INT301: Open-Source Technologies

Project Report

NAME: K AKANKSHA

REG NO: 11909575

SECTION: KE022

ROLL NO: 27

1. INTRODUCTION

1.1 OBJECTIVE OF THE PROJECT

The objective of the project is to use an 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

For the given project we will be using the NMAP open-source software. Using the Nmap we will be carrying out our project objectives. Nmap (Network Mapper) is a tool that is free of charge and can be used to explore and scan networks, detect and identify hosts and services, and gather information about them. It can be utilized for various network-related tasks such as security audits, network inventory, and vulnerability assessments. To put it simply, Nmap is like a detective that can investigate a network and provide details about the connected devices, services running on those devices, and any vulnerabilities that could be exploited by attackers. Nmap suits our project objectives perfectly and with the help of this GUI software we will able to perform various network scans and related services on our device.

1.3 SCOPE OF THE PROJECT

To carry out this project we would first need to download and install Nmap on our local machine. The following is the link from their official website:

https://nmap.org/download.html

We would then be required to identify our system's ip address to carry out scans and everything related to it. After we have known our target ip address we can use in the Nmap software to explore further information about the network.

2. SYSTEM DESCRIPTION

2.1 TARGET SYSTEM DESCRIPTION

Target System: The target system for this project is my own Laptop

Operating System: The operating system that I would be using for this is my primary OS i.e., Windows 10 for both the scanning of networks and installation of Nmap.

Network type: Private Network

IP Address of the target system: **192.168.56.1**

To find out the ip address of the system we will be running the command ipconfig on the windows command prompt.

