ST#IS#4899

TASK – 3

TARGET: -

1) Scan the complete network of the domain you selected

i.e the complete IP range.

1-255

Ex: website1.com - 192.168.0.10

192.168.0.1 - 192.168.0.255

- total no. of devices/IP addresses live on the network

2) Filter the IP addresses in the entire network which are having the following ports open:

PORT: 22

PORT: 80

PORT: 3306

i.e select the IP addresses which have all these ports(22,80,3306) open.

NOTE: The IP address should have all the 3 ports (22,80,3306) opened and its okay if other ports are also opened.

3) Gather the following details from the filtered IP addresses:

A. Services

B. Versions

C. Banner Details

D. Operating System

NOTE: Gather the services from entire port range:

0-65535 ports

- With and without using a VPN.

ST#IS#4899

SYNOPSIS:

➔ An IP address is a unique address that identifies a device on the internet

Or a local network. IP stands for “internet protocol”, which is set of rules governing the format of data sent via internet or local network.

➔ A port is a gateway for data transfer between devices. Port number is used

To direct data to correct location within the device. There are 65536 ports. Range of port number: 0-65535

➔ Port 22 is used for secure shell(SSH) communication and allows remote

Administration access to the VM.

➔ Port 80 is assigned to commonly used internet communication protocol,

Hypertext Transfer Protocol (HTTP)

❖ Port 3306 is default port for classic MySQL protocol.

ANSWER-1:

➔ Finding the IP addresses for the selected three educational domains.

STEP-1:

Select any three educational domains of your wish.

MY DOMAINS:

1) sreenidhi.edu.in

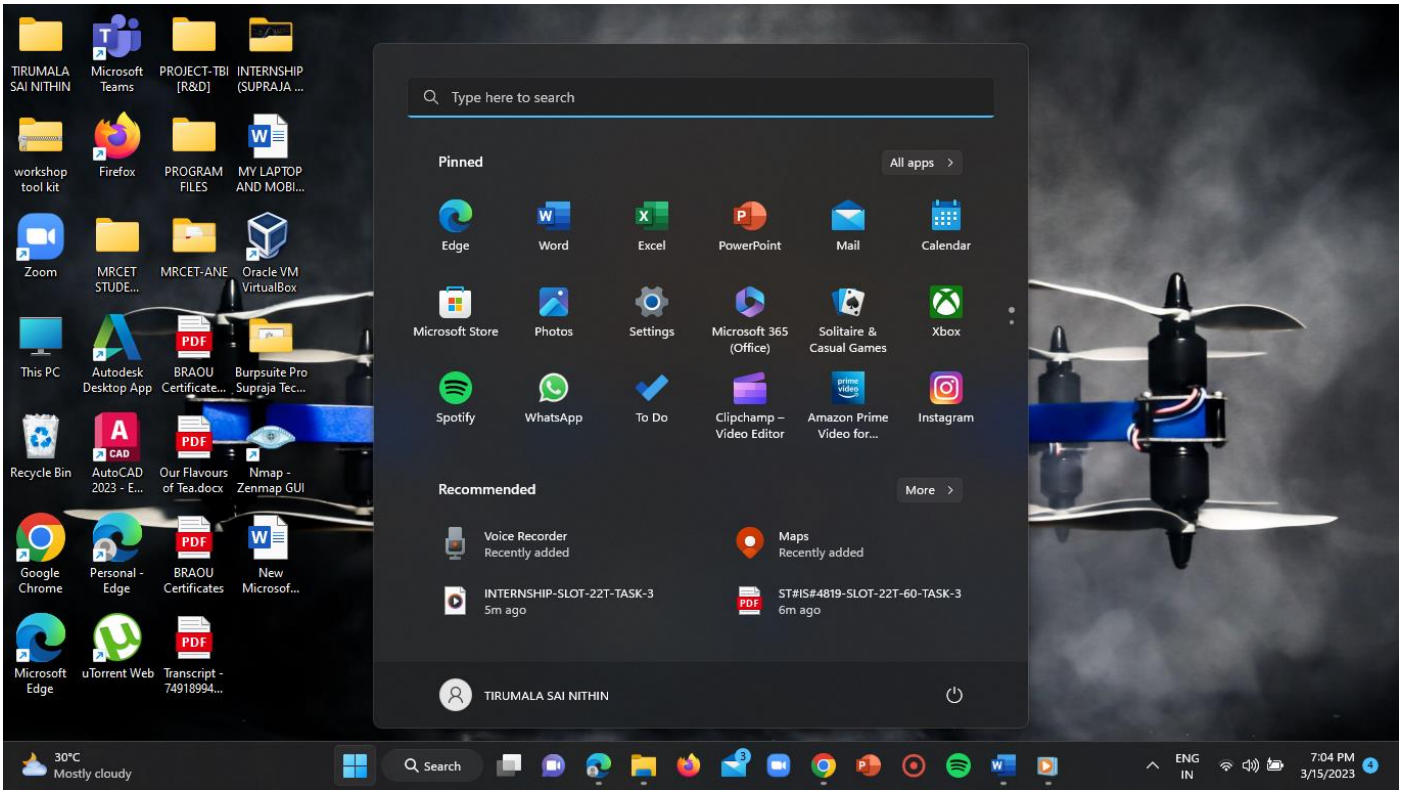
2) cmrec.ac.in

3) acc.edu.in

STEP-2:

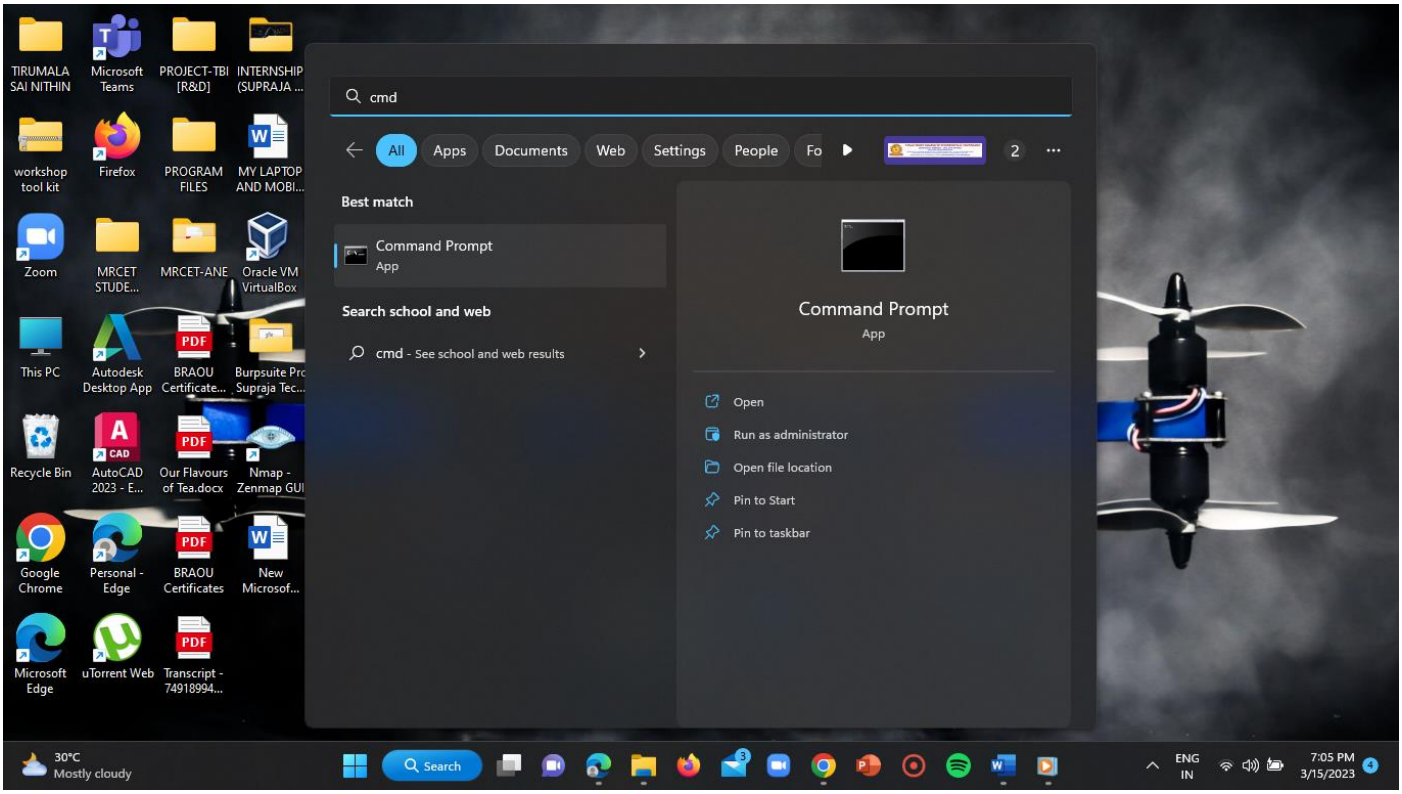
Now click on start.

