

# **CA 3 – PROJECT**

## **INT 301 - OPENSOURCE TECHNOLOGIES**

Kuldeep Singh Shekhawat  
11915005

### **1. Introduction:**

Network security has assumed an increasingly critical role in our fast-paced modern society, in which technology has become an inseparable component of our everyday lives. Because of the increasing sophistication and complexity of networks, it is very necessary to have a complete awareness of all of the devices that are linked to the network. Network scanning tools have evolved as a strong option that may assist in the accomplishment of this objective. These tools enable users to gather a large variety of information on each connected device, such as the operating systems, hostnames, and services that are installed on those devices.

This research will investigate the usage of open source software for network scanning, focusing on the programme's capacity to give in-depth insights about the topology, services, and hosts of a network. The study will go into the specifics of installing and configuring a network scanning tool, as well as illustrate how to make the most of it in order to do an efficient scan of a network. In addition to this, the report will include concrete instructions on how to list all of the connected hosts in a text file and how to determine the operating system that is used by each host.

The readers of this study will come away from it with a more in-depth comprehension of the essential function that network scanning serves to serve in the improvement of network security. In addition to this, they will learn the knowledge and abilities necessary to make efficient use of open source software in order to scan networks, identify devices, and extract essential information. This research, in its whole, offers a complete guide to network scanning via the use of open source software. The insights included within this paper may be utilised by individuals as well as organisations in order to defend their networks against possible threats.

#### **1.1 Objective of the project**

Use of any open source software to scan your network and discover everything connected to it, retrieve variety of information about what's connected, what services each host is operating, scan the hostname, list all the hosts in a text file, identify a host's operating system (OS).

#### **1.2 Description of the project**

You will be able to do a full analysis of your network and get a detailed report on all of the devices that are presently connected to it if you use software that is available under an open source licence for network scanning. The programme was developed to gather a broad variety of data points, such as the exact services that are being operated by each device, the hostname that is linked with each device, and the operating system (OS) that is powering it. After you have

scanned your network, the programme will be able to provide a comprehensive list of all the devices that are presently connected to it. This list can then be saved as a text file and analysed at a later time. You will be able to acquire useful insights on the topology of your network and discover any possible security threats that may be present if you make use of this open source software.

### 1.3 Scope of the project

It is possible for a project to have a highly comprehensive scope when it makes use of open source software for network scanning and device identification. The scope of such a project is determined by the particular objectives and prerequisites of the undertaking. The following are some potential areas on which to concentrate:

**Security of the network:** The major objective of the project could be to determine whether or not the network has any vulnerabilities or potential security issues. This might entail scanning for open ports or unprotected services, identifying old software versions or firmware, or detecting any unauthorised devices that have joined to the network. Alternatively, it could involve finding any outdated software versions or firmware.

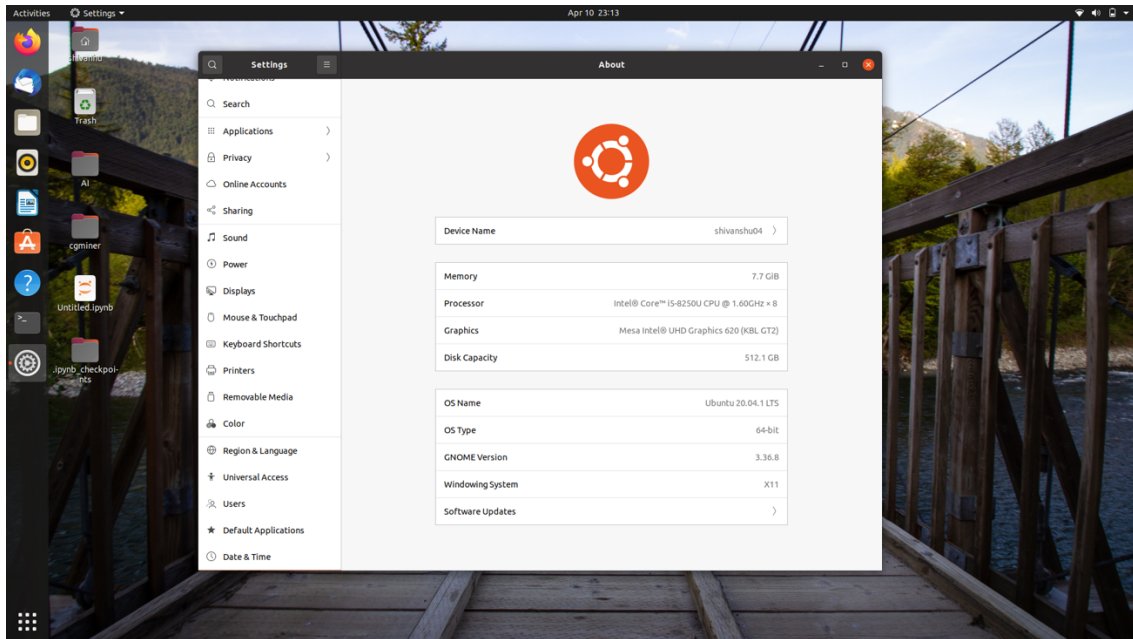
**Management of the network's inventory:** The project may also be used to compile an exhaustive inventory of all devices that are connected to the network. This inventory would include the devices' makes and models, as well as the software versions and physical locations of each item. The management of hardware and software assets, the identification of devices that are no longer in use, and the planning of future network improvements might all benefit from this information.

