There are several open source software tools that can be used to scan a network and discover everything connected to it. One such tool is Nmap (Network Mapper), which is a free and open source utility for network exploration, administration, and security auditing.

Here are the steps to use Nmap to scan your network and retrieve information about what's connected:

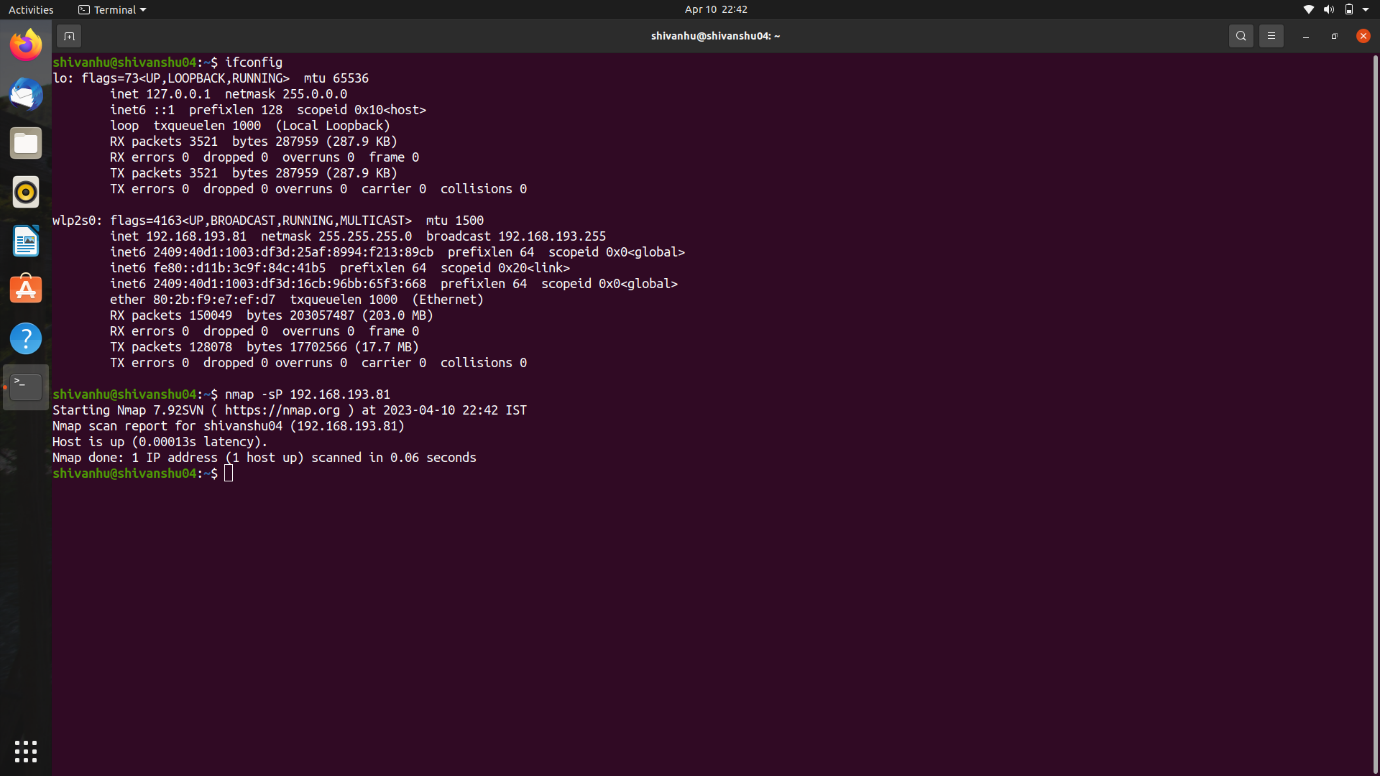
1. Install Nmap: If you're using a Linux-based operating system, you can install Nmap using your distribution's package manager. For example, on Ubuntu, you can use the command **sudo apt-get install nmap**. If you're using Windows, you can download Nmap from the official website at <https://nmap.org/download.html>.

