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:
What is Nmap?

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.

Download and install Nmap:
Here are the general steps to download and install it on different operating systems:

For Linux: Debian/Ubuntu-based systems:

Open a terminal and run the following commands:

For Windows:

1. Visit the official Nmap download page: https://nmap.org/download.html
2. Scroll down to the "Windows" section and locate the latest stable release.
3. Download the installer corresponding to your Windows version (32-bit or 64-bit).
4. Run the downloaded installer and follow the on-screen instructions to complete the installation.

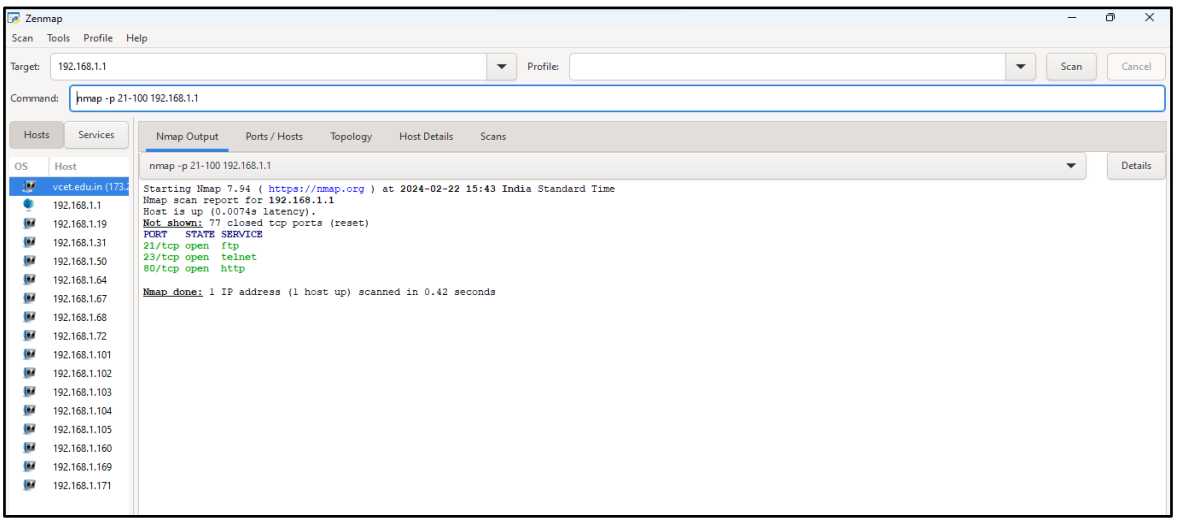
For Other Systems:

1. Visit the official Nmap download page: https://nmap.org/download.html
2. In the "Source Code" section, you can find the source code for Nmap. Follow the provided instructions for building and installing it on your system.
3. After installation, you can use Nmap from the command line. Open a terminal or command prompt and type nmap followed by the desired options and the target address.

Some common Commands used in Nmap are as follows:

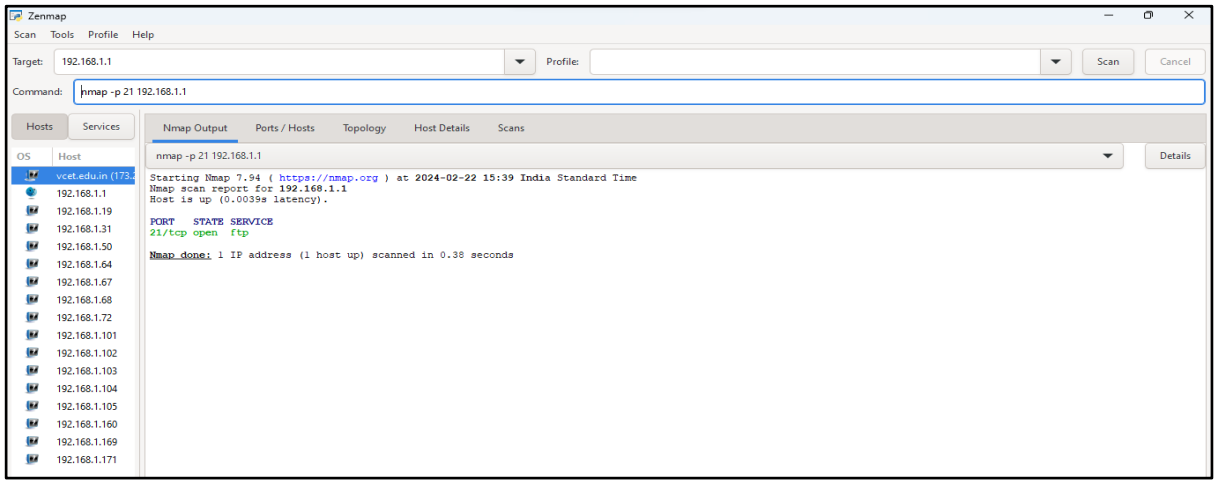
1. **To detect operating system:**
   The -O flag in this command instructs Nmap to perform operating system detection on the specified target. Nmap analyzes various network characteristics and responses to determine the likely operating system running on the target machine.
   Command: nmap -O 192.168.1.1