**Network troubleshooting and optimisation:** The project might be used to discover bottlenecks or other performance problems inside the network, such as devices that are consuming an excessive amount of bandwidth or services that are operating inefficiently. One example of a performance issue is a device that is using an excessive amount of bandwidth. This information may be put to use to enhance both the performance of the network and the system as a whole.

**Compliance and regulation:** The goal of the project might be to ensure that the network complies with a set of compliance standards or fulfils the requirements of the regulatory agency. For instance, if the network has devices that deal with sensitive data, the project might be used to guarantee that all security standards are followed and that the devices are correctly set to guard against data breaches. This would be useful in situations where the network already contains devices that deal with sensitive data.

In general, the aims and needs of the organisation or the person who is performing the network scan will determine the extent to which the project will be carried out. The findings of the scan may give useful insights into the current condition of the network and may also assist in identifying sections of the system that might want improvement as well as possible vulnerabilities.

## 2. System Description



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.

### 3. Analysis Report

Starting Nmap 7.92SVN ( <https://nmap.org> ) at 2023-04-10 22:46 IST

Nmap scan report for shivanshu04 (192.168.193.81)

Host is up (0.000036s latency).

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.41 ((Ubuntu))

139/tcp open netbios-ssn Samba smbd 4.6.2

445/tcp open netbios-ssn Samba smbd 4.6.2

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6.32

OS details: Linux 2.6.32

Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds

#### Explanation:

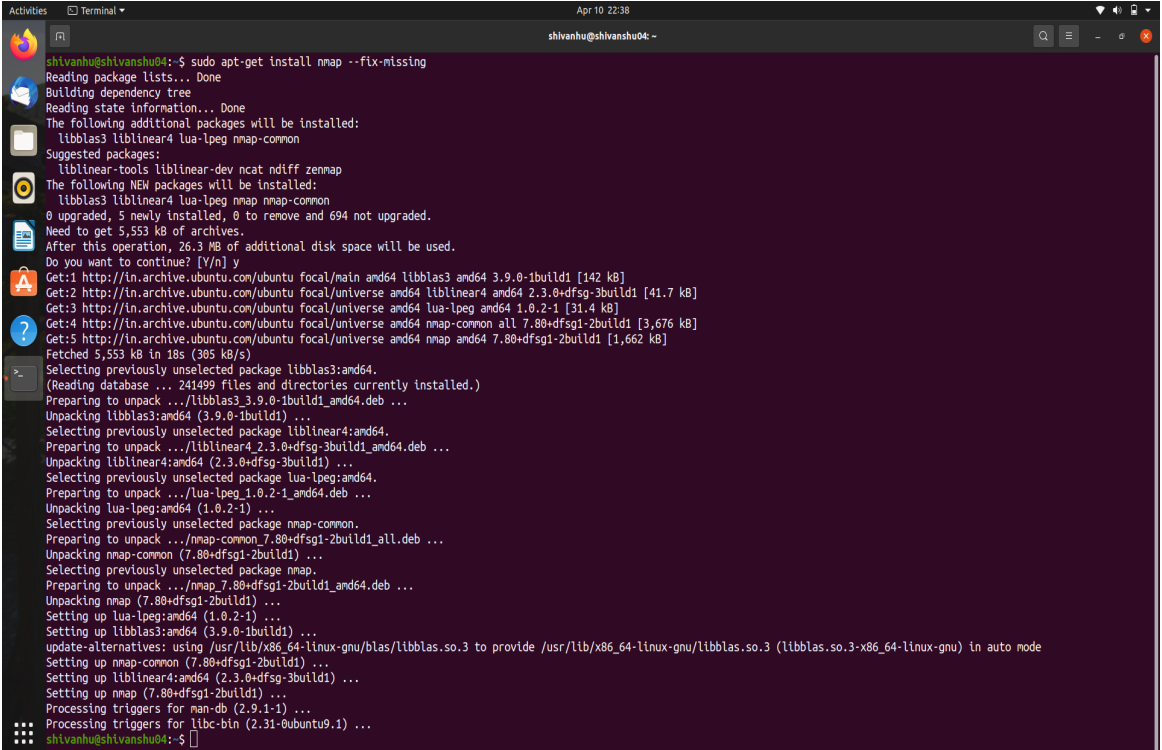
- The Nmap scan report shows that a device with the hostname "shivanshu04" and IP address "192.168.193.81" is up and responsive.
- It also shows that there are three open ports on this device, which are TCP ports 80 (used for HTTP), 139 and 445 (used for NetBIOS over TCP/IP protocol).
- Nmap has also detected that this device is running Apache httpd 2.4.41 on port 80, and Samba smbd 4.6.2 on ports 139 and 445.
- Furthermore, Nmap has identified the device as a general purpose device running Linux 2.6.X, with an operating system Common Platform Enumeration (OS CPE) of cpe:/o:linux:linux\_kernel:2.6.32.
- Overall, this scan has provided valuable information about the connected device, including its IP address, open ports, running services and operating system.

### 3.1 System snapshots and full analysis report

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:

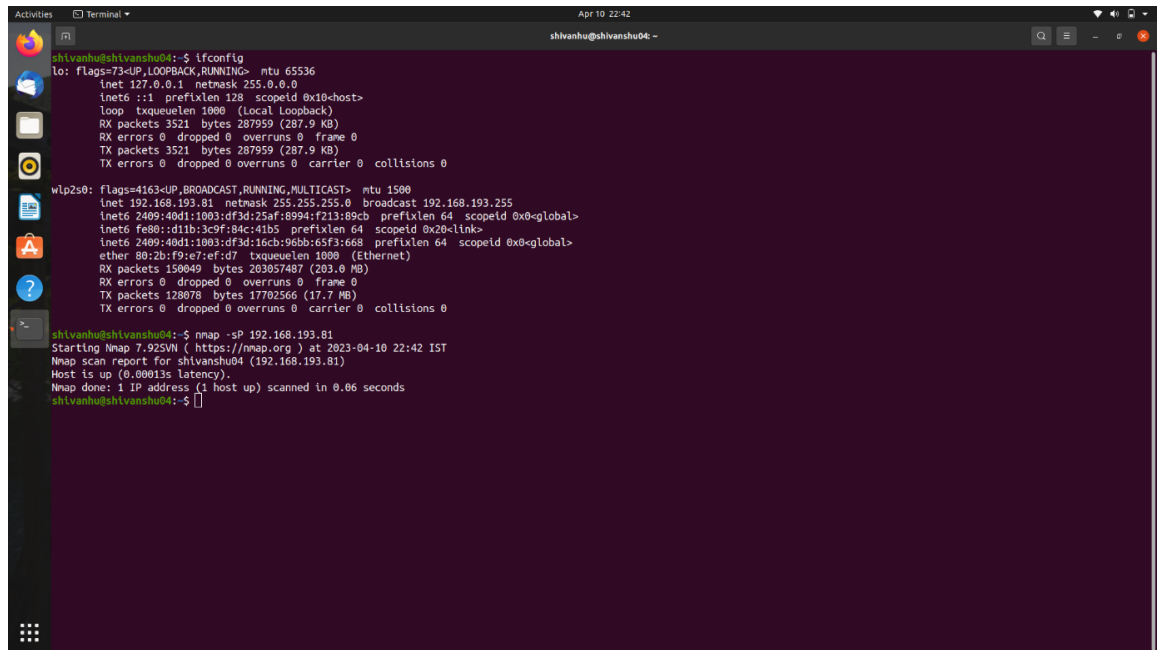
1. **Install Nmap:** If you're using a Linux-based operating system, you can install Nmap using your distribution's package manager. For example, on Ubuntu, you can use the command `sudo apt-get install nmap --fix-missing`. If you're using Windows, you can download Nmap from the official website at 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