Text

Description automatically generated

**ifconfig** is a command-line utility in Linux and Unix operating systems that is used to display information about network interfaces, such as their IP addresses, netmasks, and hardware addresses (MAC addresses).

To use **ifconfig**, open a terminal window and type the command followed by the name of the network interface you want to display information about. If you don't specify an interface name, **ifconfig** will display information for all



Our IP address is: 192.168.193.81

Scan the network: Once you have Nmap installed, you can use it to scan your network by running the following command in a terminal or command prompt:

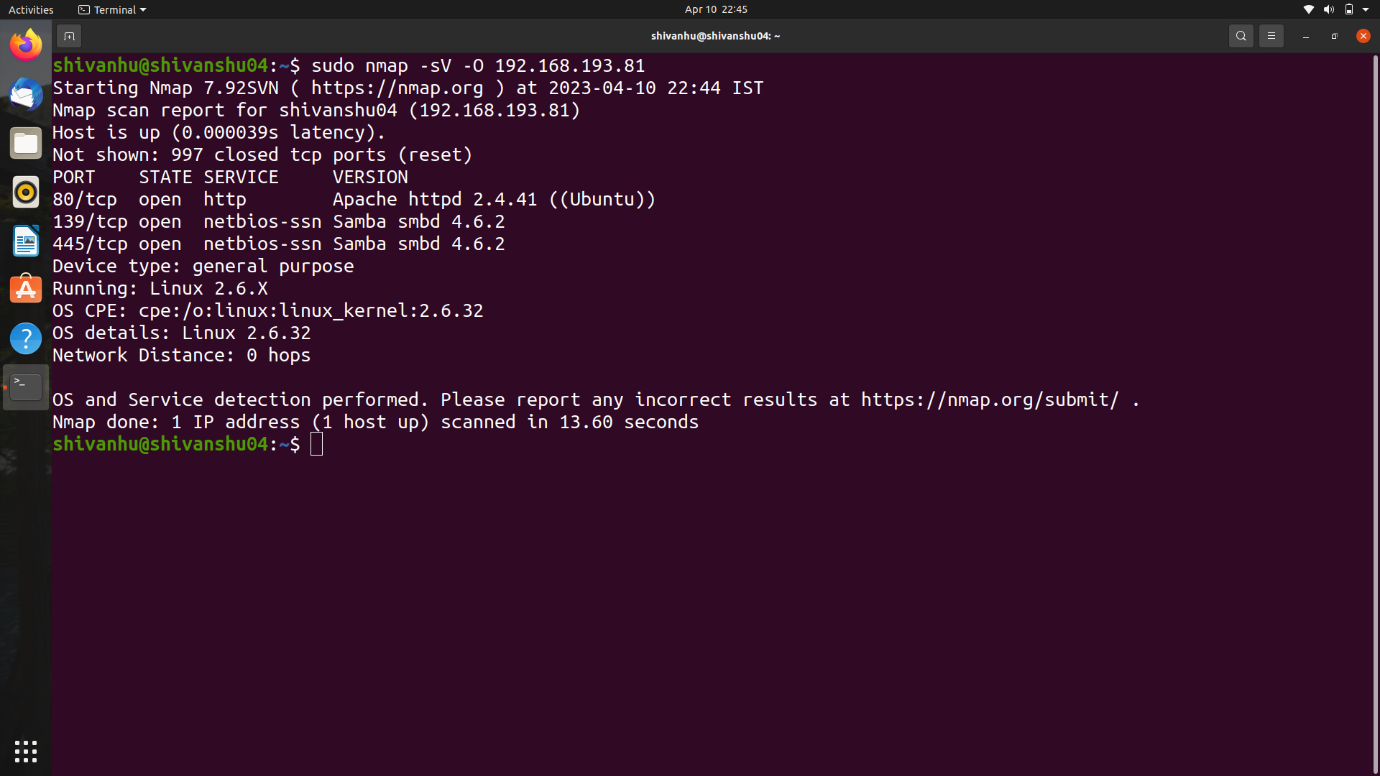
nmap -sP 192.168.193.81

Replace 192.168.193.81 with the IP address range of your network. This will scan all the hosts in the range and report which ones are up.

