EXPERIMENT 08

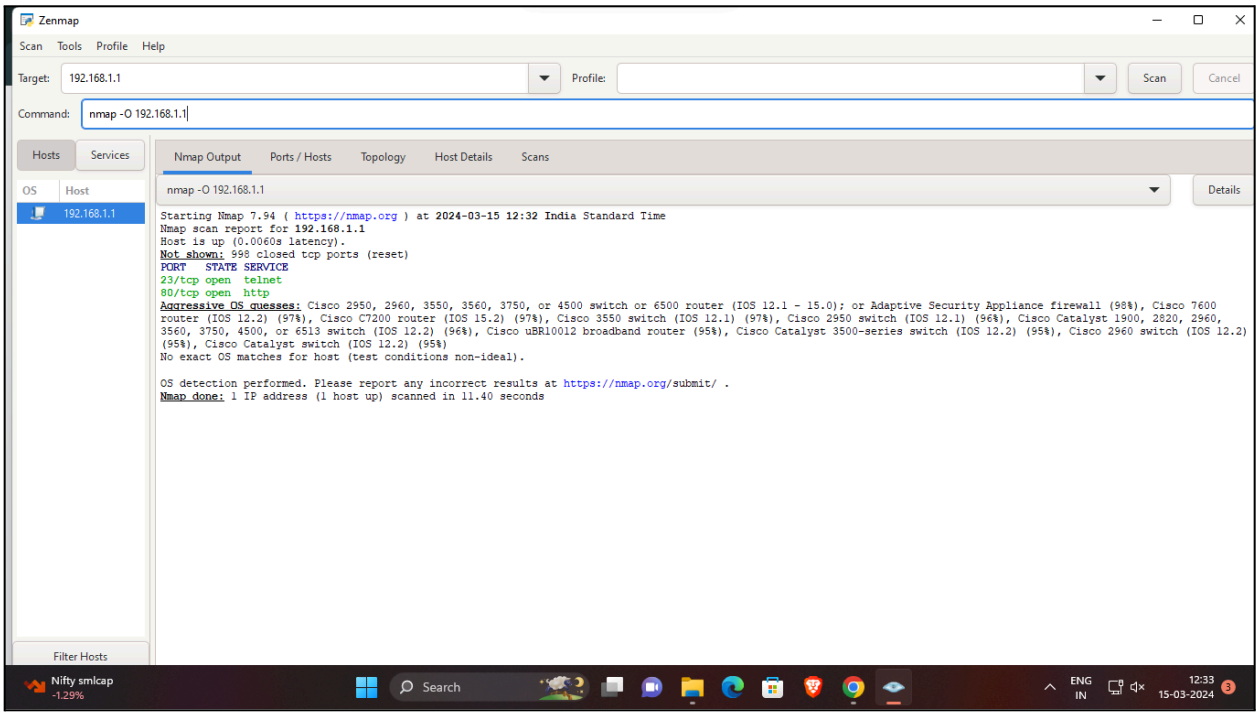
Aim:- Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, TCP port scan, UDP port scan, etc.

Theory:-

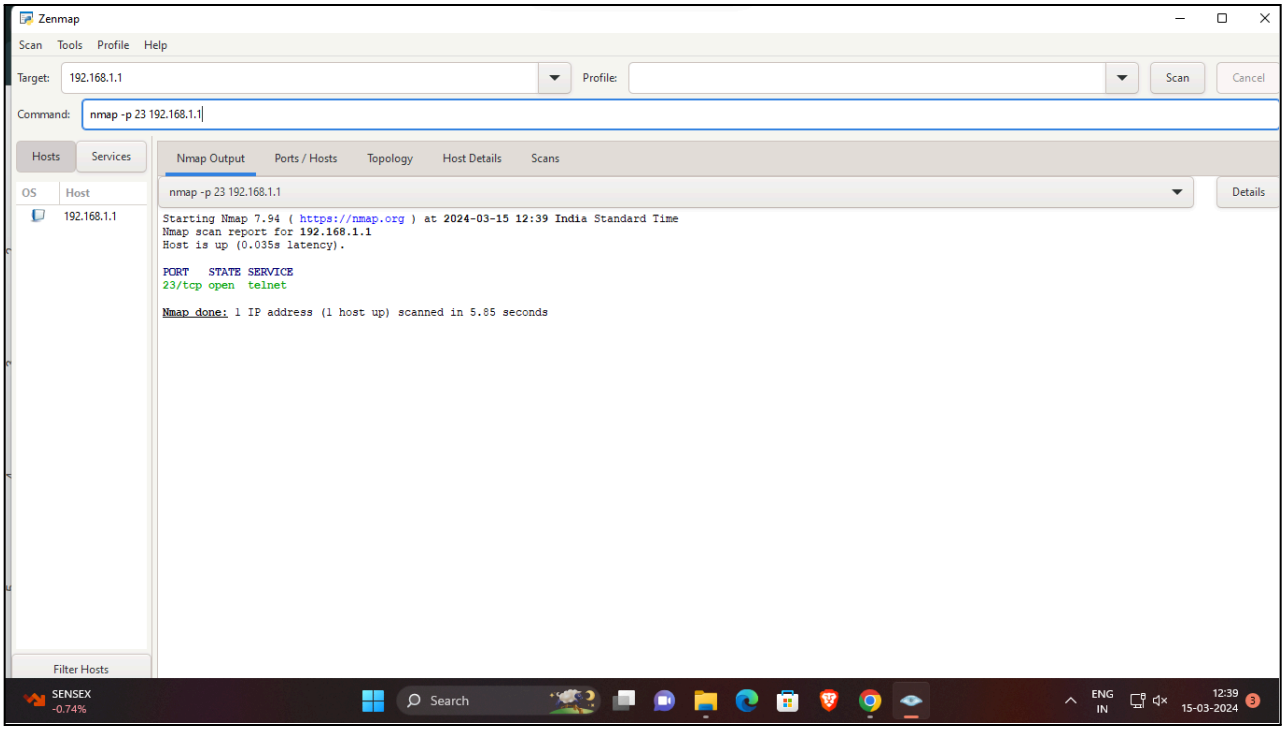
Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Nmap was named "Security Product of the Year" by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even featured in twelve movies, including The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, and The Bourne Ultimatum.