2. **To scan a specific port:**

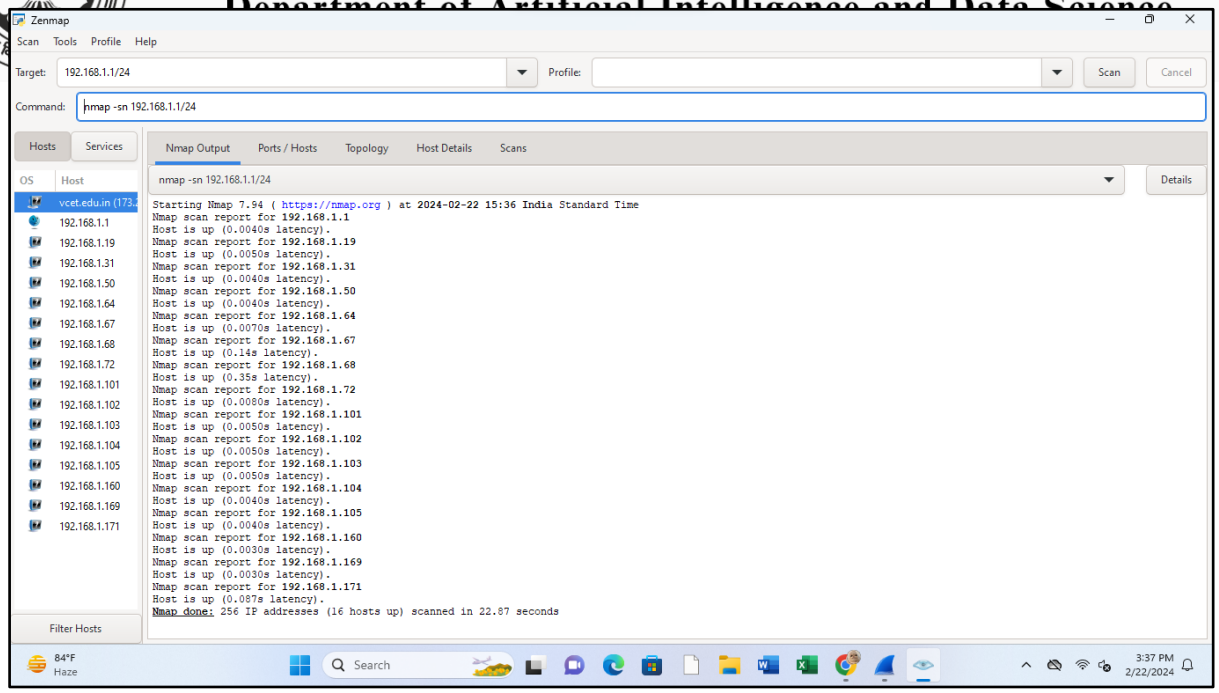


With the -p flag followed by a specific port number (in this case, 80), Nmap scans only that particular port on the target.
Command : nmap -p 21 192.168.1.1