1. Retrieve hostnames and OS information: Once you know which hosts are up, you can use Nmap to retrieve more information about each one. For example, to scan for hostnames and identify the operating system of each host, you can run the following command:

nmap -sV -O 192.168.193.81

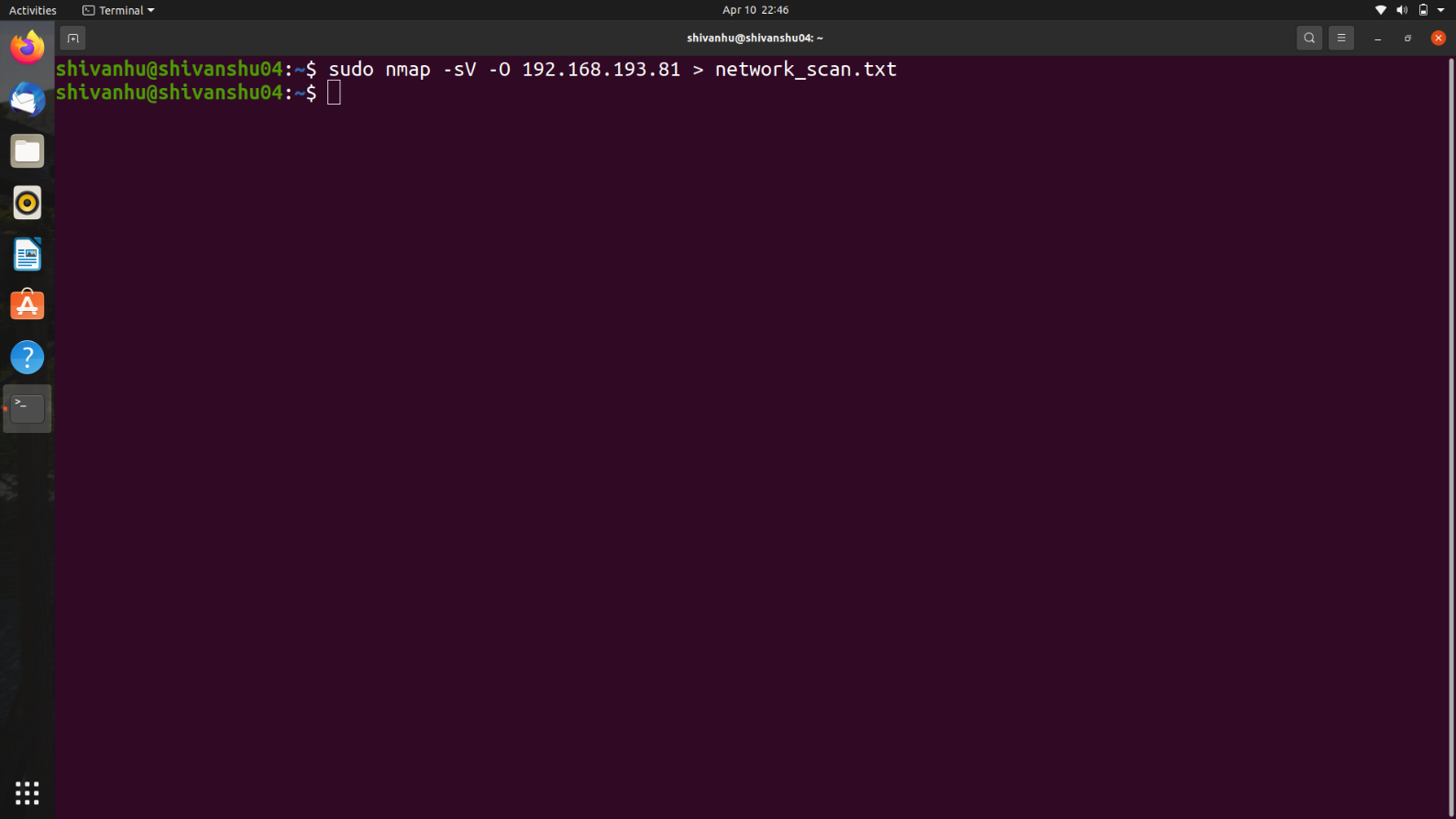
This will not only retrieve the hostname and OS information, but it will also scan for the services each host is operating and report any open ports.

