LOVELY PROFESSIONAL UNIVERSITY

Academic Task-3 (Compulsory)

INT301: Open Source Technologies

NAME- HARDEEP SINGH
SECTION-KE009
ROLL-NO-27
REGISTRATION NUMBER-11909238
GITHUB LINK- https://github.com/hardeep809/OpenSource-Project

TOPIC- "use 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) INTRDUCTION

1.1) Objective of the Project

The objective of this project is to perform a thorough network scan using open-source software tools in order to find all connected devices and obtain details about each one, such as the services each host is running, its hostname, and its operating system (OS).

The primary objective of this project is to compile data on the network's hardware so that network managers may recognise security threats and weaknesses. Also, this data can be used to enhance network performance and resolve any connectivity problems.

Another goal could be to export the list of identified hosts to a text file for further analysis or reporting reasons in addition to finding and identifying devices on the network. Network administrators may benefit from this.

1.2) Description of the Project

The project described is an open source network scanning tool that locates and gathers data on all devices associated with a specific network. The programme may search for a variety of information, including hostnames, IP addresses, services used by each host, and OS systems used by each device. The application may also create a list of every host found on the network and export this data to a text file. This project's overall goal is to give network managers a thorough overview of their network infrastructure and the linked devices.

1.3) Scope of the Project

The scope of the project is to scan a network and find every device linked to it using an open source software tool. Each host's hostname and different bits of information, such as the services it is providing, will be retrieved by the software. The software will then compile a text file with a list of all the hosts it has discovered, along with the operating system for each host. (OS). Network administrators who wish to keep track of the devices connected to their network and make sure they are all setup safely and appropriately will find this project useful. Additionally, this effort might be able to help find network security holes.

2) System description

2.1) Target System description

The network of connected devices with a variety of operating systems and services would be the target system description for the project. The network may be a wide area network (WAN) or a local area network (LAN). (WAN). The project seeks to list all hosts in a text file, retrieve information about each host's services and hostname, scan the network using open source software to find all the devices linked to it, and identify each device's operating system. Network administrators will find this material useful in ensuring good network administration and security.

2.2) Assumptions and Dependencies (If applicable)

Assumptions:

- The device that is executing the scanning programme can connect to and access the network being examined.
- The network's gadgets are not set up to prevent the scan from finding them or to conceal their presence.
- The operating systems of the networked devices are supported by the open source software that is used for scanning.

Dependencies:

- The scanning software's ability to correctly identify the services, hostnames, and operating systems of the network's devices will determine how accurate the information it retrieves.
- The network's size, complexity, and the system resources used to execute the scanning programme all affect how quickly and effectively the scan is conducted.

2.3) Functional/Non-Functional Dependencies (if any)

Functional dependencies:

- The scanning software must be able to detect the devices connected to the network and retrieve information about their services, hostname, and operating system.
- The software must export the list of hosts to a text file for further analysis or processing.

Non-functional dependencies:

- The scanning software should be easy to use and have a user-friendly interface for efficient operation by network administrators.
- The software should be reliable and stable and not cause any disruptions or downtime on the network during the scanning process.
- The scanning process should be fast and efficient to minimize the time it takes to gather the necessary information.
- The software should have good documentation and support from the community in case of any issues or errors.

2.4) Data set used in support of your project (if any then paste the link)

The data set used in support of this project is the output of the network scan generated by the open source scanning software. The output may include information such as:

- IP addresses of devices on the network
- Hostnames of devices on the network
- Operating system of each device
- Open ports and services running on each device

The specific data set used will depend on the software used for the scan, and there is no one specific link to provide. However, some popular open source tools for network scanning include Nmap.

3) Analysis Report

3.1 System snapshots and full analysis report

Step 1) There are many open source network scanners available but the one which i am going to use is -: Nmap

Nmap - Nmap is a popular open source tool for network exploration and security auditing. It can be used to scan networks, discover hosts and services, and identify vulnerabilities.