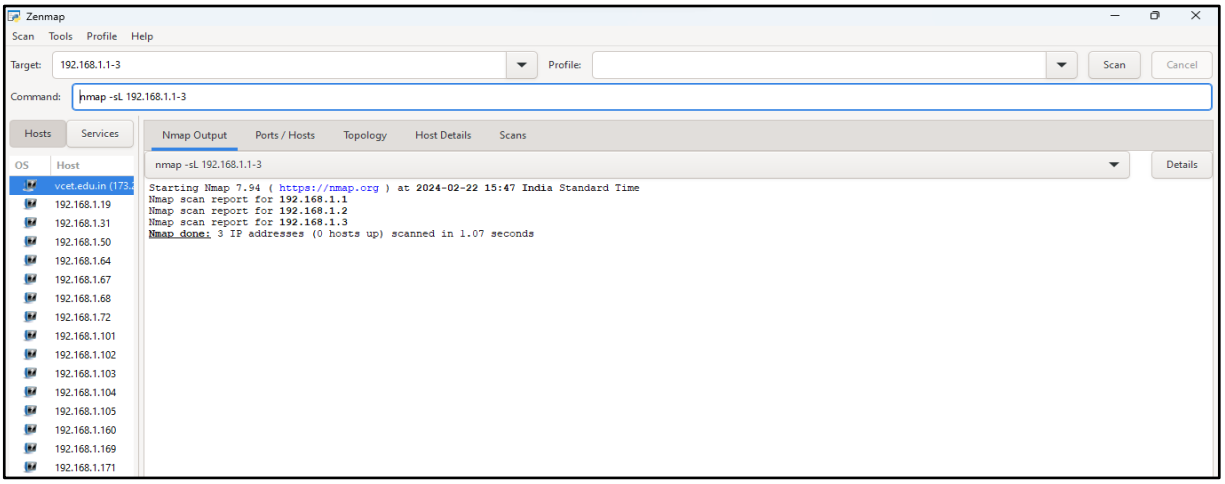
3. To scan a range of ports: The -p flag can also take a range of ports. This command scans ports from 1 to 100 on the target. It helps when you want to investigate a broader range of services.
   Command : nmap -p 21-100 192.168.1.1



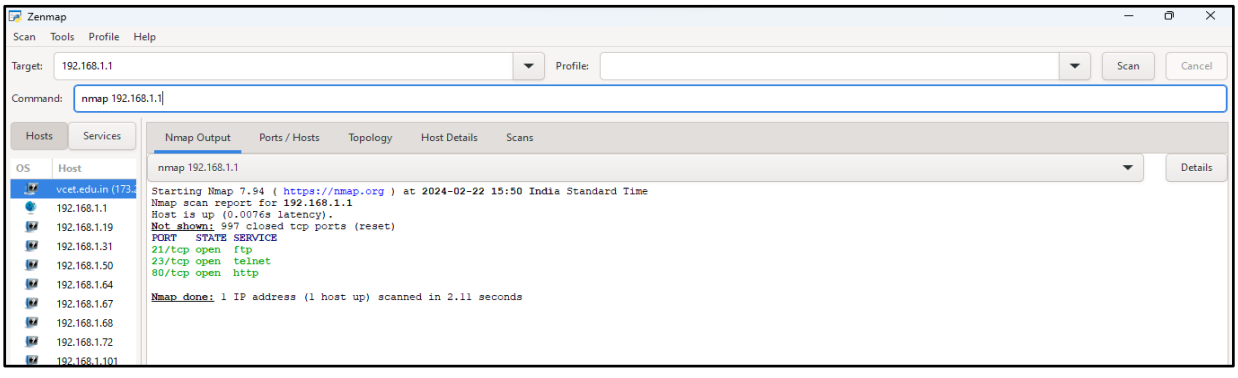
4. To scan all ports: The -p- flag scans all 65535 ports on the target. This comprehensive scan provides a thorough examination of all potential services running on the target.
   Command : nmap 192.168.1.1 -p-



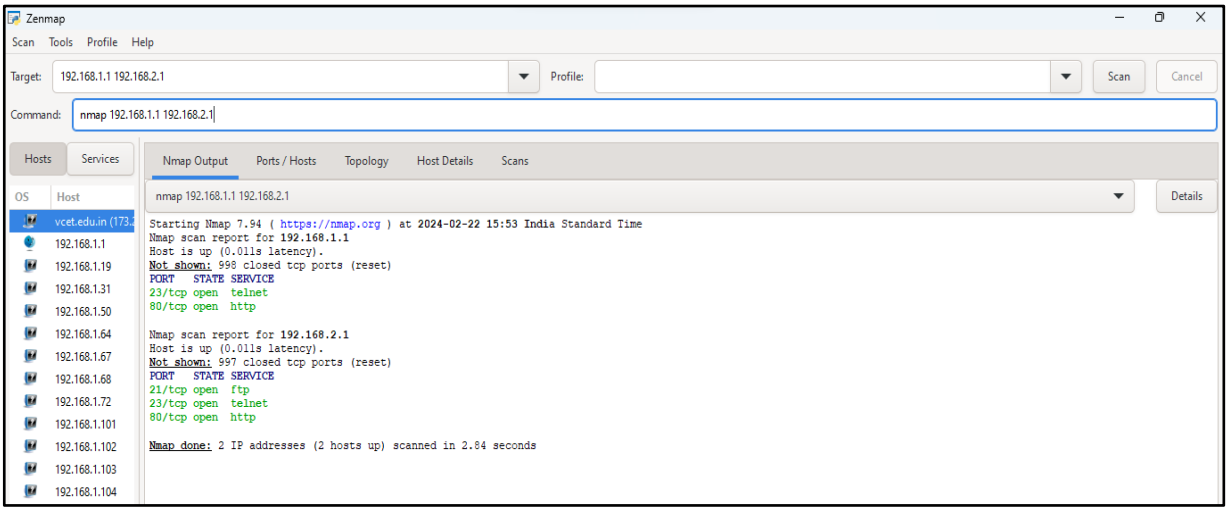
5. To list IP addresses when scanning: The -sn flag performs a ping scan without initiating a full port scan. It lists the IP addresses of hosts that respond to the ping within the specified network range (192.168.1.0/24 in this case).
Command : nmap 192.168.1.1-3 -sL