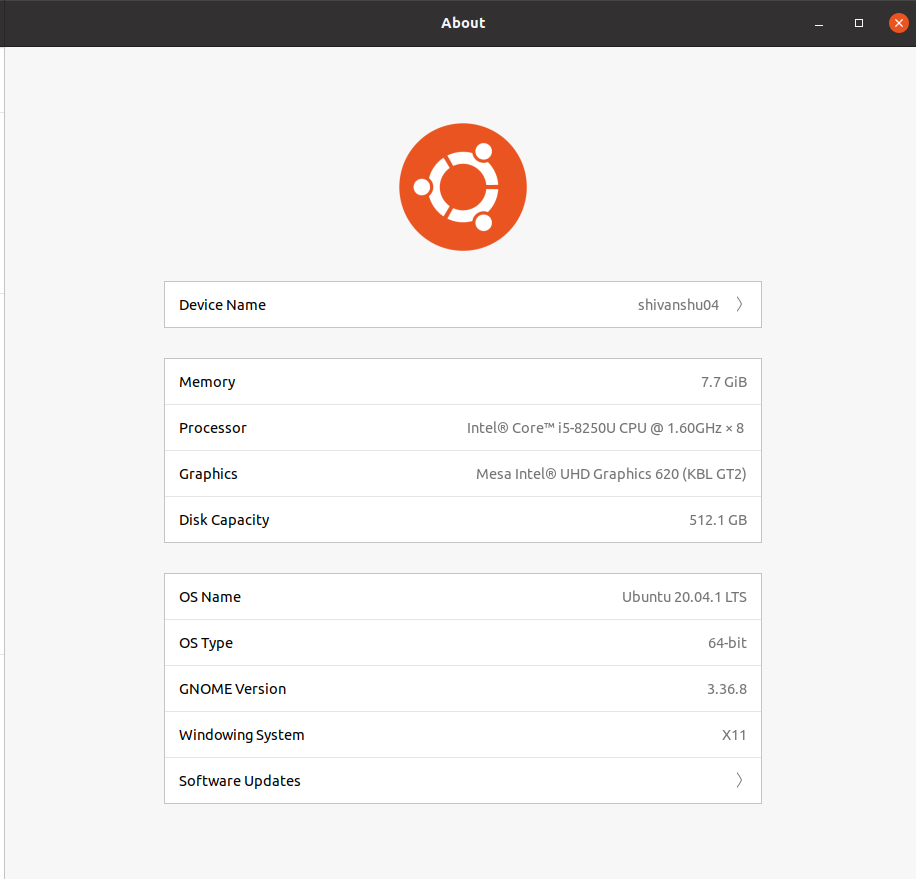


Save the output to a text file: To save the output to a text file, you can redirect the output of the command to a file using the **>** symbol. For example:

nmap -sV -O 192.168.1.0/24 > network\_scan.txt

This will save the output to a file named **network\_scan.txt** in the current directory.





Device Name: shivanshuo4

Memory: 1 TCB (exact memory capacity not specified)

Processor: Intel Core i5-8250U CPU @ 1.8 GHz (4 cores, 8 threads)

Graphics: Mesa Intel UHD Graphics 620 (KBL CT2)

Disk Capacity: 512.1 GB

OS Name: Ubuntu 20.04.1 LTS OS

Type: 64-bit GNOME Version: 3.36.8

This information gives an overview of the main hardware components and software specifications of your device.