Command Prompt

```
Microsoft Windows [Version 10.0.19044.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>ipconfig

Windows IP Configuration


Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8a48:ceb6:fb6c:9bdd%14
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

3. ANALYSIS REPORT

3.1 SYSTEM SNAPSHOTS AND FULL ANALYSIS REPORT

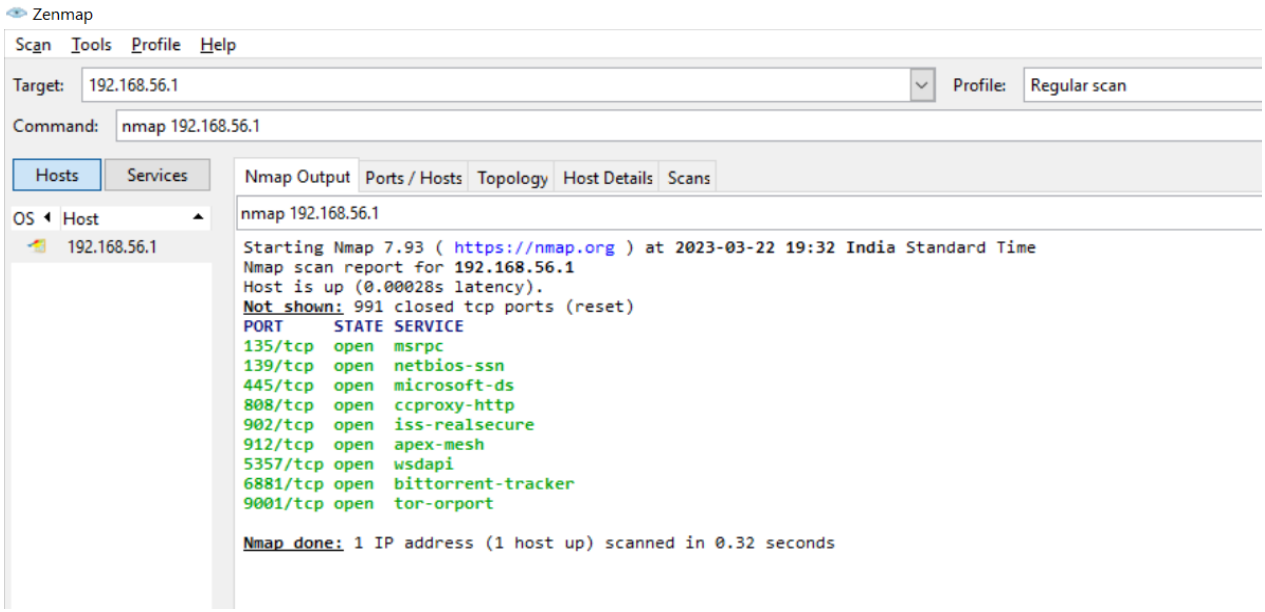
a) Use of Nmap to scan your network: **nmap 192.168.56.1**

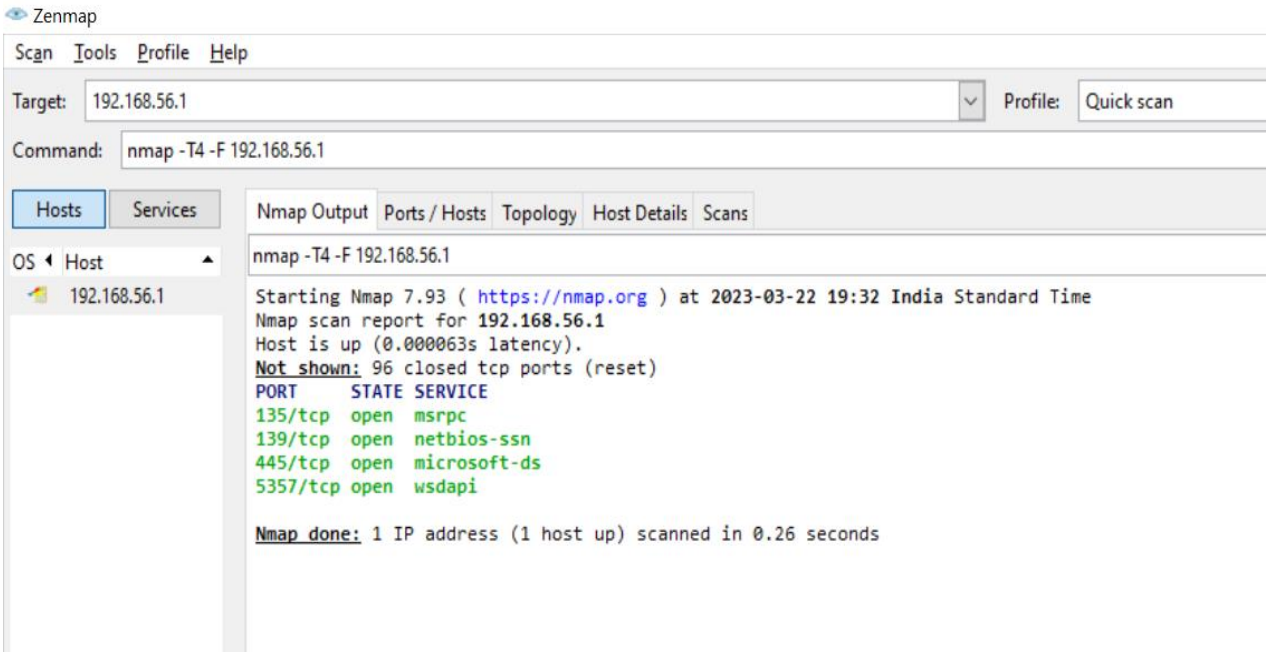