- Sudo apt-get nmap command to install nmap on ubuntu

1) Scan the Network

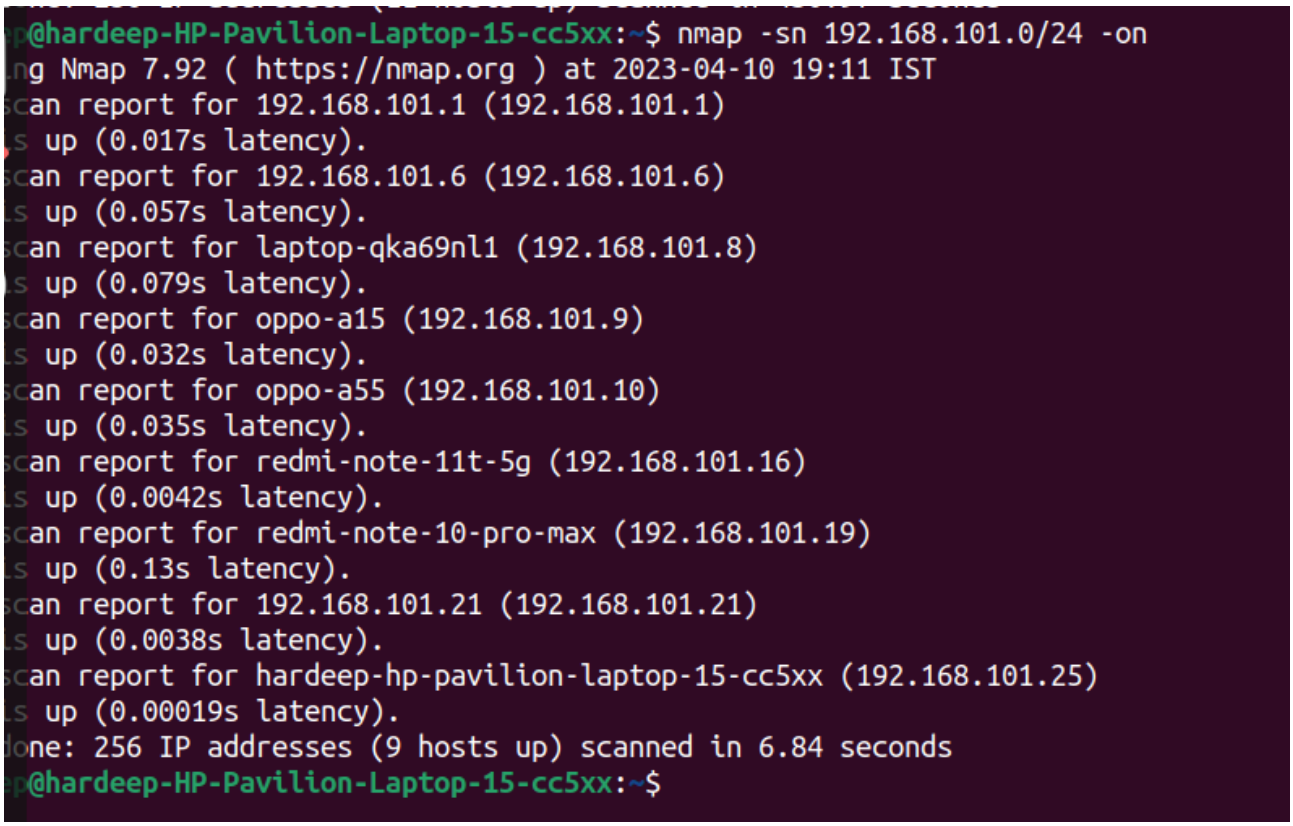
Run Basic Scan

```
hardeep-HP-Pavilion-Laptop-15-cc5xx:~$ nmap -sn 192.168.101.0/24
g Nmap 7.92 ( https://nmap.org ) at 2023-04-10 18:46 IST
an report for _gateway (192.168.101.1)
 up (0.051s latency).
an report for 192.168.101.3
 up (0.19s latency).
an report for 192.168.101.6
 up (0.15s latency).
an report for 192.168.101.8
 up (0.19s latency).
an report for 192.168.101.9
 up (0.20s latency).
an report for 192.168.101.10
 up (0.46s latency).
an report for 192.168.101.16
 up (0.47s latency).
an report for 192.168.101.21
 up (0.015s latency).
an report for hardeep-HP-Pavilion-Laptop-15-cc5xx (192.168.101.25)
 up (0.00027s latency).
ne: 256 IP addresses (9 hosts up) scanned in 29.97 seconds
hardeep-HP-Pavilion-Laptop-15-cc5xx:~$
```