ST#IS#4899



STEP-3:

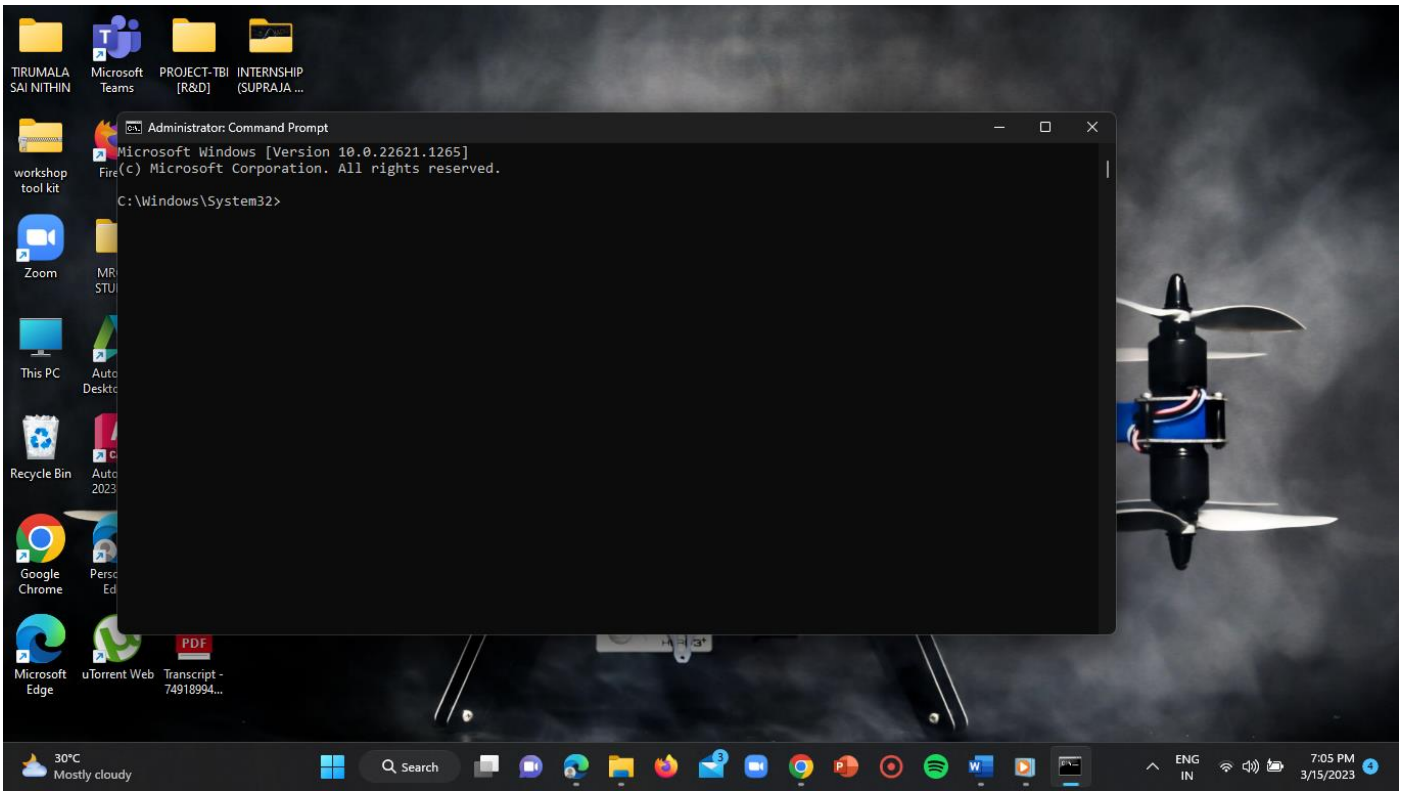
In the search bar enter “cmd”.



STEP-4:

ST#IS#4899

Now open the command prompt in the “ADMINISTRATOR” mode by clicking on “run as administrator”.



