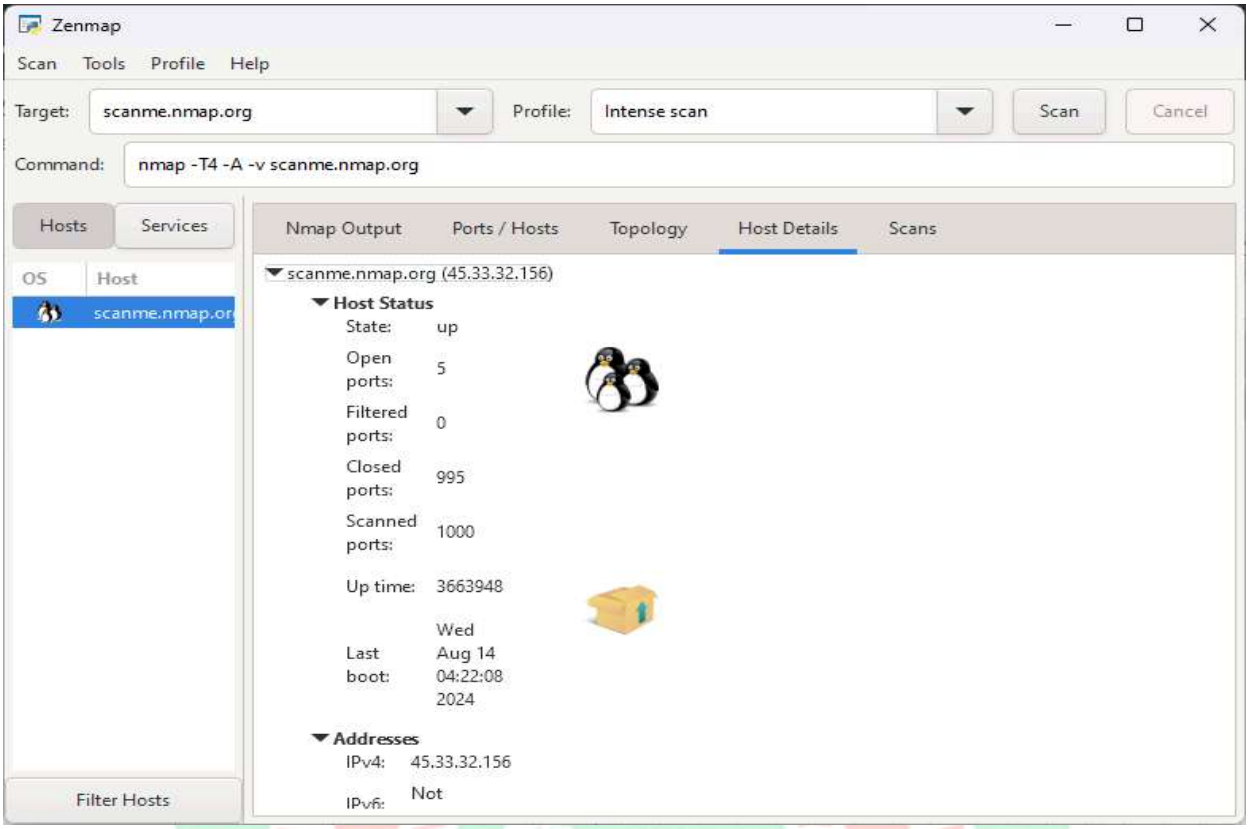




In Zenmap's "Ports/Hosts" tab, a Intense Scan of scanme.nmap.org (45.33.32.156) shows five open ports: 22/tcp (SSH), 80/tcp (HTTP), 443/tcp (HTTPS),9929/tcp and 31337/tcp . All services are active and reachable.