A screenshot of a terminal window on a Linux system. The terminal shows the command `sudo apt-get install nmap --fix-missing` being executed. The output displays the process of reading package lists, building a dependency tree, and installing the requested package along with its dependencies. It lists the additional packages to be installed (libblas3, liblinear4, lua-lpeg, nmap-common), suggested packages (liblinear-tools, liblinear-dev, ncat, ndiff, zenmap), and the new packages to be installed. It also shows the disk space requirements and the progress of downloading and unpacking the packages. The terminal output ends with the command prompt `shivanhu@shivanhu04:~$`.

```
shivanhu@shivanhu04:~$ sudo apt-get install nmap --fix-missing
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 lua-lpeg nmap nmap-common
0 upgraded, 5 newly installed, 0 to remove and 694 not upgraded.
Need to get 5,553 kB of archives.
After this operation, 26.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libblas3 amd64 3.9.0-1build1 [142 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 liblinear4 amd64 2.3.0+dfsg-3build1 [41.7 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 lua-lpeg amd64 1.0.2-1 [31.4 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 nmap-common all 7.80+dfsg1-2build1 [3,676 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 nmap amd64 7.80+dfsg1-2build1 [1,662 kB]
Fetched 5,553 kB in 18s (305 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 241499 files and directories currently installed.)
Preparing to unpack .../libblas3_3.9.0-1build1_amd64.deb ...
Unpacking libblas3:amd64 (3.9.0-1build1) ...
Selecting previously unselected package liblinear4:amd64.
Preparing to unpack .../liblinear4_2.3.0+dfsg-3build1_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-3build1) ...
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../lua-lpeg_1.0.2-1_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-1) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../nmap-common_7.80+dfsg1-2build1_all.deb ...
Unpacking nmap-common (7.80+dfsg1-2build1) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.80+dfsg1-2build1_amd64.deb ...
Unpacking nmap (7.80+dfsg1-2build1) ...
Setting up lua-lpeg:amd64 (1.0.2-1) ...
Setting up libblas3:amd64 (3.9.0-1build1) ...
update-alternatives: using /usr/lib/x86_64-linux-gnu/blas/libblas.so.3 to provide /usr/lib/x86_64-linux-gnu/libblas.so.3 (libblas.so.3-x86_64-linux-gnu) in auto mode
Setting up nmap-common (7.80+dfsg1-2build1) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-3build1) ...
Setting up nmap (7.80+dfsg1-2build1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.1) ...
shivanhu@shivanhu04:~$
```

2. **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.