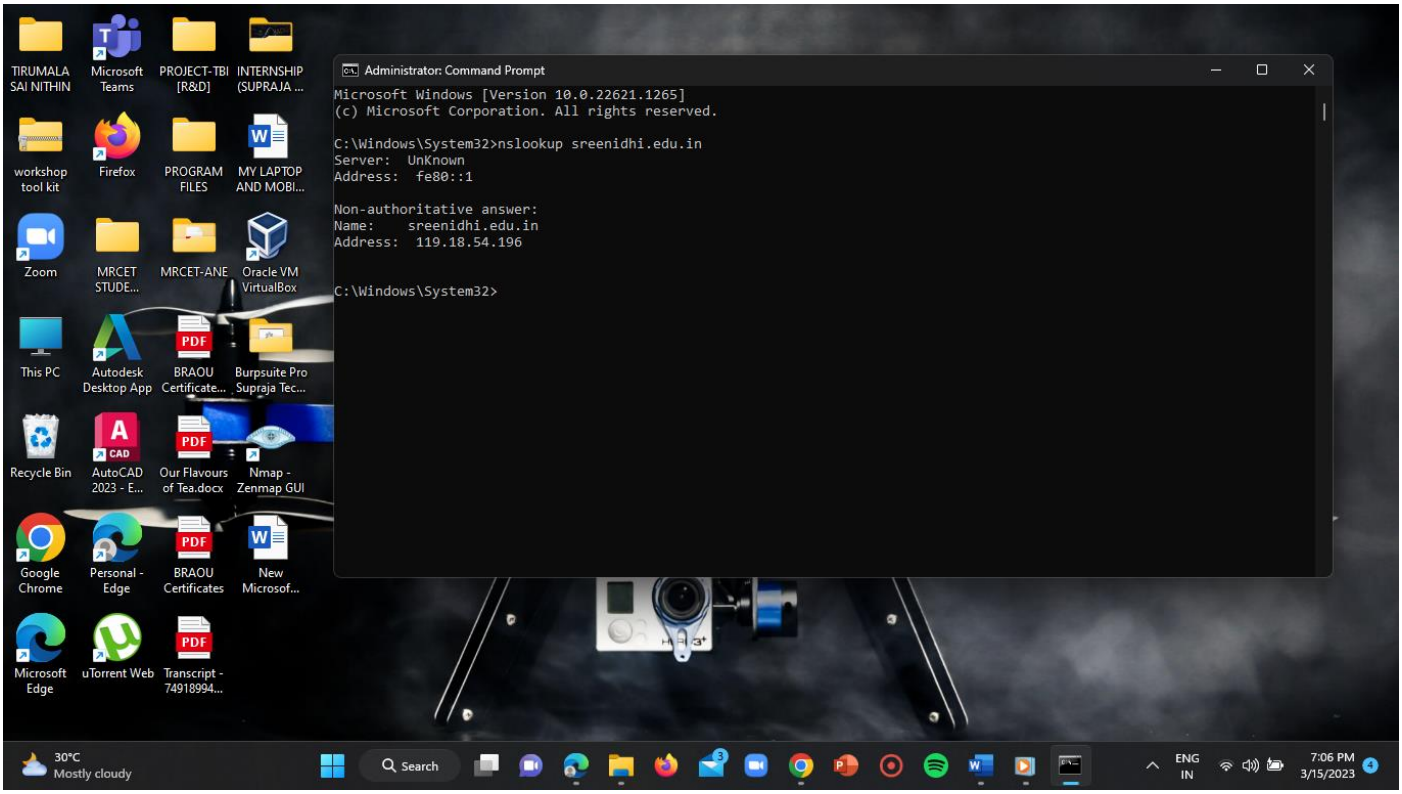
STEP-5:

Now type the syntax as “nslookup<space>domain name” and click on enter.

For DOMAIN-1:

Type= nslookup sreenidhi.edu.in

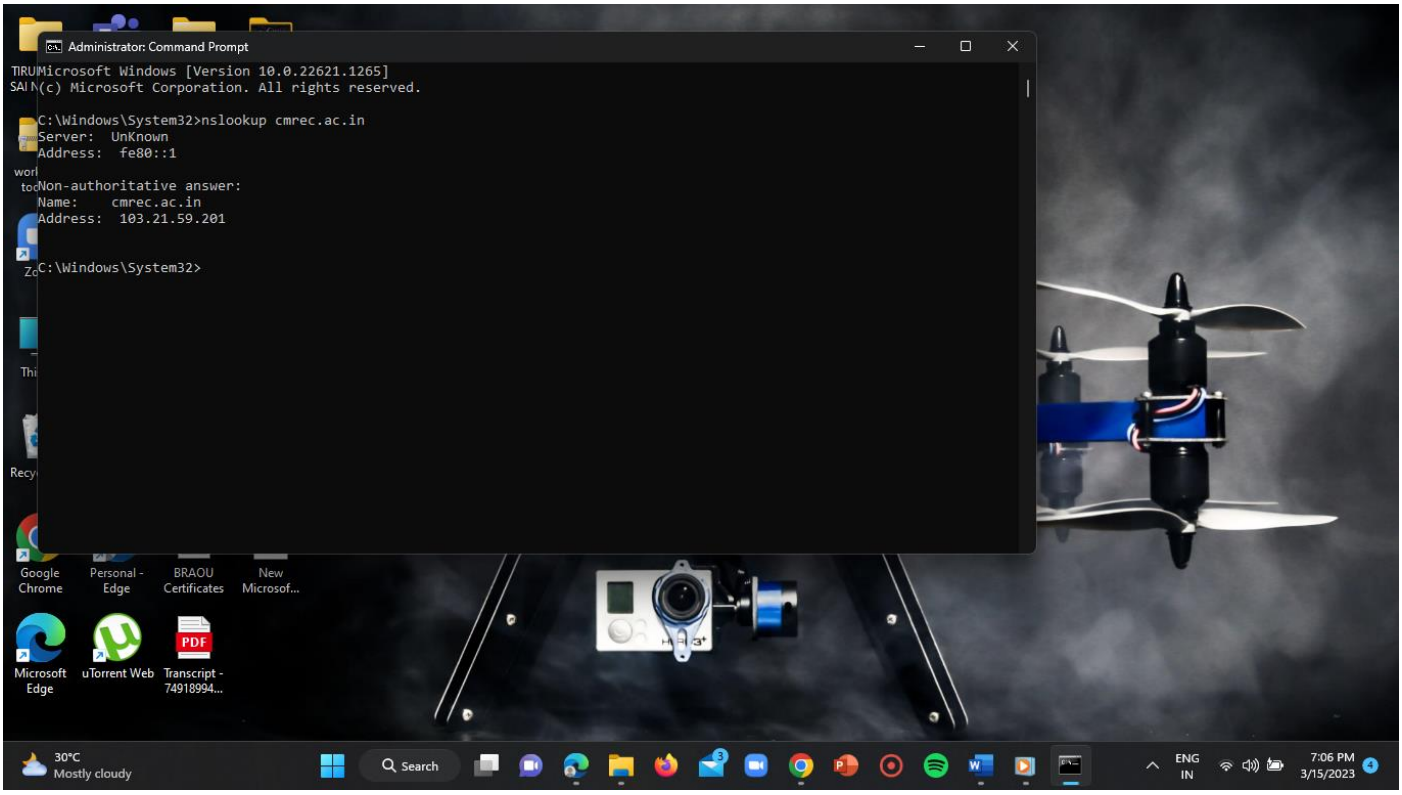
ST#IS#4899



IP ADDRESS = 119.18.54.196

For DOMAIN-2:

Type= nslookup cmrec.ac.in

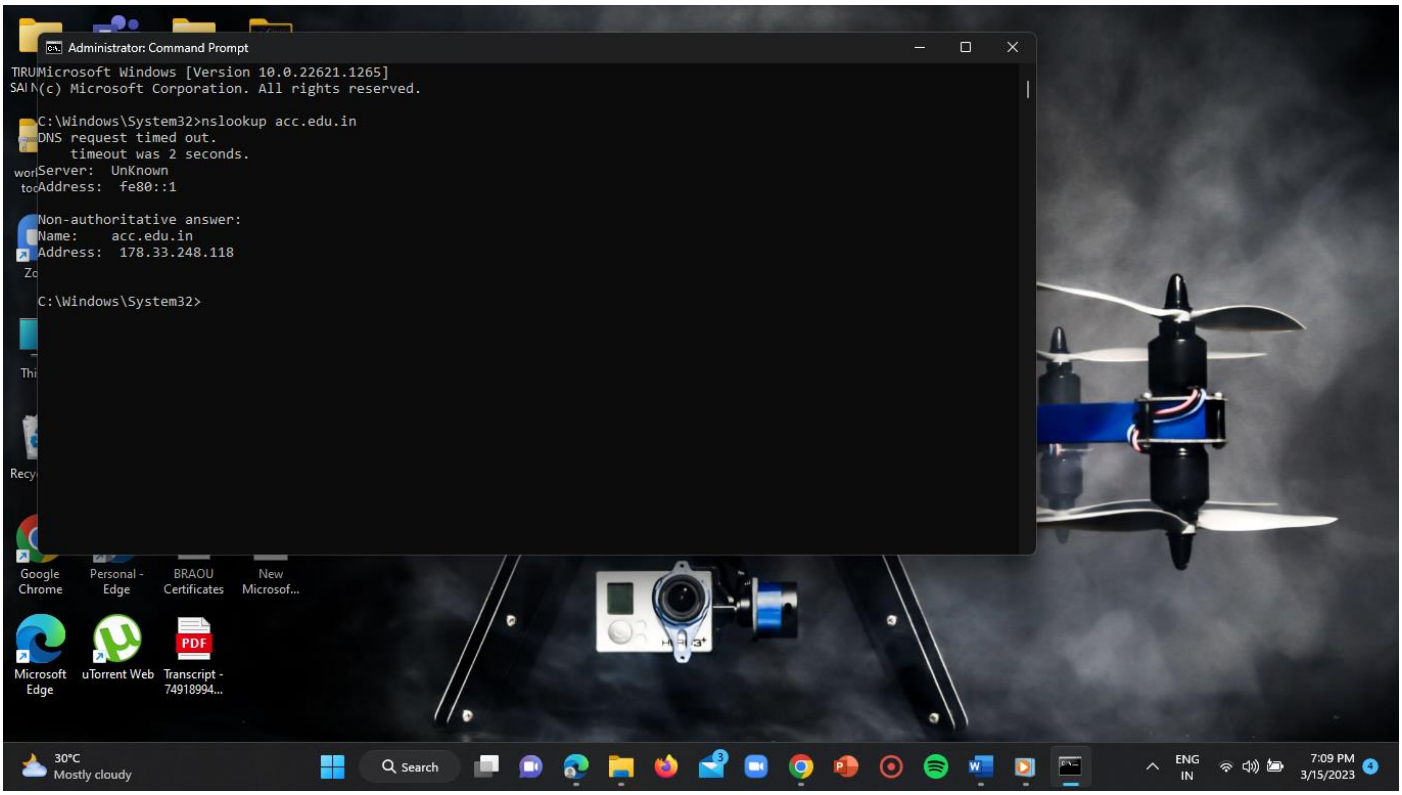


IP ADDRESS = 103.21.59.201

For DOMAIN-3:

ST#IS#4899

Type= nslookup acc.edu.in

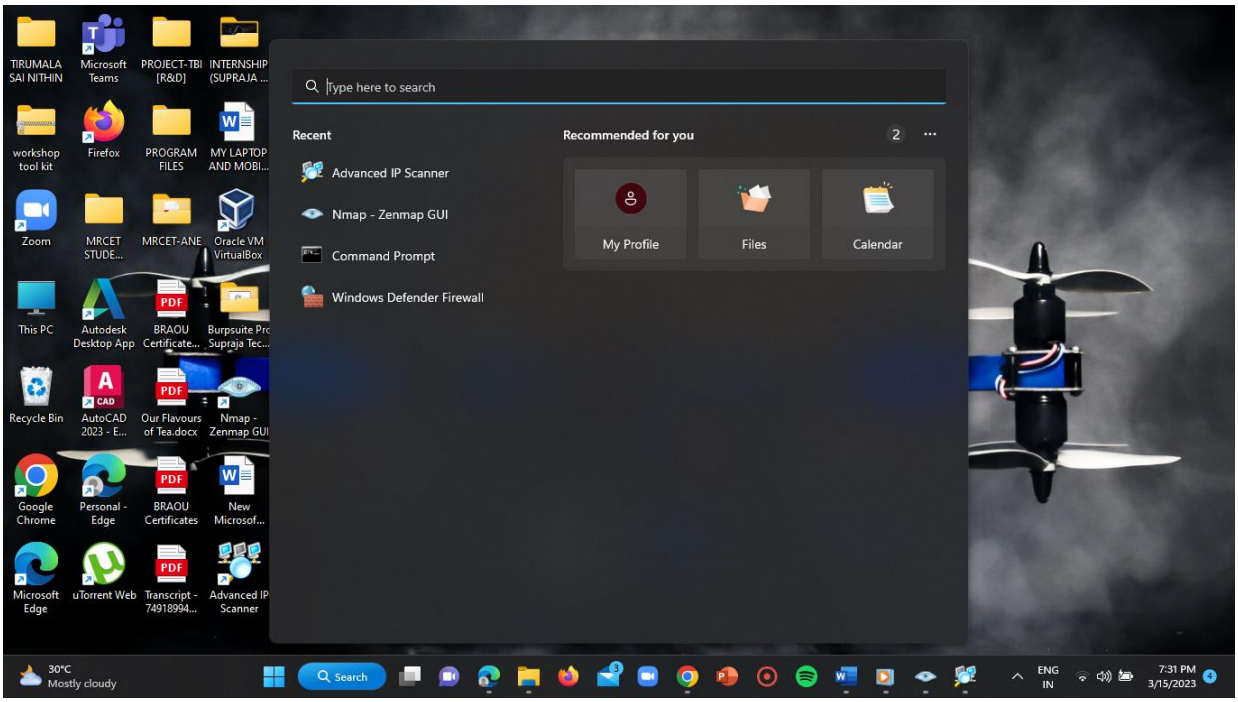


IP ADDRESS = 178.33.248.118

➔ Scanning the entire domain's IP addresses and finding the open ports.

STEP-1:

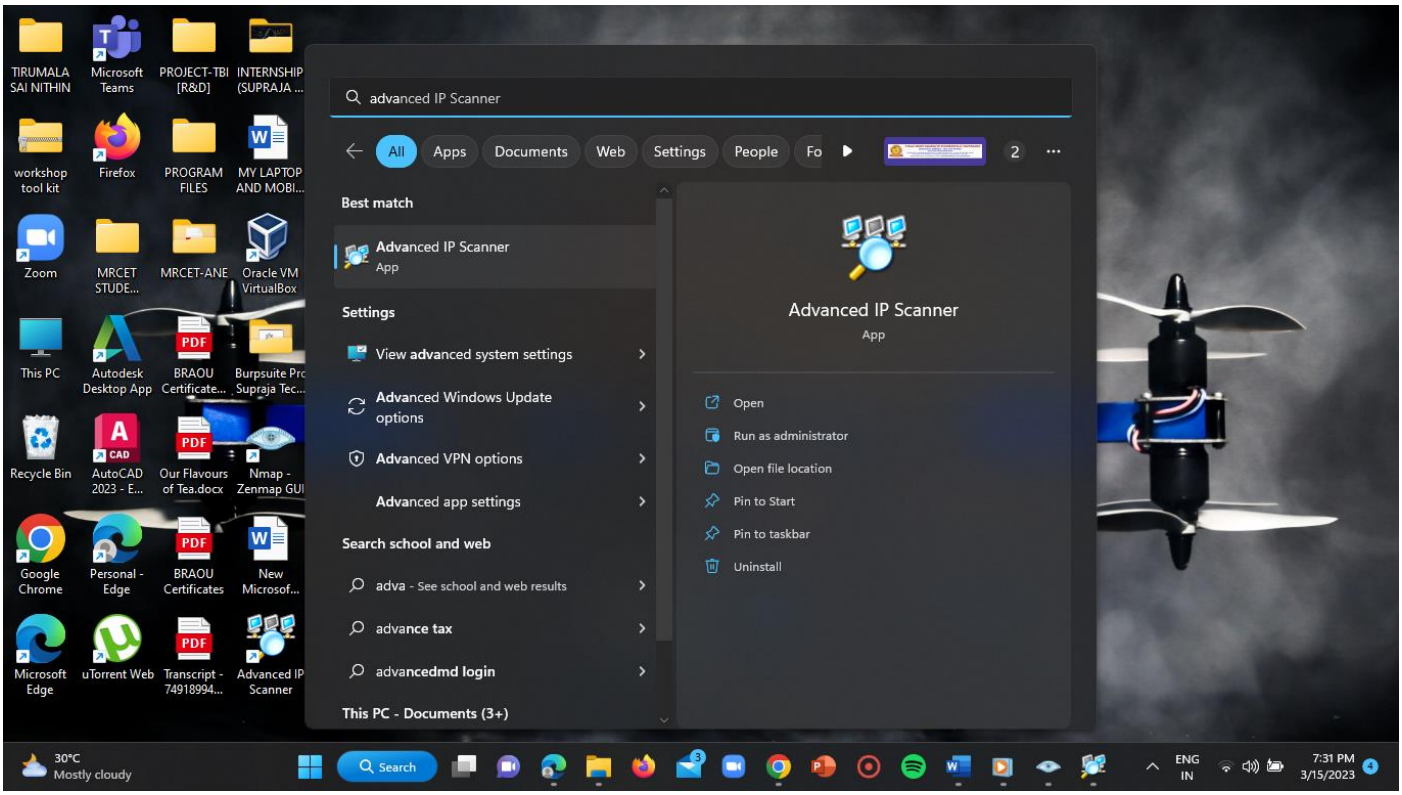
Click on start button.