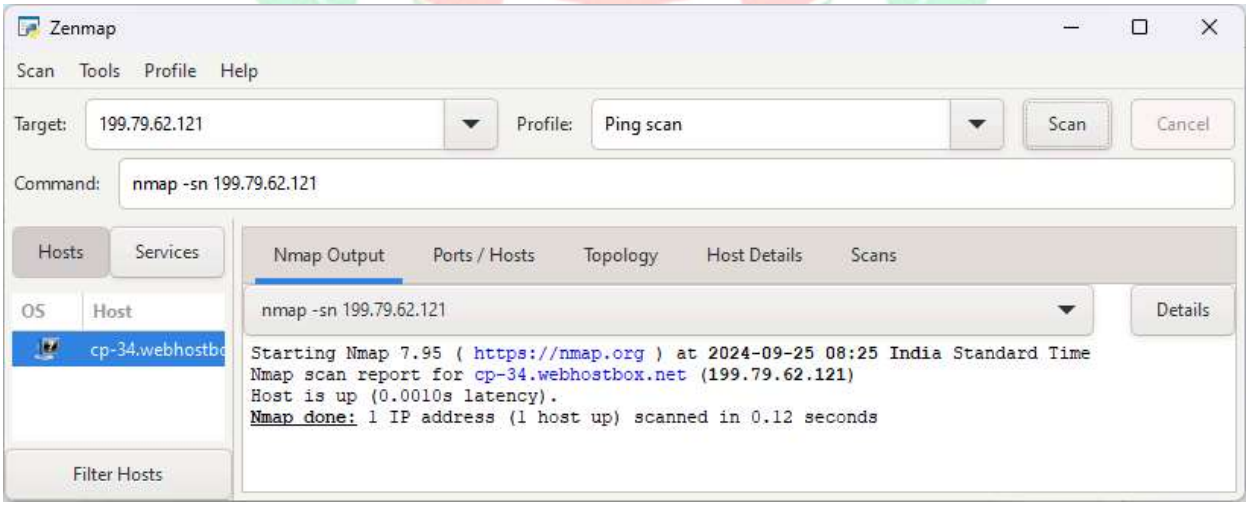


In Zenmap's topology view for the intense scan, localhost (your machine) is represented as a black dot, while scanme.nmap.org (45.33.32.156) appears as a yellow dot, indicating the host is up but not responding to pings. There are 11 white dots in between, representing intermediate devices or nodes on the network. A dashed line connects your system to the target host, visually illustrating the network path.

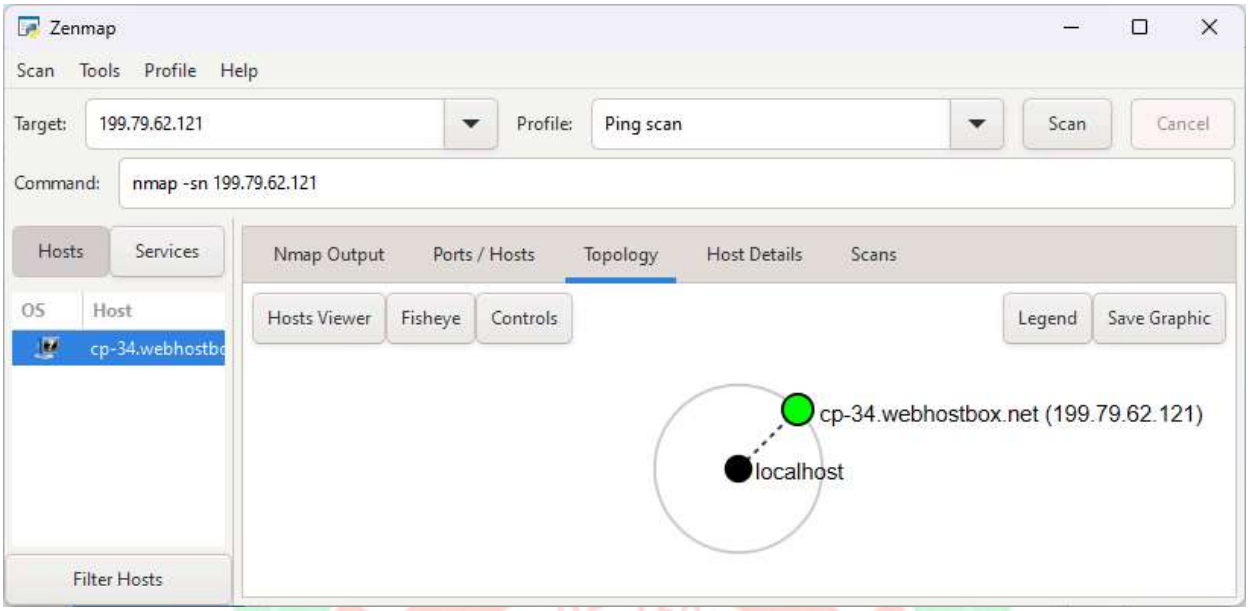


In Zenmap's "Host Details" for the intense scan, the target scanme.nmap.org (45.33.32.156) shows that five ports are open while 995 ports are closed. A total of 1000 ports were scanned, with an uptime of 3,663,948 seconds. The IP address remains 45.33.32.156, confirming the host's active status and network connectivity.

Ping Scan of Public IP of SFIT (199.79.62.121)