We can use various scans for our network ranging anywhere from quick scan, intense scan, regular scan, ping scan, etc. There's a unique command for each scan. We can also get manual by using the command nmap –help

Below is the attached screenshots for both regular scan and quick scan

Command for regular scan: **nmap 192.168.56.1**

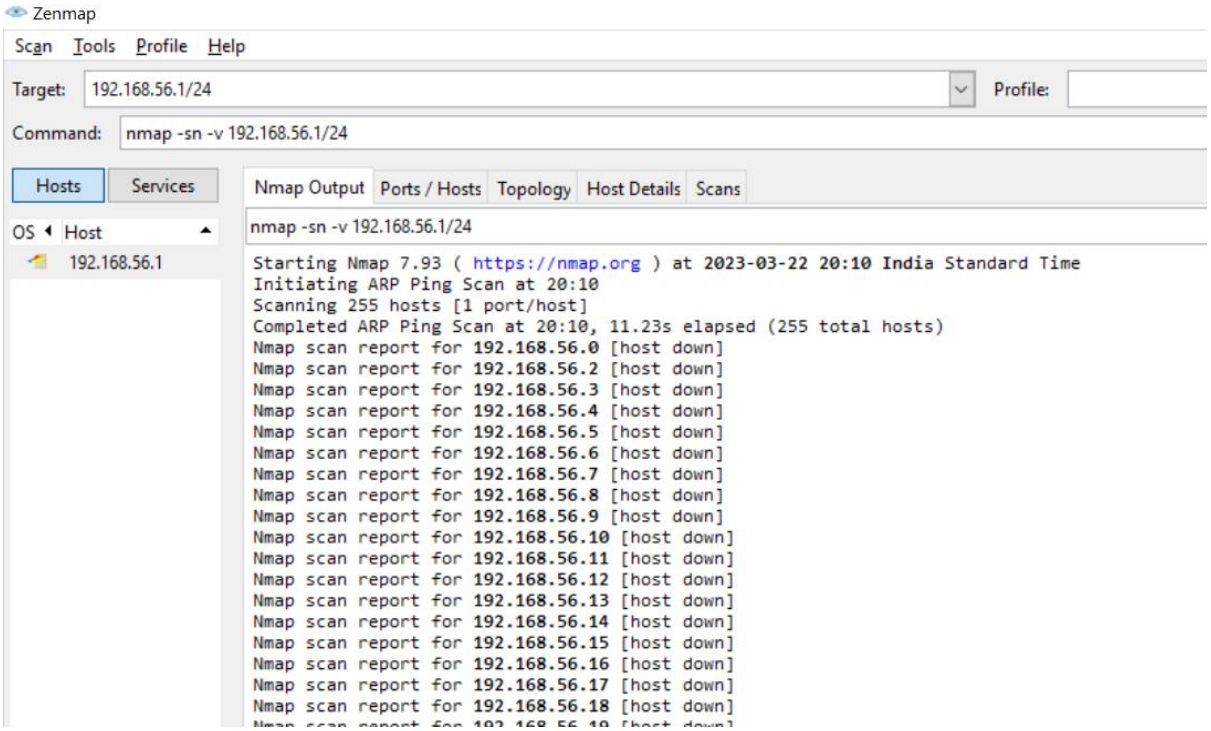
Command for quick scan: **nmap -T4 -F 192.168.56.1**

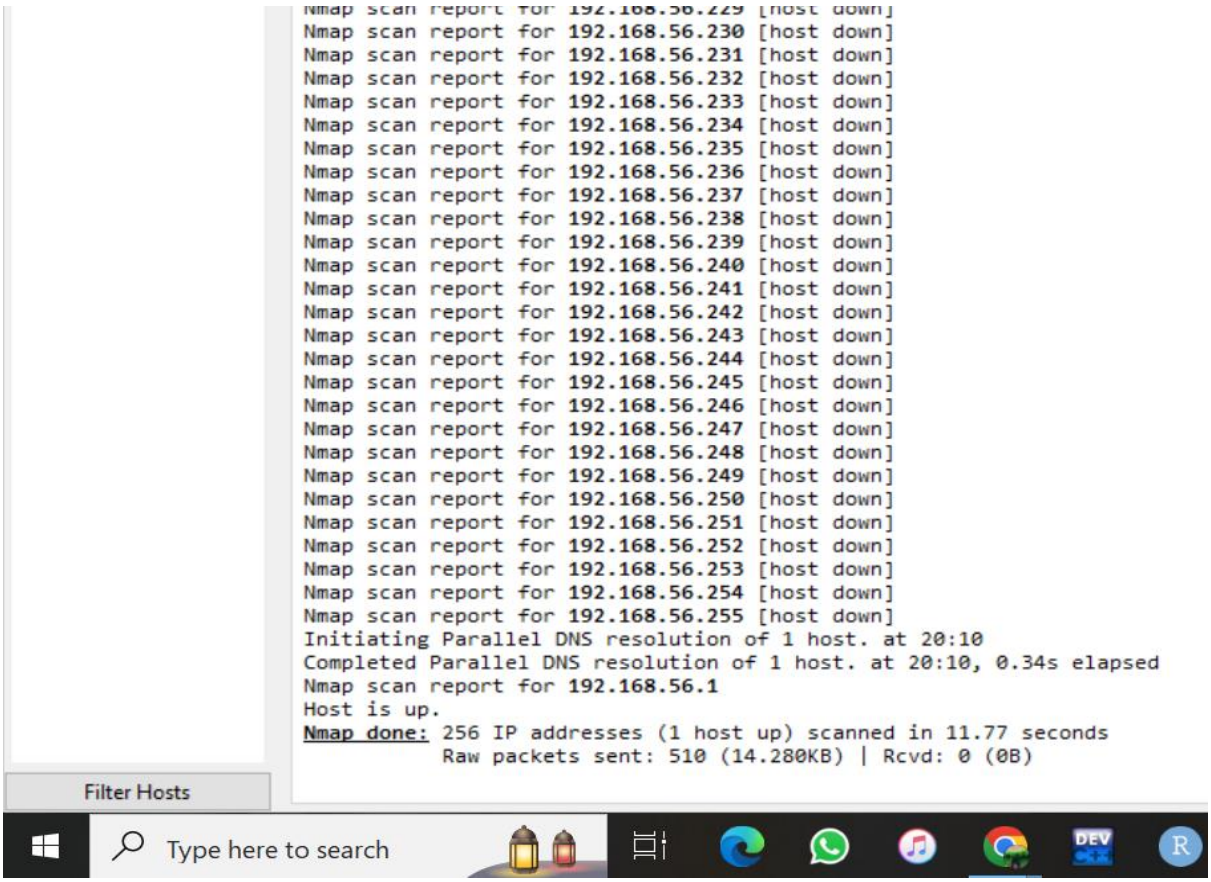




b) Discover everything connected to it**: nmap -sn -v 192.168.56.1/24**

This following command will scan all IP addresses on the 192.168.56.1/24 subnet and show a list of hosts that are online.