Run a Detailed Scan

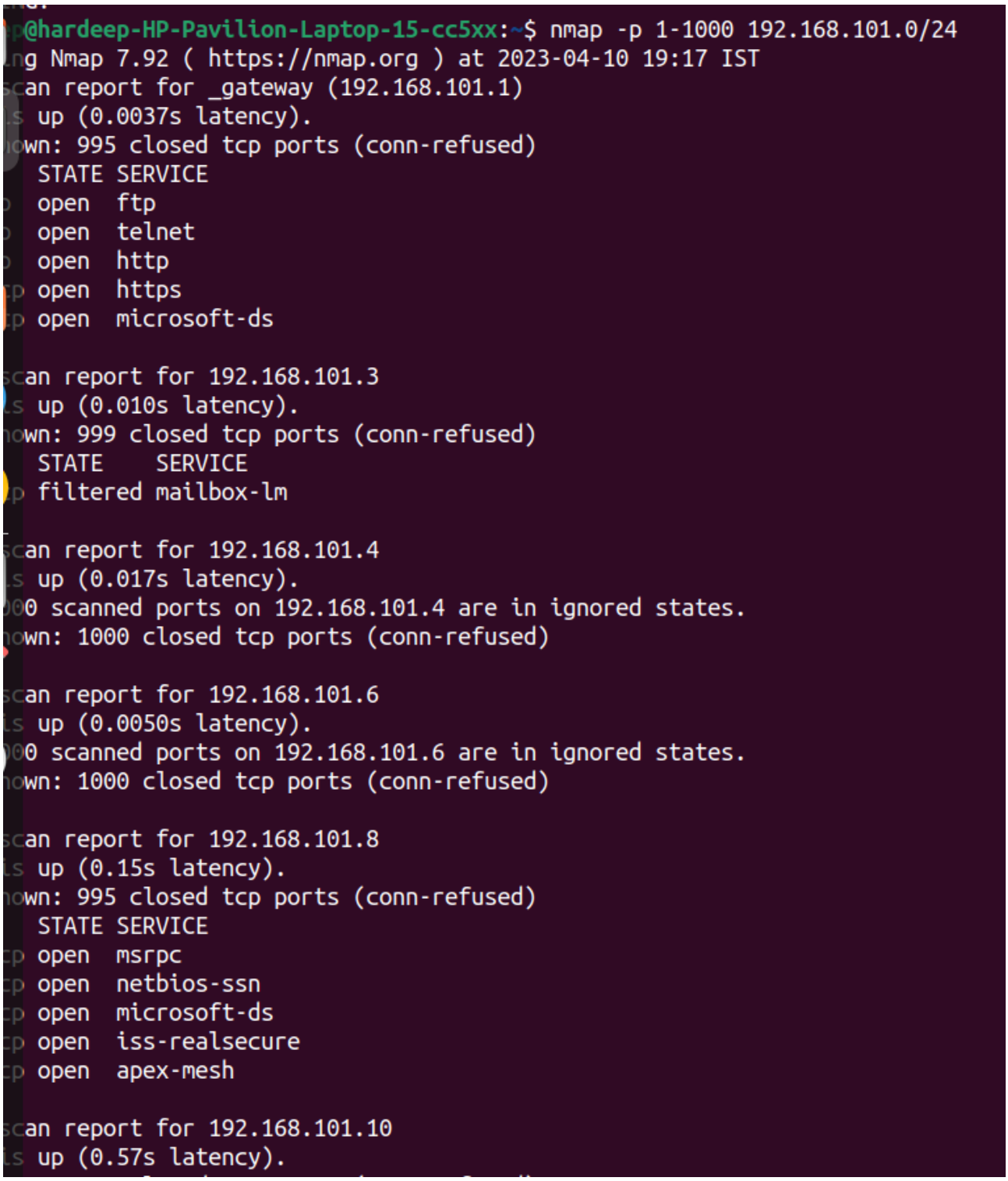
```
hardeep-HP-Pavilion-Laptop-15-cc5xx:~$ sudo nmap -sS -A -T4 192.168.101.0/24
g Nmap 7.92 ( https://nmap.org ) at 2023-04-10 19:03 IST
has grown to over 2.3 seconds, decreasing to 2.0
has grown to over 2.3 seconds, decreasing to 2.0
has grown to over 2.3 seconds, decreasing to 2.0
has grown to over 2.3 seconds, decreasing to 2.0
has grown to over 2.3 seconds, decreasing to 2.0
```