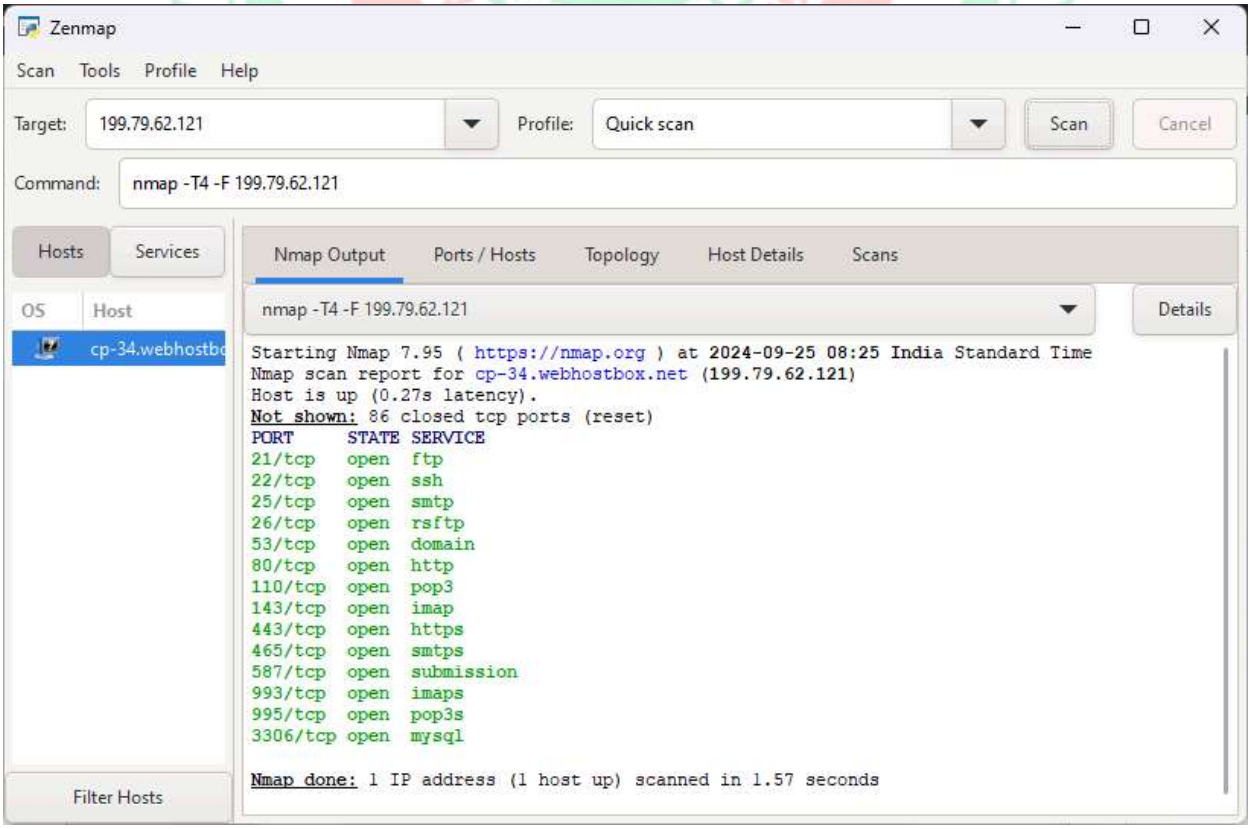


Zenmap's ping scan on 199.79.62.121 shows the host is up with 0.0010s latency. The scan completed in 0.12 seconds, confirming the host is reachable.