In order to perform scan on a particular IP address, use the following command:
Command: nmap 192.168.1.1 -O

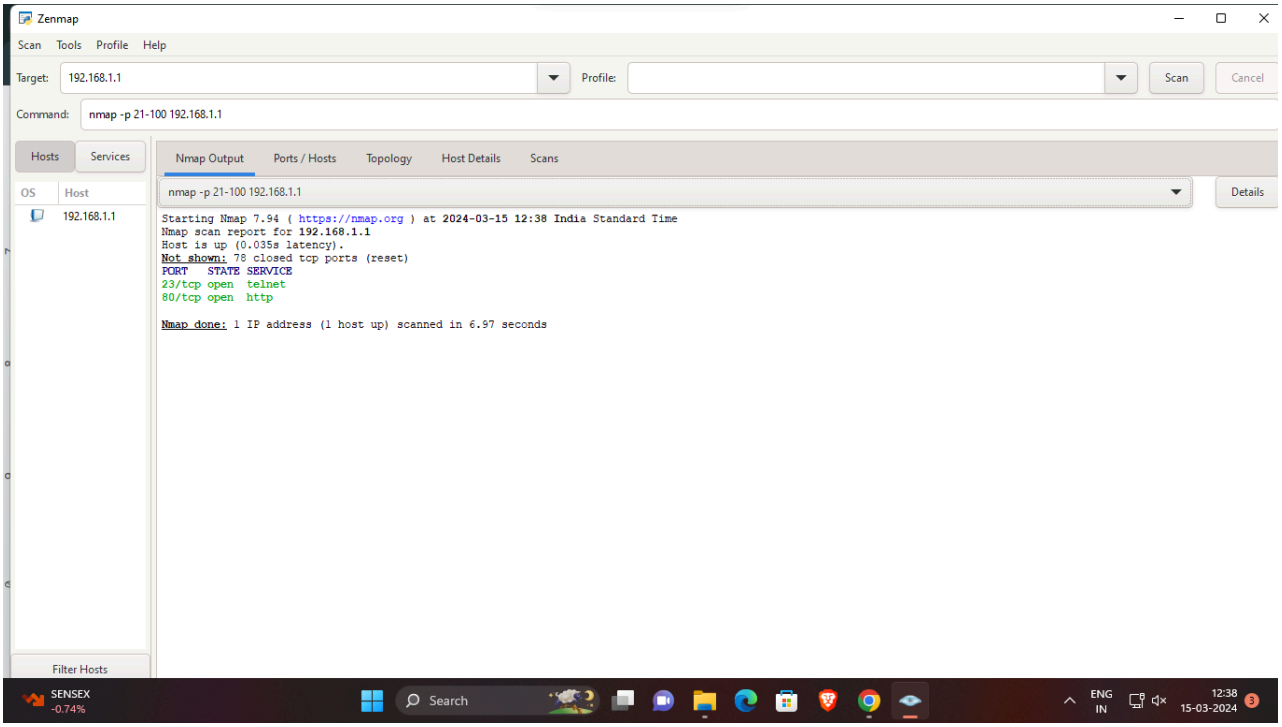


In order to scan a particular port, use the following command:
Command: nmap -p 23 192.168.1.1