A terminal window with a dark purple background. The user is at a prompt 'shlvanshu@shlvanshu04:~'. They run 'ifconfig' which shows details for 'lo' and 'wlp2s0'. Then they run 'nmap -sP 192.168.193.81'. The output shows Nmap version 7.92SVN, the scan time, and a report for 'shlvanshu04 (192.168.193.81)' stating the host is up with 0.00013s latency. The prompt returns to '\$'.

```
shlvanshu@shlvanshu04:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (local loopback)
    RX packets 3521 bytes 287959 (287.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3521 bytes 287959 (287.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.193.81 netmask 255.255.255.0 broadcast 192.168.193.255
    inet6 2409:40d1:1003:df3d:25af:8994:f213:89cb prefixlen 64 scopeid 0x0<global>
    inet6 fe80::d11b:3c9f:84c:41b5 prefixlen 64 scopeid 0x20<link>
    inet6 2409:40d1:1003:df3d:16cb:96bb:65f3:668 prefixlen 64 scopeid 0x0<global>
    ether 80:2b:f9:e7:ef:d7 txqueuelen 1000 (Ethernet)
    RX packets 150649 bytes 203857407 (203.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 128878 bytes 17702566 (17.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

shlvanshu@shlvanshu04:~$ nmap -sP 192.168.193.81
Starting Nmap 7.92SVN ( https://nmap.org ) at 2023-04-10 22:42 IST
Nmap scan report for shlvanshu04 (192.168.193.81)
Host is up (0.00013s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
shlvanshu@shlvanshu04:~$
```

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:

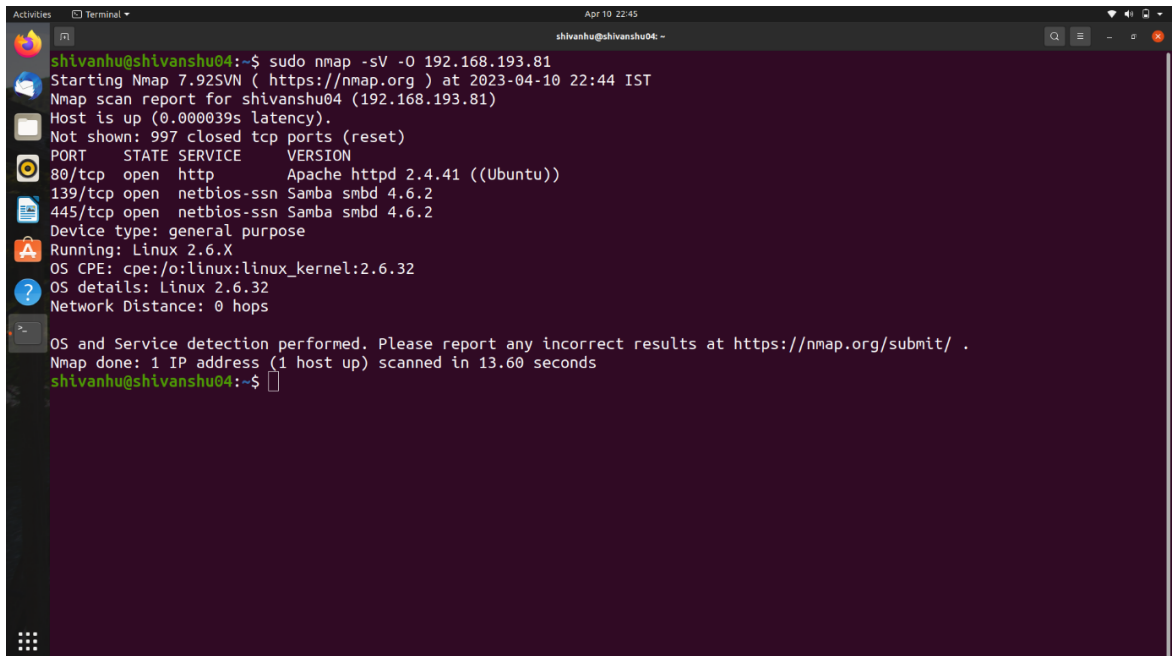
**nmap -sP 192.168.193.81**

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.

3. 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.

A terminal window with a dark purple background. The prompt is 'shivanhu@shivanshu04:~\$'. The command 'sudo nmap -sV -O 192.168.193.81' has been executed. The output shows the Nmap scan report for shivanshu04 (192.168.193.81). It indicates the host is up, shows open ports (80, 139, 445) and their services (http, netbios-ssn, Samba), and provides OS details (Linux 2.6.32).