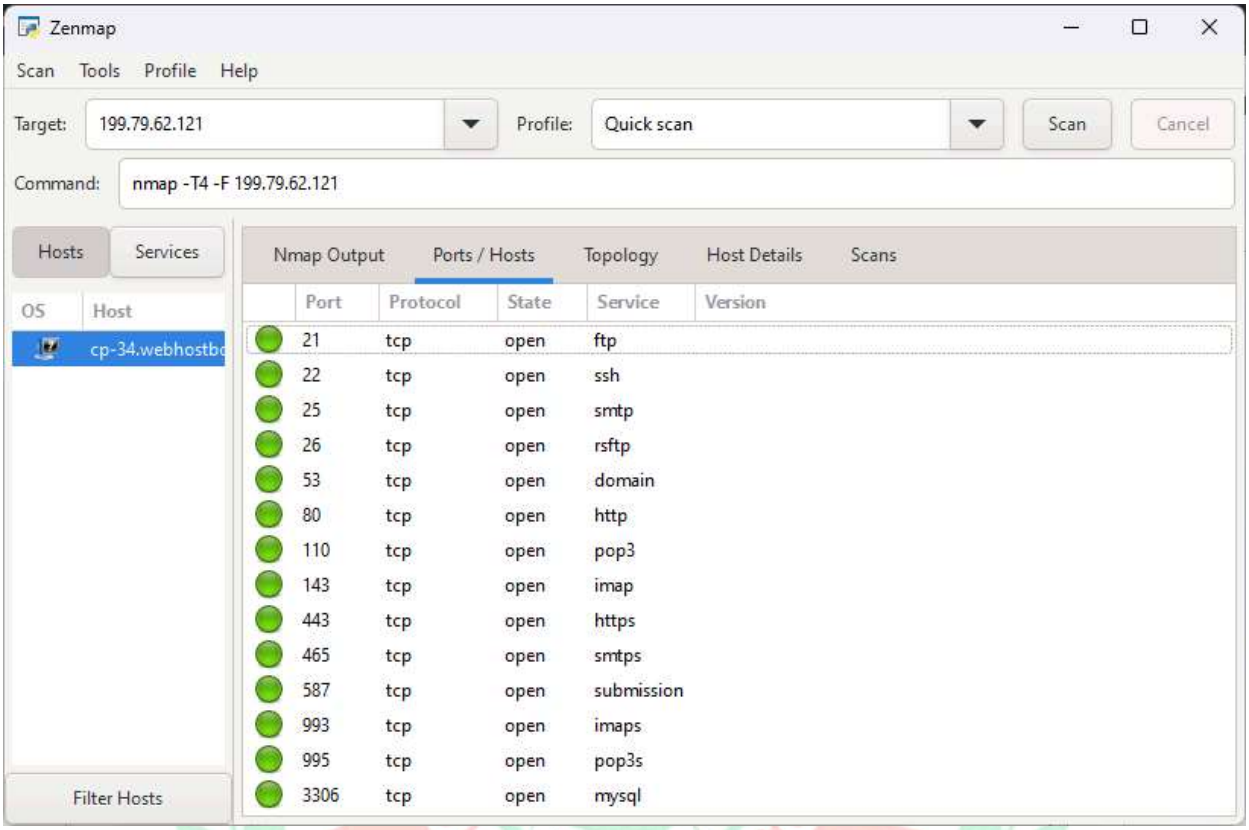


In Zenmap's Topology view, localhost (your machine) appears as a black dot, and 199.79.62.121 as a green dot, indicating the host is up. A dashed line connects them, representing the network link between your system and the target.