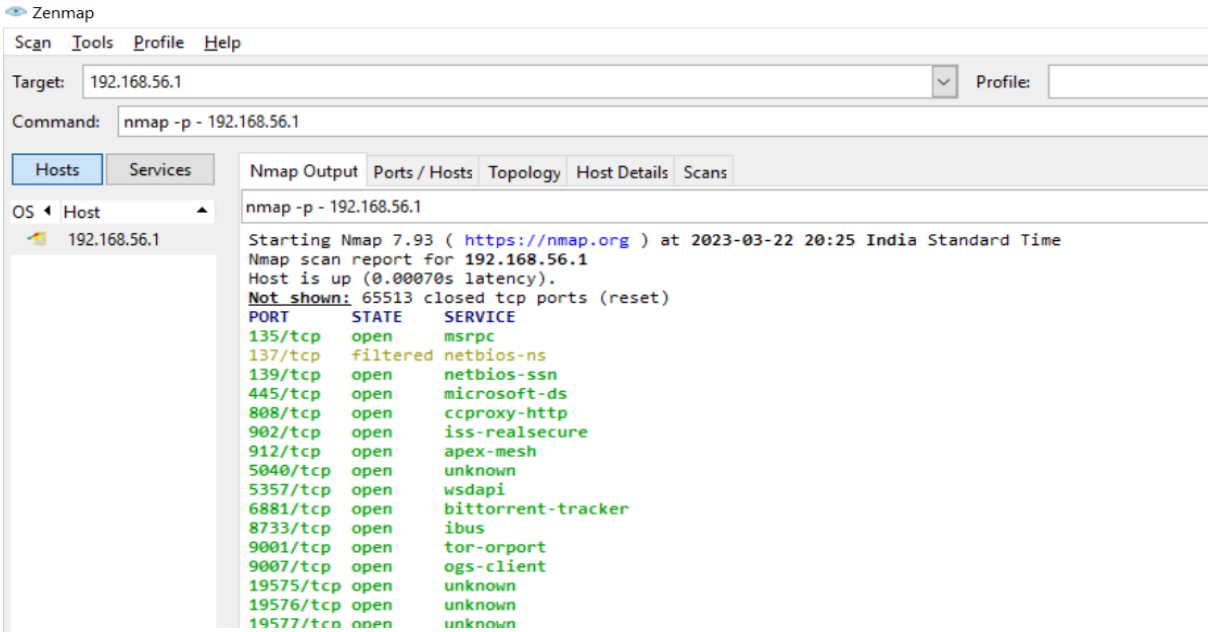


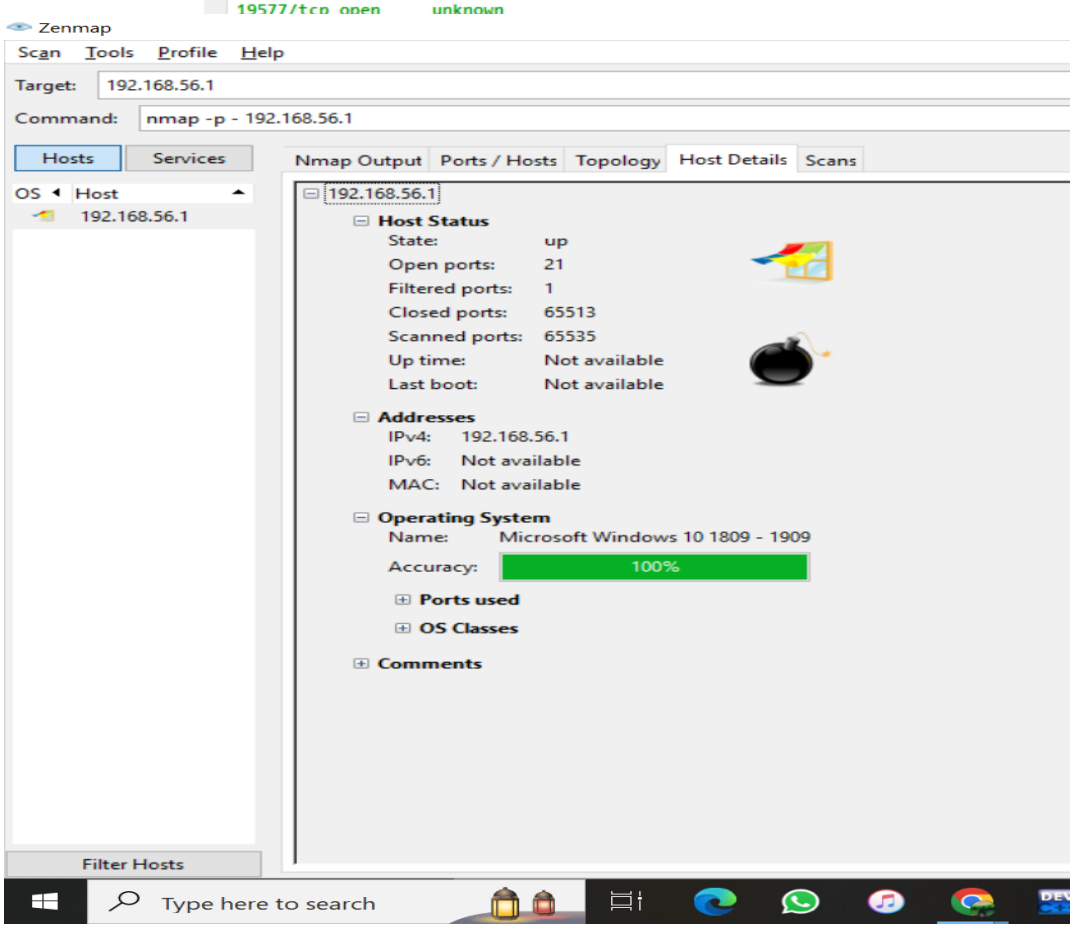


c) Retrieve variety of information about what's connected:

nmap -p – 192.168.56.1

to retrieve a list of open ports on a host, you can run the following command: **nmap -p- 192.168.56.1**. This will scan all 65535 ports on host 192.168.56.1 and show a list of open ports.





Zenmap

Scan Tools Profile Help

Target: 192.168.56.1

Command: nmap -p - 192.168.56.1

Hosts | Services

OS | Host

192.168.56.1

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	