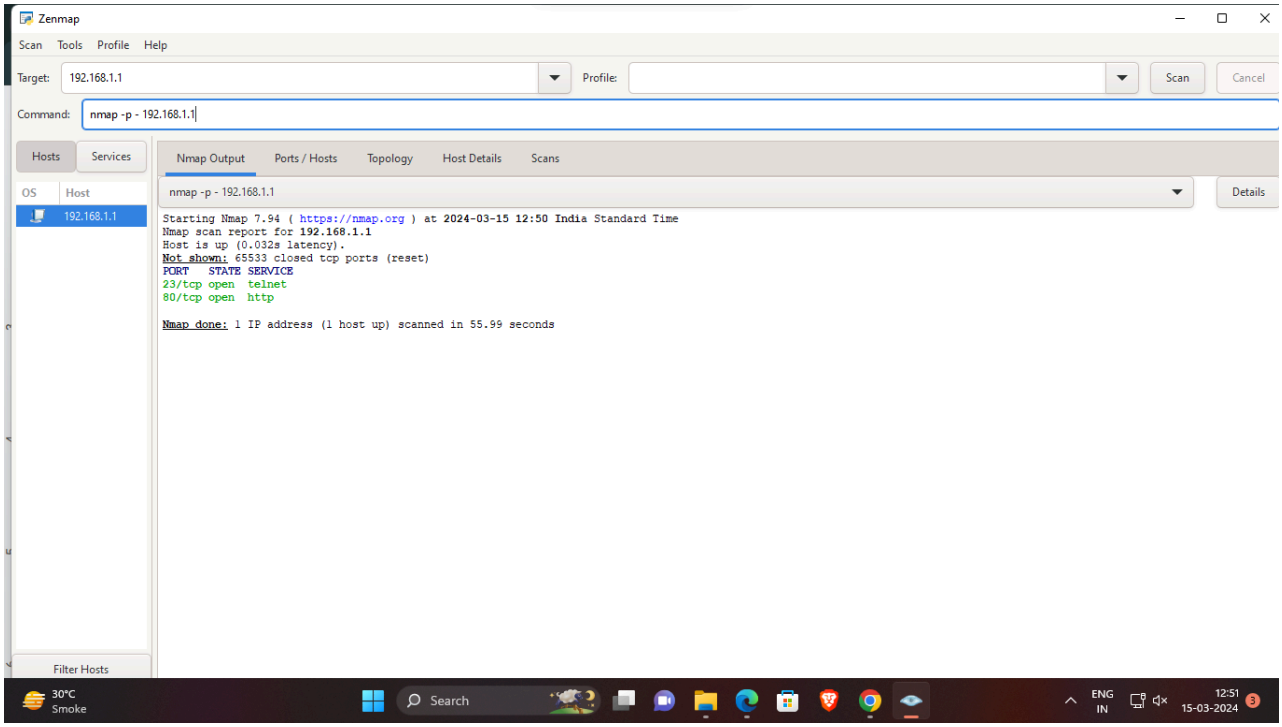
In order to scan range of IP, use the following command:

Command: nmap -p 21-100 192.168.1.1

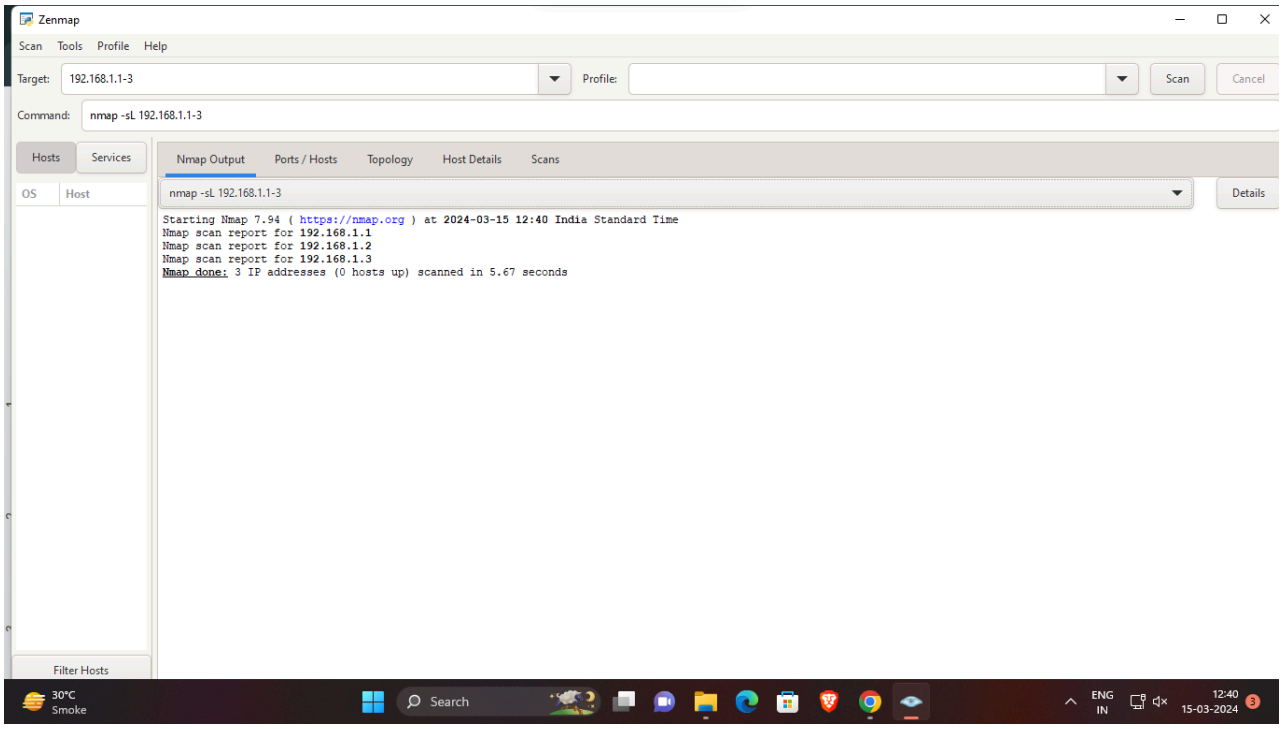


In order to scan available ports, use the following command:

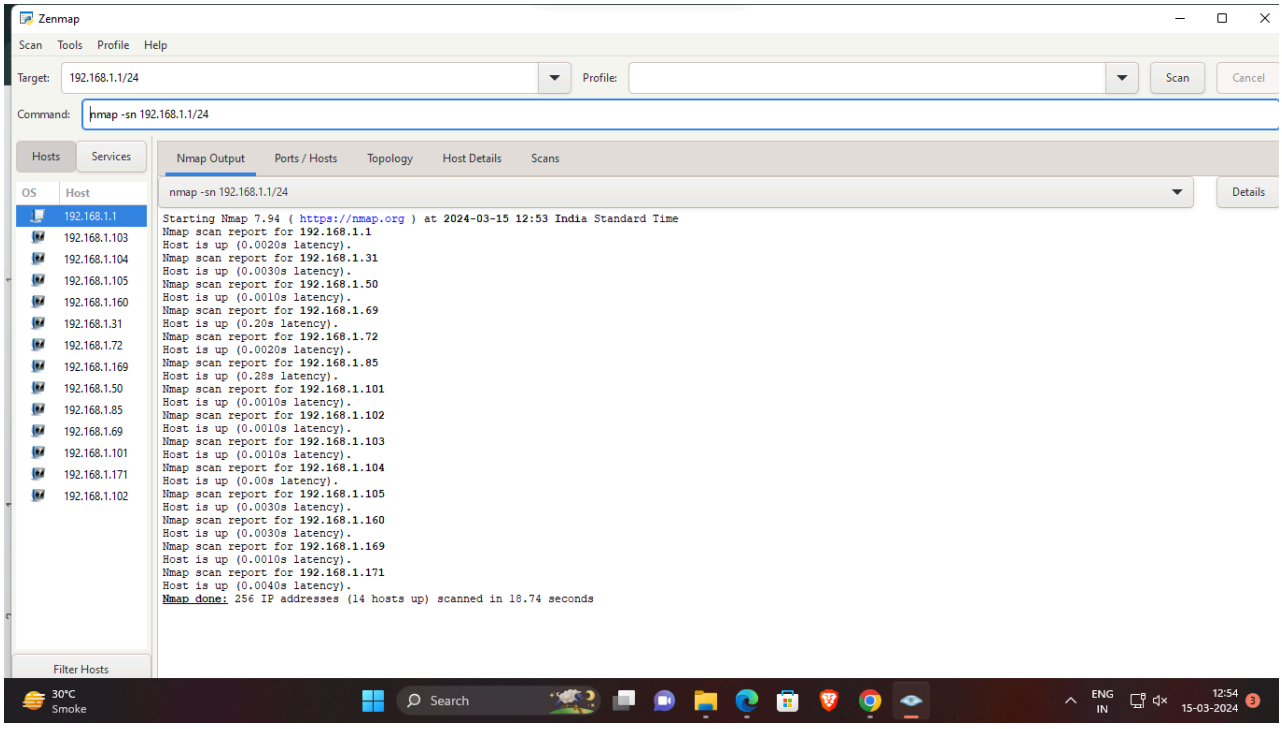
Command: nmap 192.168.1.1 -p-



In order to List Scan from port 1-3, use the following command:
Command: nmap 192.168.1.1-3 -sL



In order to disable port scan, use the following command:
Command: nmap 192.168.1.1/24 -sn



In order to disable Domain, use the following command:

Command: nmap vcet.edu.in