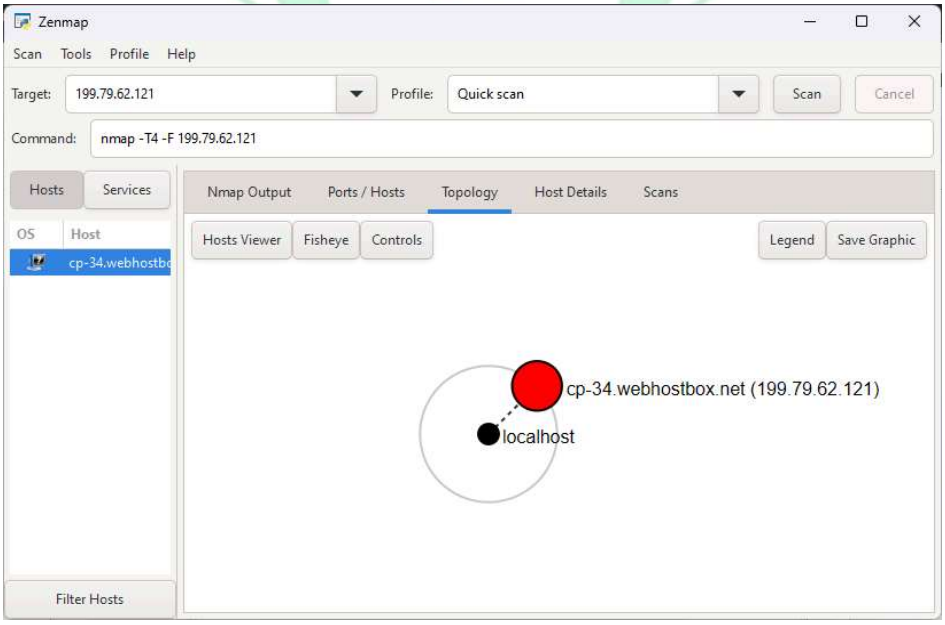
Quick Scan of Public IP of SFIT (199.79.62.121)



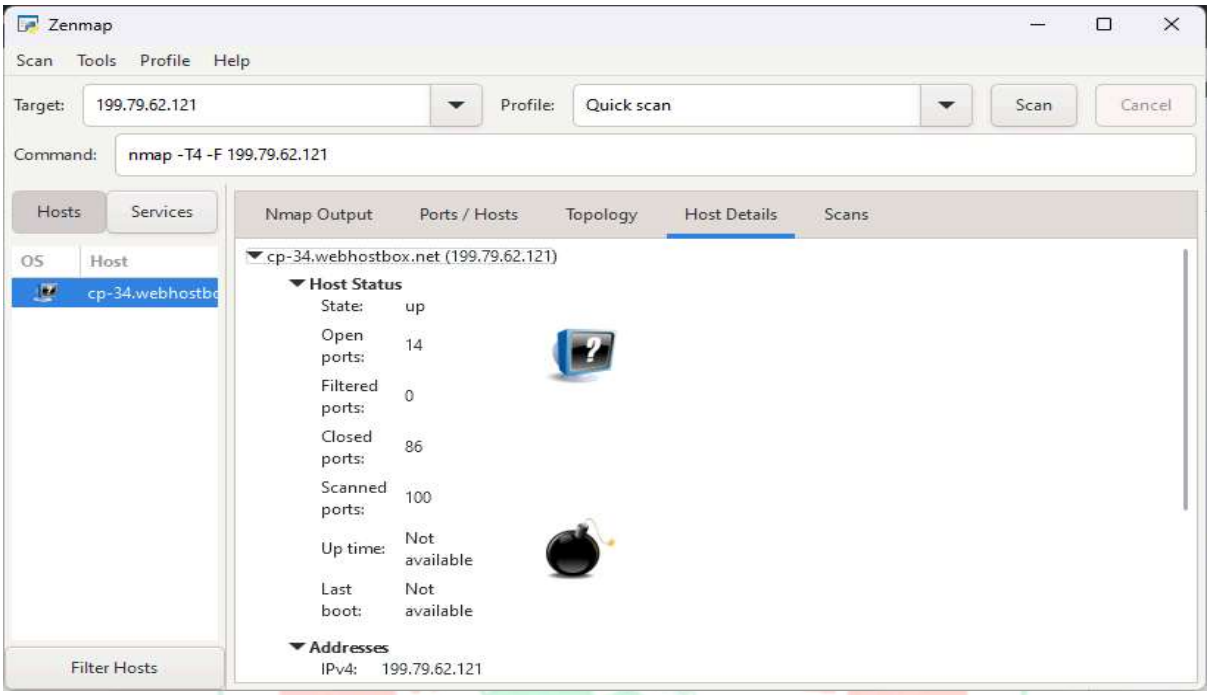
In Zenmap's Quick Scan of 199.79.62.121 , the host is up with 0.27s latency. It shows 14 open ports. The scan completed in 1.57 seconds.