139	tcp	open	netbios-ssn	
445	tcp	open	microsoft-ds	
808	tcp	open	ccproxy-http	
902	tcp	open	iss-realsecure	
912	tcp	open	apex-mesh	
5357	tcp	open	wsdapi	
6881	tcp	open	bittorrent-tracker	
9001	tcp	open	tor-orport	
137	tcp	filtered	netbios-ns	
5040	tcp	open	unknown	
8733	tcp	open	ibus	
9007	tcp	open	ogs-client	
19575	tcp	open		
19576	tcp	open		
19577	tcp	open		
49664	tcp	open		
49665	tcp	open		
49666	tcp	open		
49667	tcp	open		
49668	tcp	open		
49676	tcp	open		

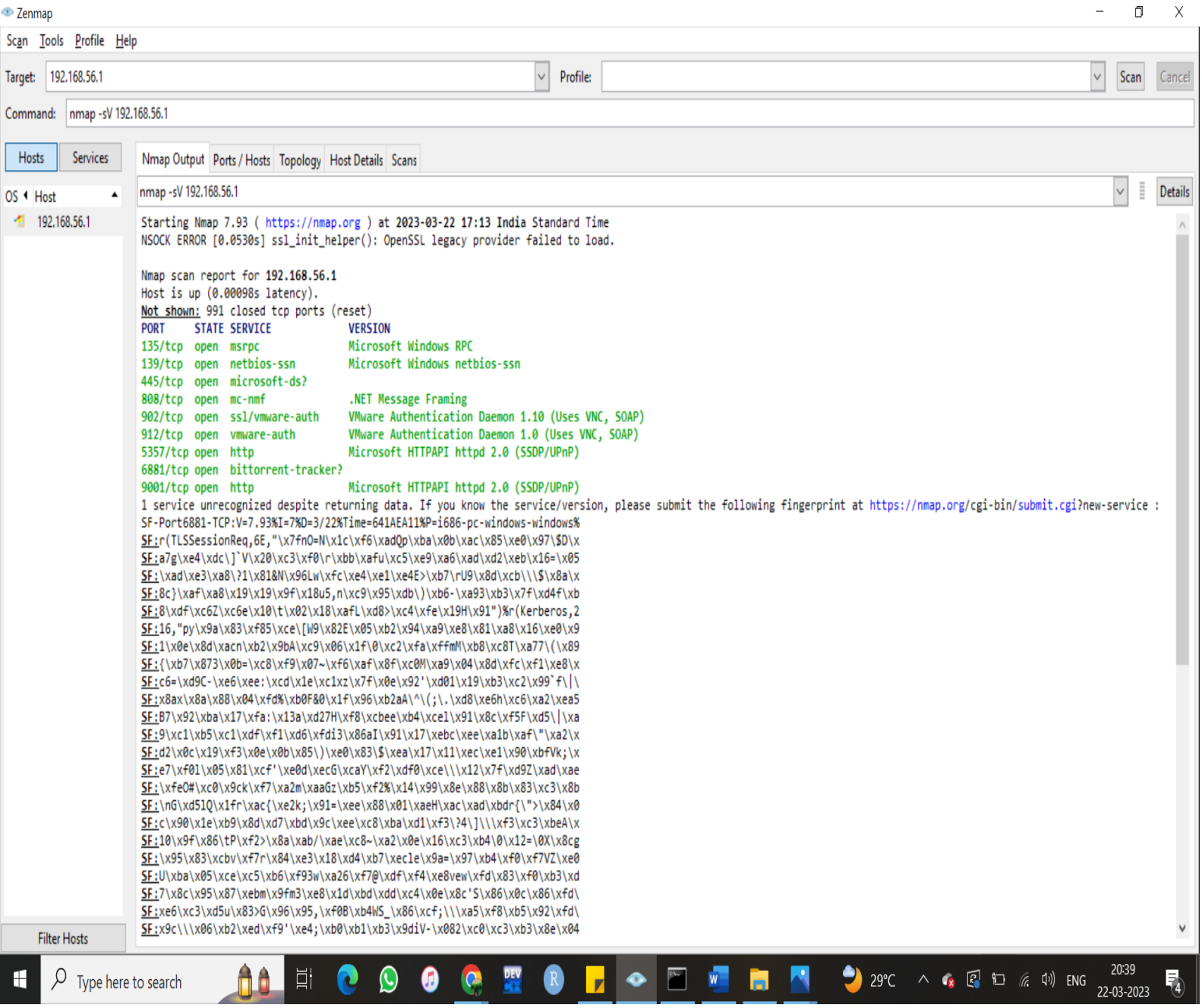
Filter Hosts

Type here to search