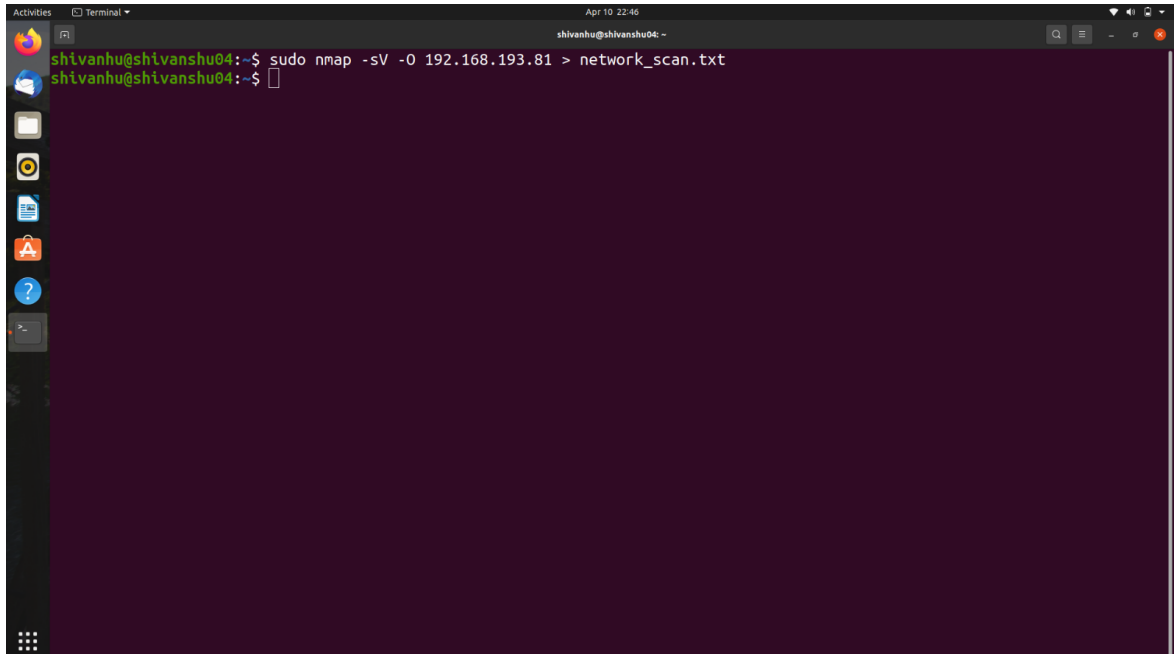
```
shivanhu@shivanshu04:~$ sudo nmap -sV -O 192.168.193.81
Starting Nmap 7.92SVN ( https://nmap.org ) at 2023-04-10 22:44 IST
Nmap scan report for shivanshu04 (192.168.193.81)
Host is up (0.000039s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Apache httpd 2.4.41 ((Ubuntu))
139/tcp   open  netbios-ssn    Samba smbd 4.6.2
445/tcp   open  netbios-ssn    Samba smbd 4.6.2
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds
shivanhu@shivanshu04:~$
```

4. 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.

A terminal window with a dark purple background. The prompt is 'shivanhu@shivanshu04:~\$'. The command 'sudo nmap -sV -O 192.168.193.81 > network\_scan.txt' has been entered, and the prompt is now 'shivanhu@shivanshu04:~\$' again, indicating the command has been executed.

```
shivanhu@shivanshu04:~$ sudo nmap -sV -O 192.168.193.81 > network_scan.txt
shivanhu@shivanshu04:~$
```

#### 4. Reference

- <https://phoenixnap.com/kb/how-to-install-nmap-ubuntu>
- <https://www.herzing.edu/blog/what-network-security-and-why-it-important>
- <https://nmap.org/>
- <https://nmap.org/book/man.html>
- <https://nmap.org/download.html>
- <https://www.comparitech.com/net-admin/find-network-devices/>
- <https://www.dummies.com/article/technology/computers/operating-systems/windows/windows-10/see-devices-connected-windows-10-computer-230424/>
- <https://www.ghacks.net/2007/01/29/find-out-which-devices-have-been-connected-to-your-pc/>
- <https://itsfoss.com/list-usb-devices-linux/>
- <https://sourcedigit.com/22048-how-to-list-connected-usb-devices-in-linux-ubuntu/>