In Zenmap's "Ports/Hosts" tab, a Quick Scan of 199.79.62.121 shows 14 open ports such as 22/tcp (SSH), 80/tcp (HTTP), and 443/tcp (HTTPS) etc. . All services are active and reachable.

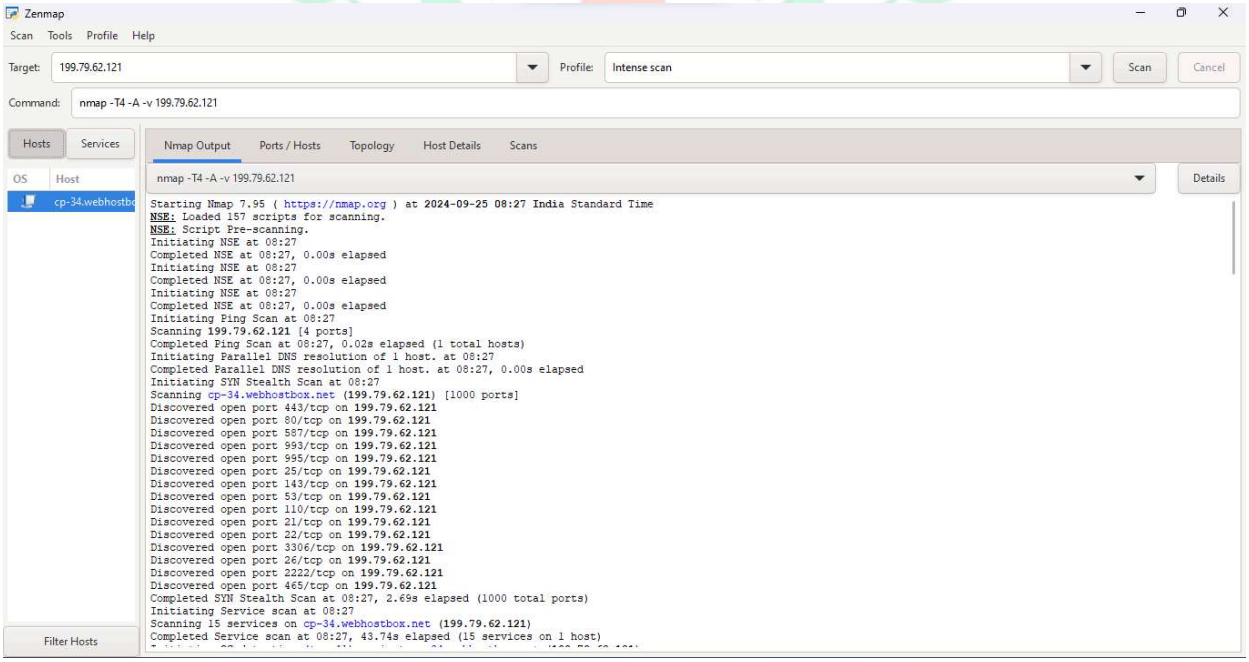


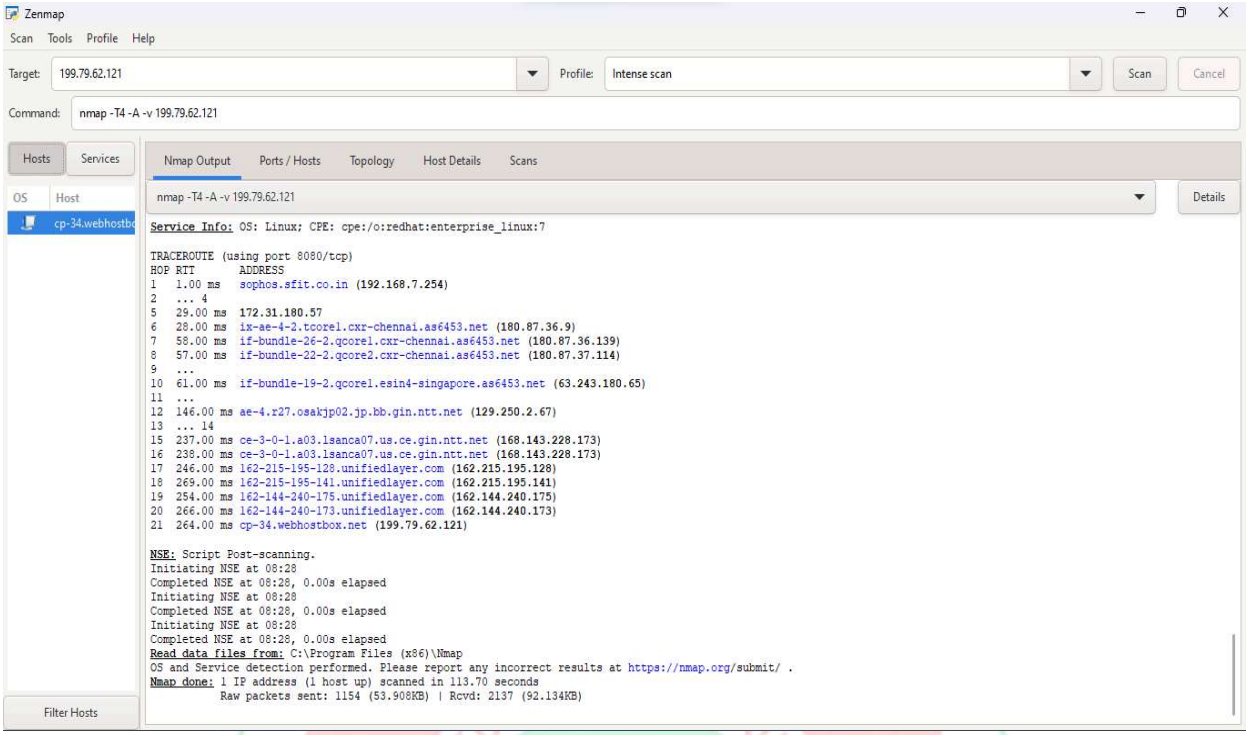
In Zenmap's topology view, localhost (your machine) is represented as a black dot, while 199.79.62.121 is shown as a red dot, indicating that the host is down or unresponsive. A dashed line connects the two, visually representing the network connection between your system and the target host.