d) What services each host is operating : **nmap -sV 192.168.56.1**

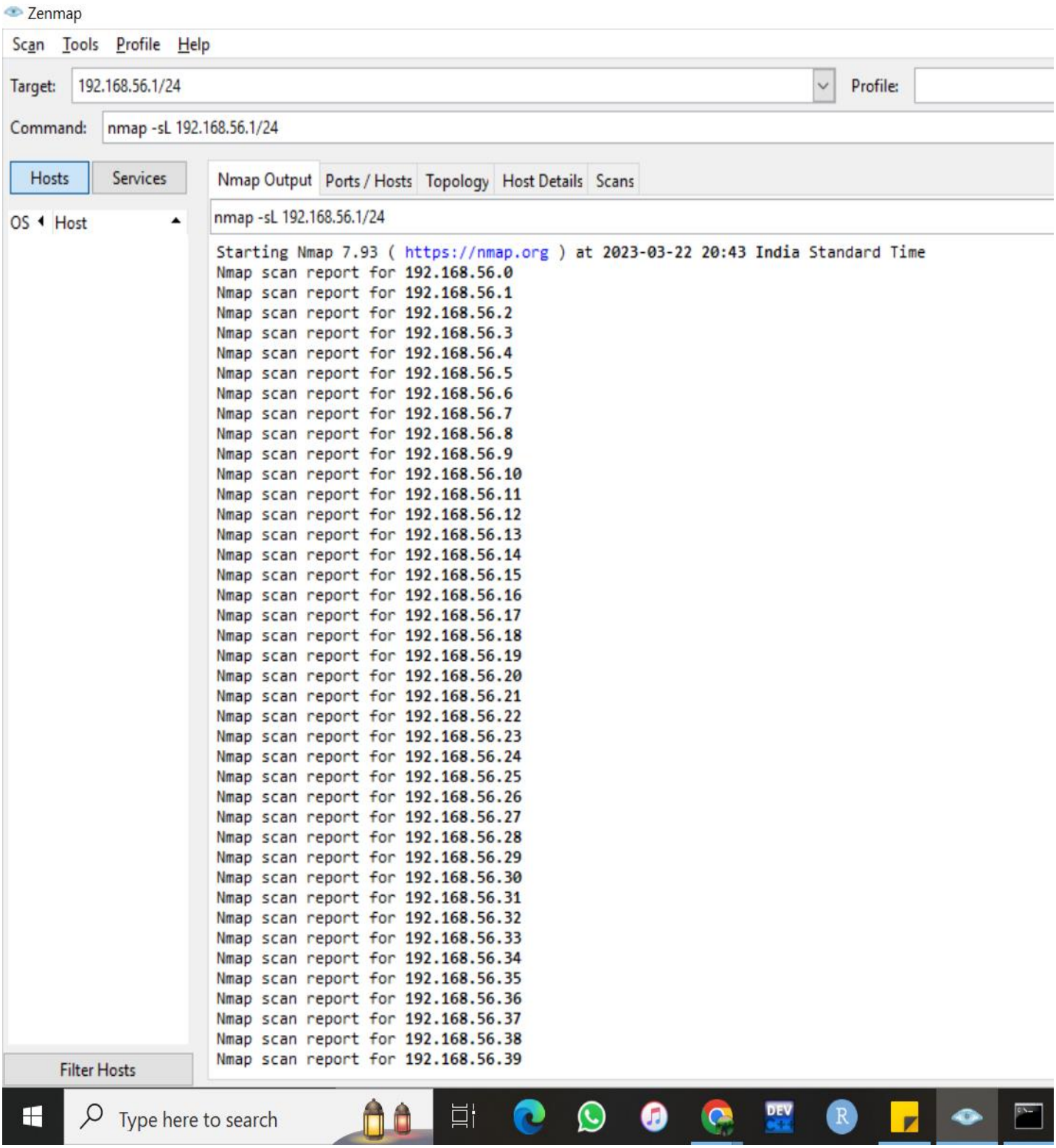
The "-sV" option enables service version detection, which allows nmap to identify the application and version number of each service running on the target hosts.

Once the scan is complete, nmap will display a report showing the open ports and services detected on each host. Look for the "SERVICE/VERSION" column to see the details of each service.



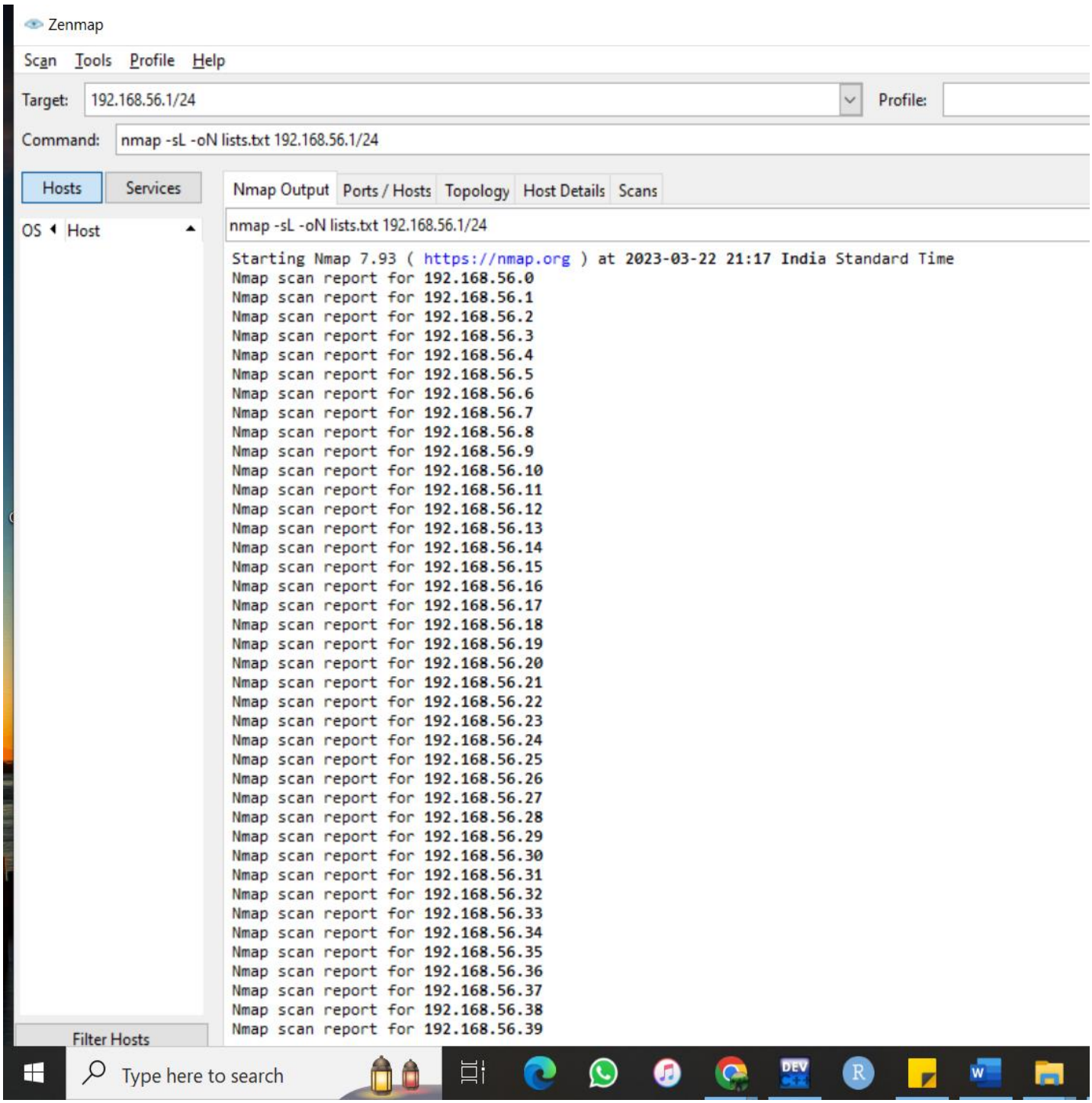
e) Scan the hostname: **nmap –sL 192.168.56.1/24**

This will perform a "list scan" of all IP addresses on the 192.168.56.1/24 subnet and show a list of hostnames.



f) List all the hosts in a text file : **nmap -sL -oN lists.txt 192.168.56.1/24**

To list all the hosts in a text file first we need to make sure that we are running the nmap application as the administrator otherwise you might face an issue of access denied. The following command in the screenshot first lists all the hosts and then saves the output in a text file. This is done for the purpose of saving information for future reference.



lists - Notepad

File Edit Format View Help