To analyse the result

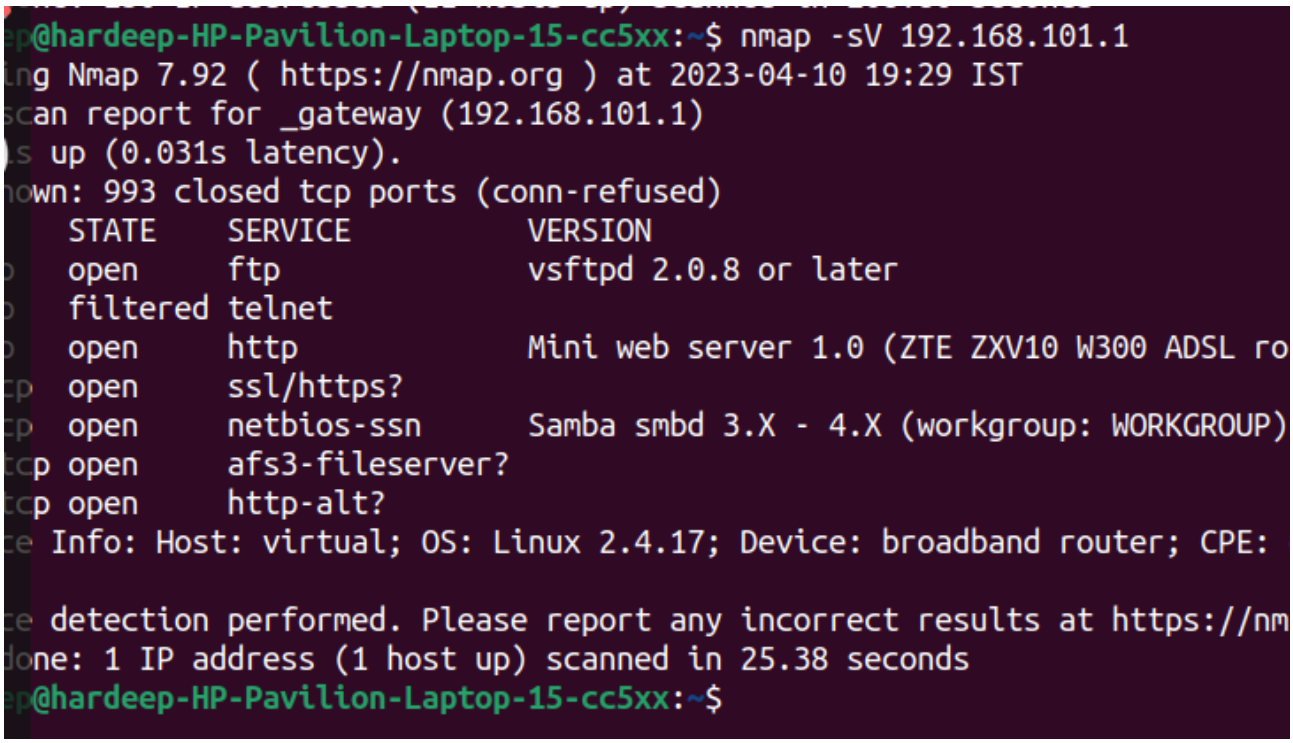


1) Host discovery: To discover hosts on your network, you can use the -sn option, which sends an ICMP ping to each IP address in a range of addresses.