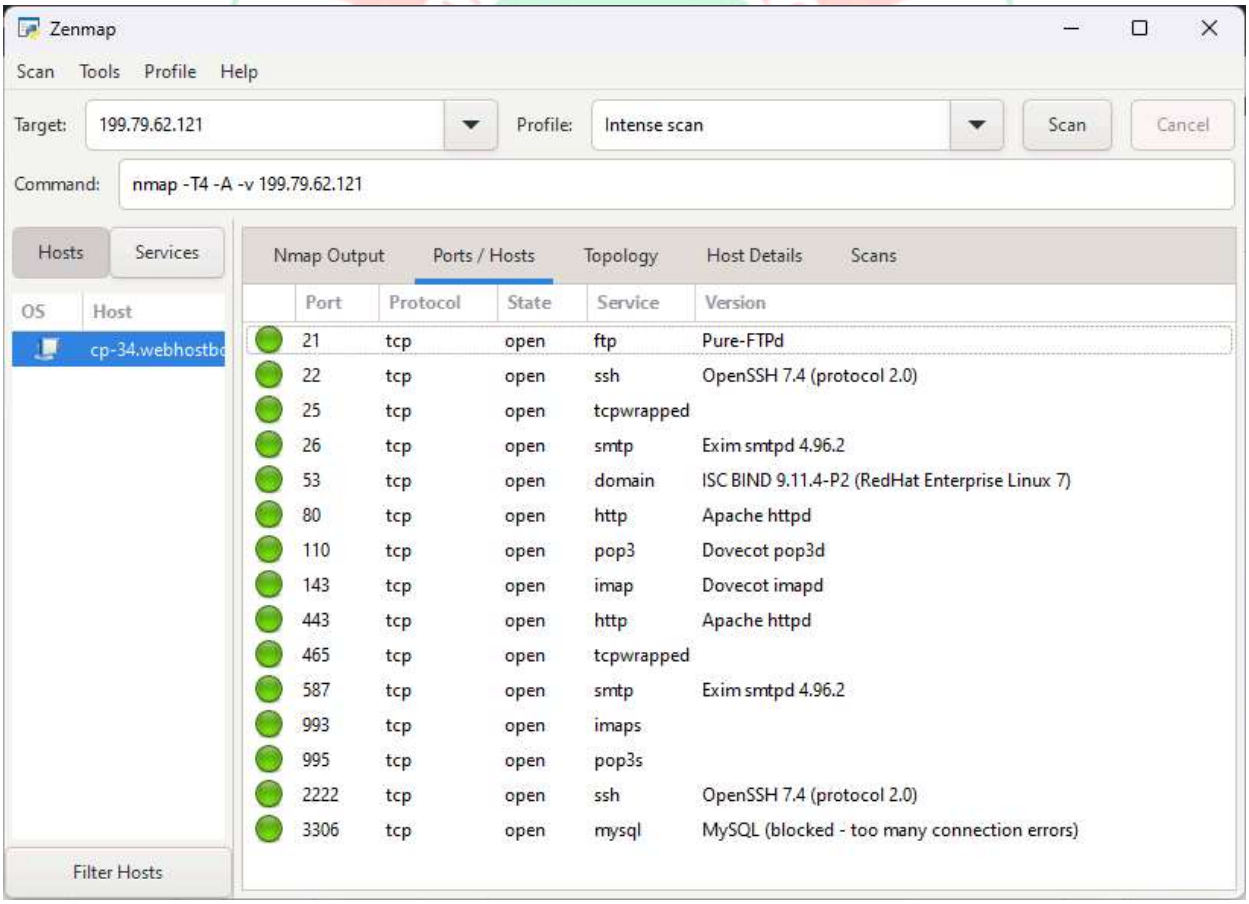


In Zenmap's "Host Details," the target 199.7962.121 shows that 14 ports are open while 86 ports are closed. The IP address is confirmed as 199.7962.121, indicating the host's active status and its network connectivity.

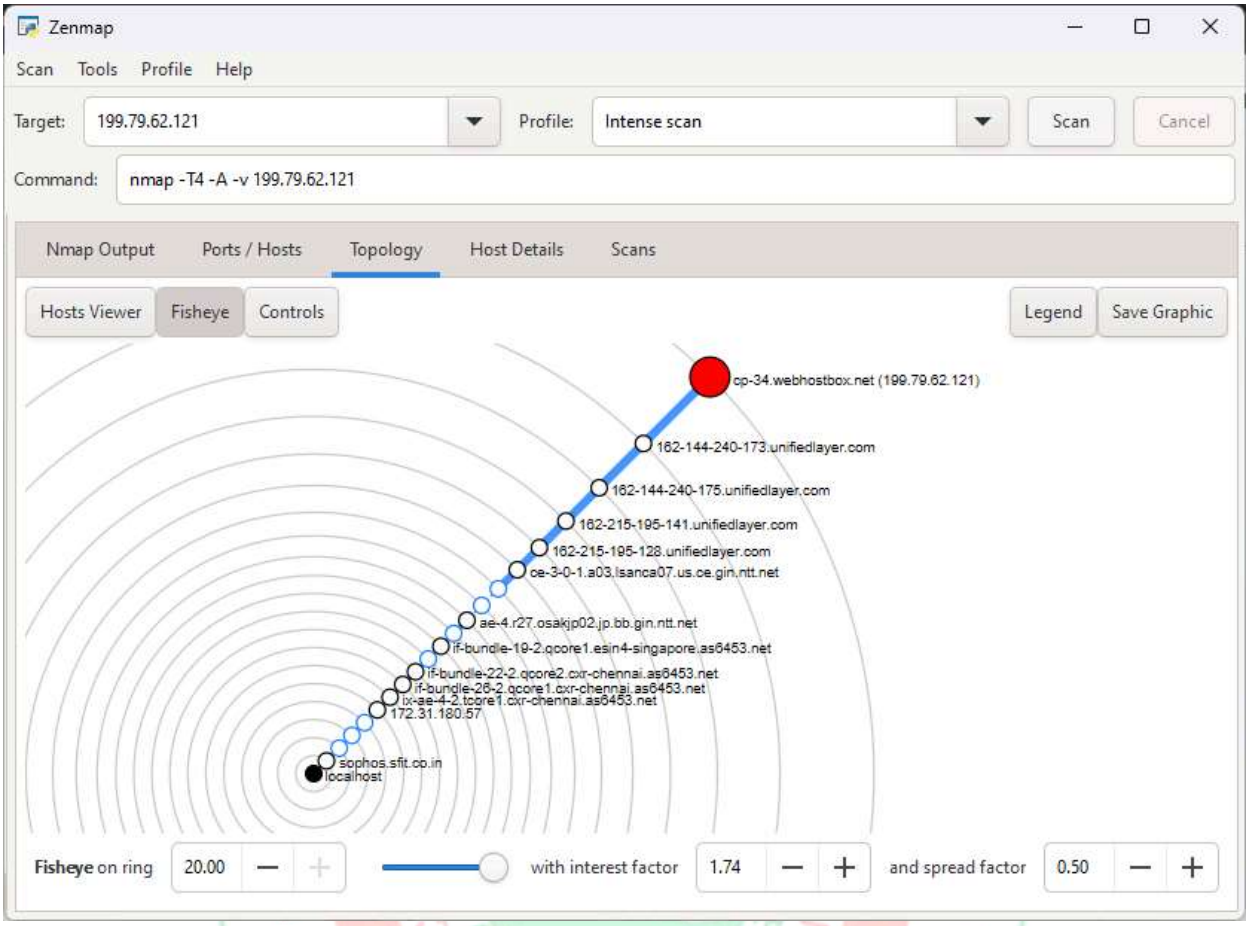
Intense Scan of Public IP of SFIT (199.79.62.121)