```
# Nmap 7.93 scan initiated Wed Mar 22 21:17:32 2023 as: nmap -sL -oN lists.txt -oX c:\\users\\hp\\appdata\\local\\temp\\zenmap-glbzwe.xml 192.168.56.1/24
Nmap scan report for 192.168.56.0
Nmap scan report for 192.168.56.1
Nmap scan report for 192.168.56.2
Nmap scan report for 192.168.56.3
Nmap scan report for 192.168.56.4
Nmap scan report for 192.168.56.5
Nmap scan report for 192.168.56.6
Nmap scan report for 192.168.56.7
Nmap scan report for 192.168.56.8
Nmap scan report for 192.168.56.9
Nmap scan report for 192.168.56.10
Nmap scan report for 192.168.56.11
Nmap scan report for 192.168.56.12
Nmap scan report for 192.168.56.13
Nmap scan report for 192.168.56.14
Nmap scan report for 192.168.56.15
Nmap scan report for 192.168.56.16
Nmap scan report for 192.168.56.17
Nmap scan report for 192.168.56.18
Nmap scan report for 192.168.56.19
Nmap scan report for 192.168.56.20
Nmap scan report for 192.168.56.21
Nmap scan report for 192.168.56.22
Nmap scan report for 192.168.56.23
Nmap scan report for 192.168.56.24
Nmap scan report for 192.168.56.25
Nmap scan report for 192.168.56.26
Nmap scan report for 192.168.56.27
Nmap scan report for 192.168.56.28
```

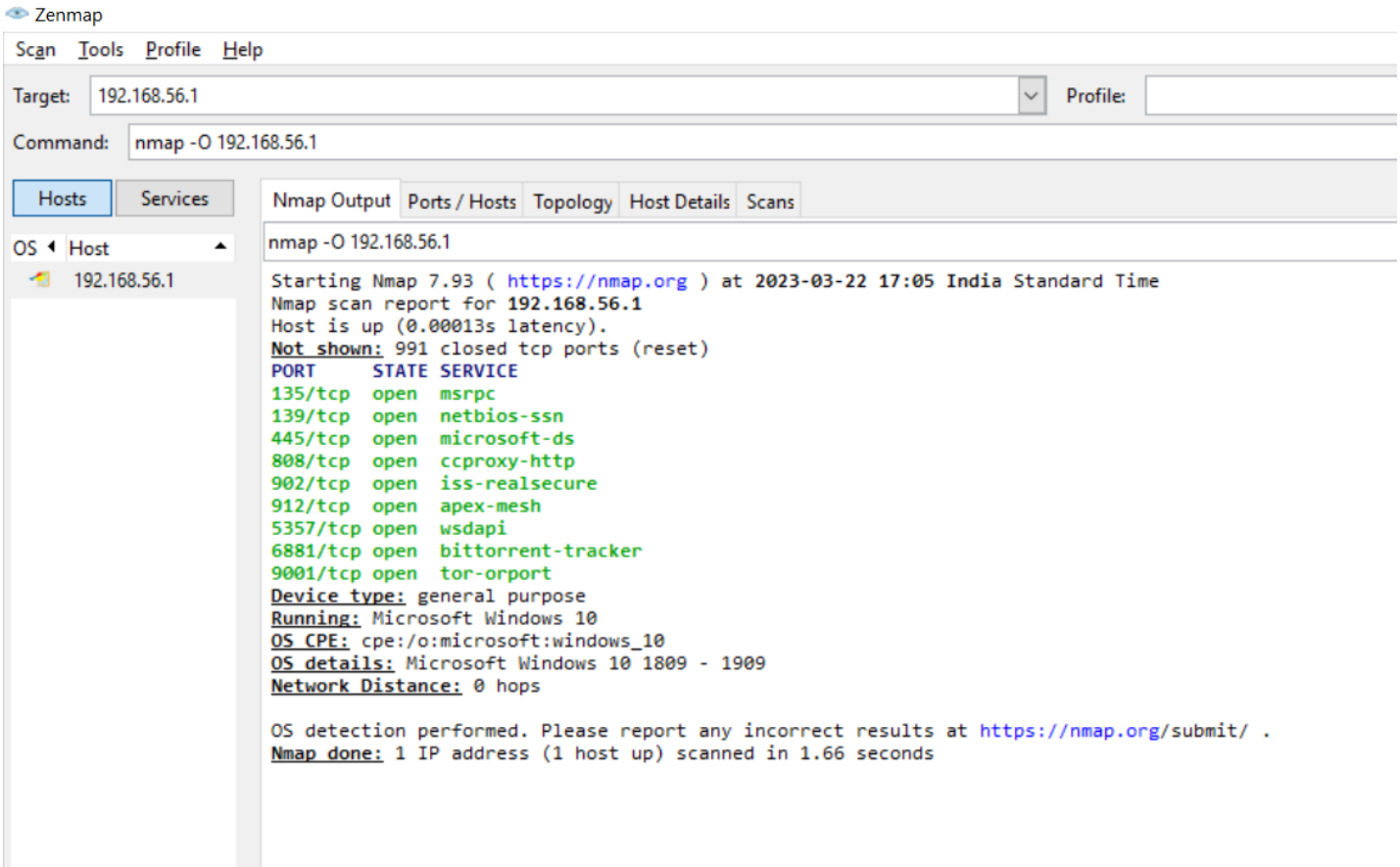
Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

Type here to search

29°C ENG 21:18 22-03-2023

g) Identify a host's operating system (OS)

This will perform an OS detection scan on host 192.168.1.1 and attempt to identify the operating system.



4. REFERENCES

a) Github Link: https://github.com/akankshakarra/Int301

b) https://www.varonis.com/blog/nmap-commands

c) https://www.edureka.co/blog/nmap-tutorial/