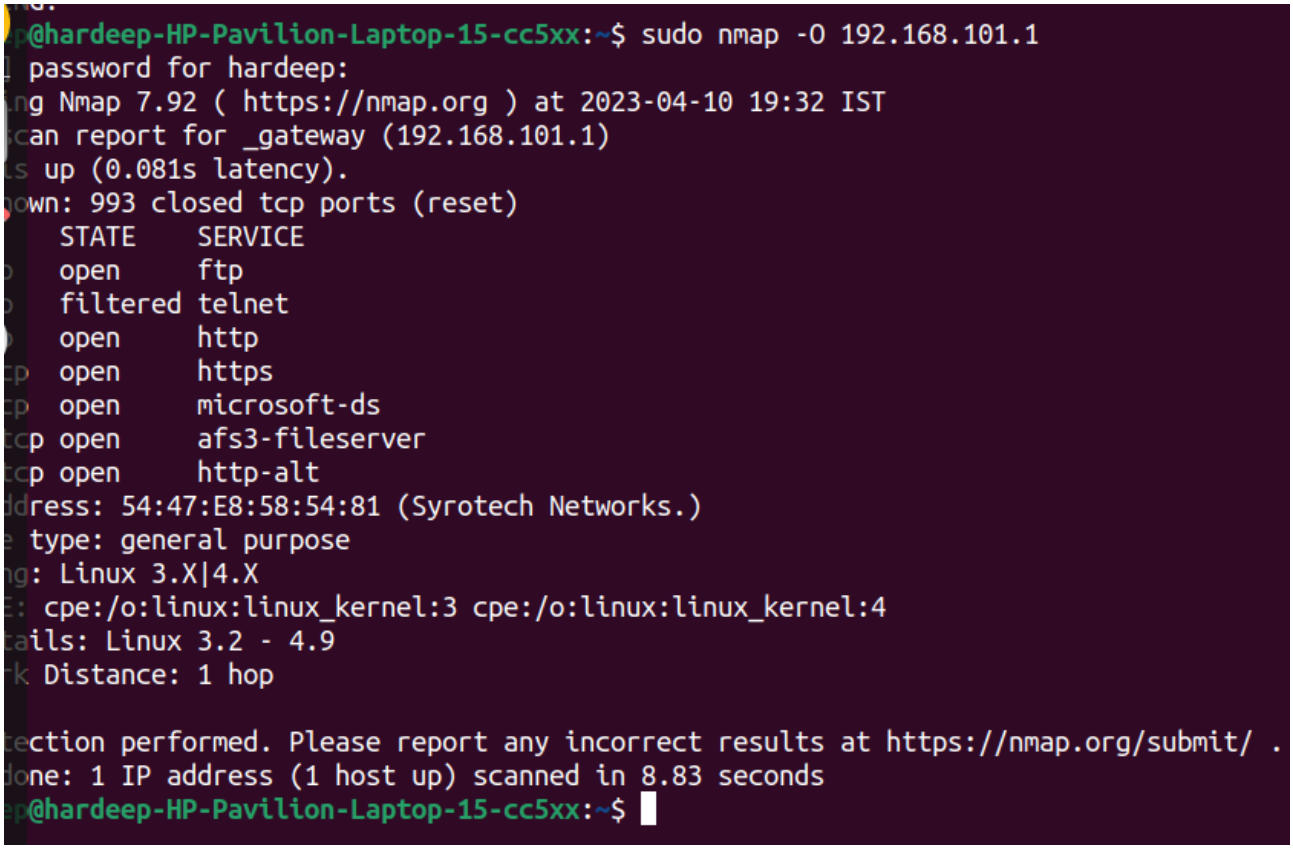
2) Port scanning: To identify open ports on a host, you can use the -p option



3) Service detection: To identify the services running on a host and their version numbers, you can use the -sV option.



4) Operating system detection: To identify the operating system running on a host, you can use the -O option.