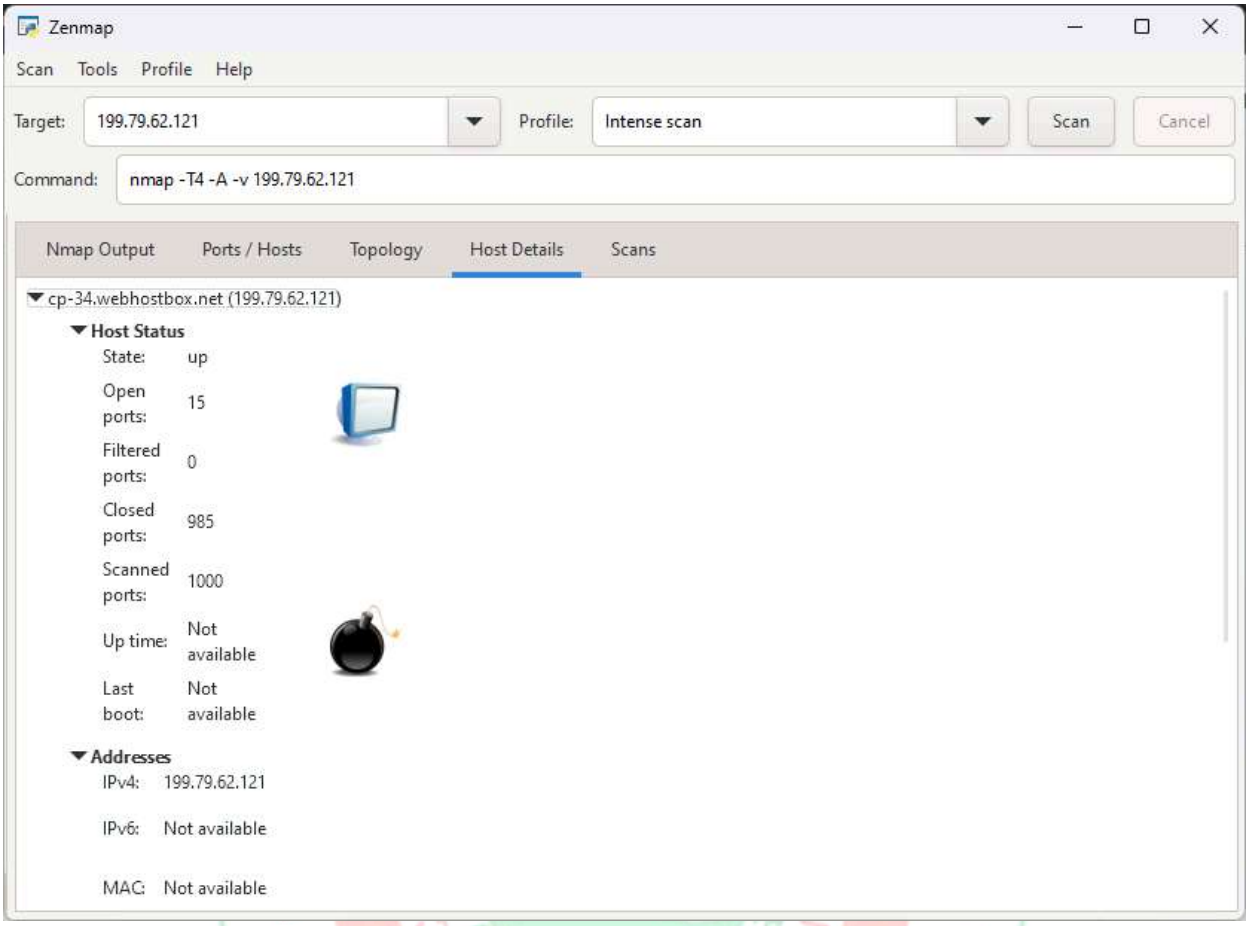




In Zenmap's "Ports/Hosts" tab, a Intense Scan of 199.79.62.121 shows 15 open ports. All services are active and reachable.



In Zenmap's topology view, localhost (your machine) is represented as a black dot, while 199.79.62.121 is shown as a red dot, indicating that the host is down or unresponsive. A dashed line connects the two, visually representing the network connection between your system and the target host. There are many white dots in between, representing intermediate devices or nodes on the network. A dashed line connects your system to the target host, visually illustrating the network path.



In Zenmap's "Host Details" for the intense scan, the target 199.79.62.121 shows that 15 ports are open while 985 ports are closed. A total of 1000 ports were scanned, with no available uptime .