6. To perform a ping scan: This command exclusively performs a ping scan on the target. It sends ICMP echo requests to check the reachability of hosts without engaging in detailed port scanning.
Command: nmap 192.168.1.1

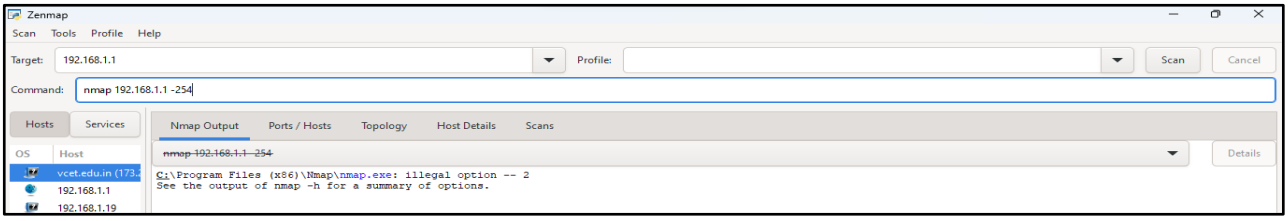


7. To perform a default scan: Without specifying additional flags, this command performs a default scan that includes host discovery, port scanning, service version detection, and operating system



detection. It provides a comprehensive overview of the target.

Command: nmap 192.168.1.1 192.168.2.1



8. To scan multiple Ip addresses:You can specify multiple targets on the command line, and Nmap will scan each of them individually. This is useful when scanning multiple systems.

Command: nmap 192.168.1.1 -254

9. To scan multiple Ip addresses(to scan specific Ip addresses) :

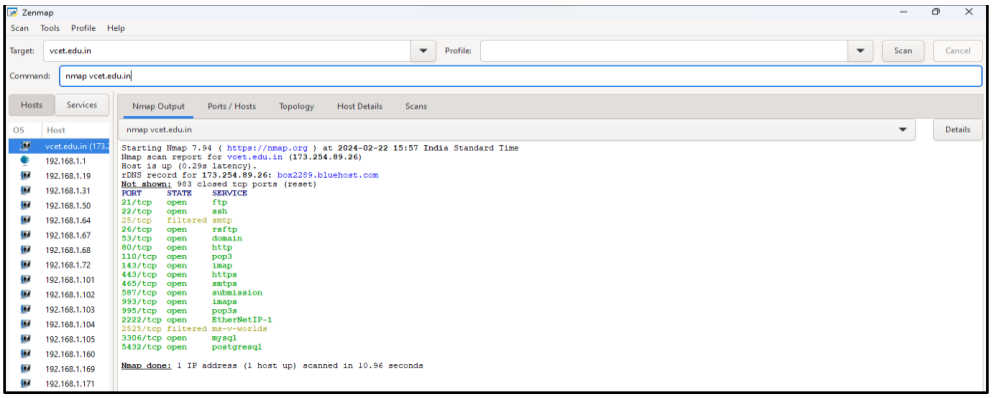
In order to scan multiple Ip addresses(to scan specific Ip addresses we use the command

Command: nmap 192.168.1.1,192.168.1.2.

10. To scan a domain :

    When a domain name is provided, Nmap first resolves it to an IP address and then performs a scan on the resulting IP. This is useful for discovering the open ports on a server associated with the given domain.

    Command : nmap example.com



Conclusion :

we explored Nmap, a versatile network discovery and security auditing tool. Nmap enables users to scan networks, detect open ports, perform OS fingerprinting, and much more. By leveraging raw IP packets, Nmap can gather detailed information about hosts, services, and operating systems on a network. Its cross-platform support and rich feature set make it indispensable for network administrators, security professionals, and researchers. Through various commands like scanning specific ports, performing ping scans, and conducting comprehensive network scans, Nmap provides valuable insights into network topology and security posture.