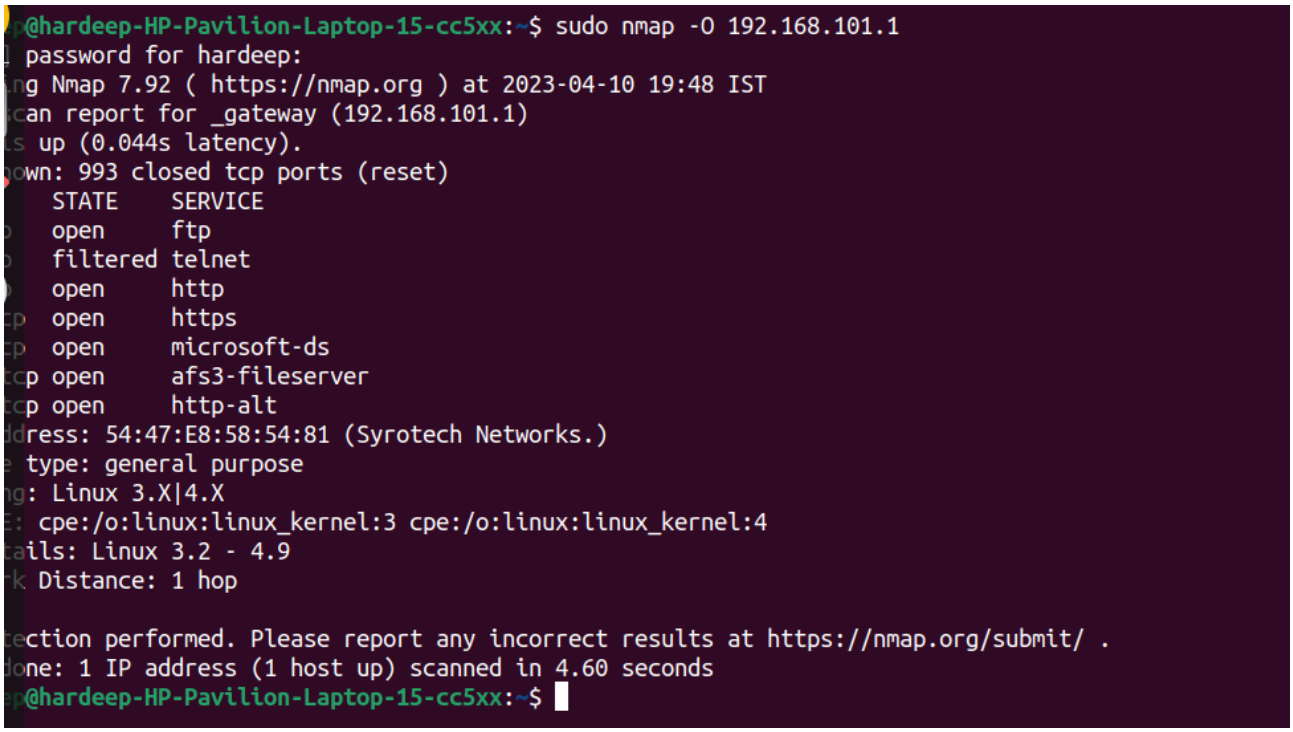
5) Aggressive scan: To retrieve more information about a host, including OS detection, service detection, and traceroute information, you can use the -A option.

```
@hardeep-HP-Pavilion-Laptop-15-cc5xx:~$ nmap -A 192.168.101.1
g Nmap 7.92 ( https://nmap.org ) at 2023-04-10 19:34 IST
an report for 192.168.101.1 (192.168.101.1)
 up (0.012s latency).
wn: 993 closed tcp ports (conn-refused)
   STATE    SERVICE          VERSION
   open     ftp              vsftpd 2.0.8 or later
   filtered telnet
   open     http             Mini web server 1.0 (ZTE ZXV10 W300 ADSL router http c
-title: SY-GPON-2010-WADONT
   open     ssl/https?
date: 2023-04-10T14:04:44+00:00; -1s from scanner time.
cert: Subject: commonName=ZXV10/organizationName=ZTE Corporation/stateOrProvinceNam
valid before: 2005-01-01T01:41:24
valid after:  2025-01-01T01:41:24
   open     netbios-ssn      Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
p open     afs3-fileserver?
info: Unable to open connection
p open     http-alt?
e Info: Host: virtual; OS: Linux 2.4.17; Device: broadband router; CPE: cpe:/h:zte:

cript results:
-time: Protocol negotiation failed (SMB2)
security-mode:
count_used: guest
thentication_level: user
allenge_response: supported
ssage_signing: disabled (dangerous, but default)
sql-info: ERROR: Script execution failed (use -d to debug)
k-skew: mean: -1s, deviation: 0s, median: -1s

e detection performed. Please report any incorrect results at https://nmap.org/subm
one: 1 IP address (1 host up) scanned in 17.72 seconds
@hardeep-HP-Pavilion-Laptop-15-cc5xx:~$
```

List Host name in Text file

```
@hardeep-HP-Pavilion-Laptop-15-cc5xx:~$ nmap -sn 192.168.101.1 -oN output_file.txt
g Nmap 7.92 ( https://nmap.org ) at 2023-04-10 19:43 IST
an report for _gateway (192.168.101.1)
 up (0.0019s latency).
one: 1 IP address (1 host up) scanned in 0.14 seconds
@hardeep-HP-Pavilion-Laptop-15-cc5xx:~$
```

Host Operating System



REFERENCE

- **Fyodor. (n.d.). Nmap: the Network Mapper. Retrieved from** https://nmap.org/
- Rapid7. (2021). Nmap Tutorial: Basic Commands & How to Use Them. Retrieved from https://blog.rapid7.com/2017/05/24/nmap-tutorial-basic-commands-how-to-use-them/
- Davidoff, S., & Ham, N. (2004). Network Forensics: Tracking Hackers through Cyberspace. Prentice Hall.
- Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley Professional.