STEP-2:

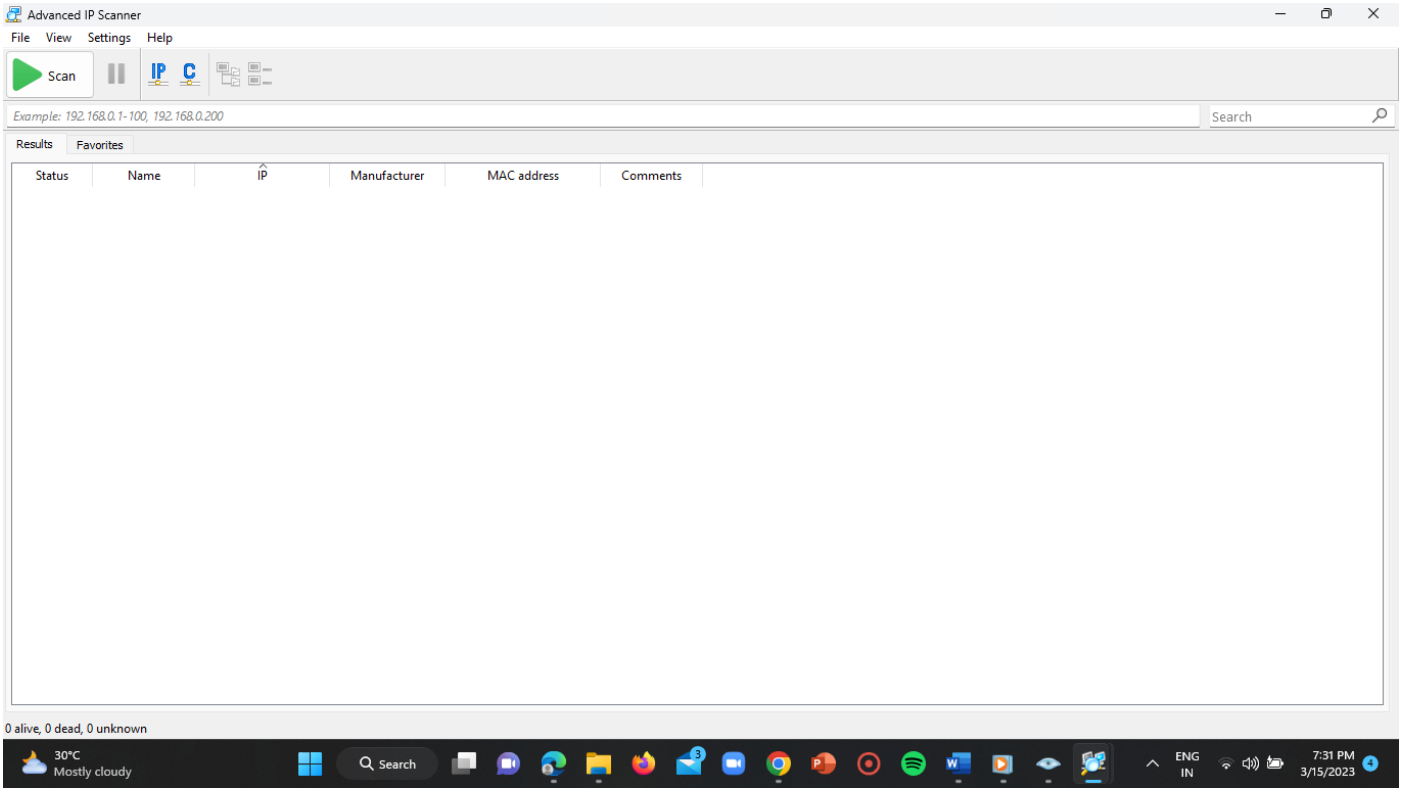
ST#IS#4899

In the search bar type “advanced IP scanner”.



STEP-3:

Open it in the ‘ADMININSTRATOR MODE’ by clicking on “run as administrator”.



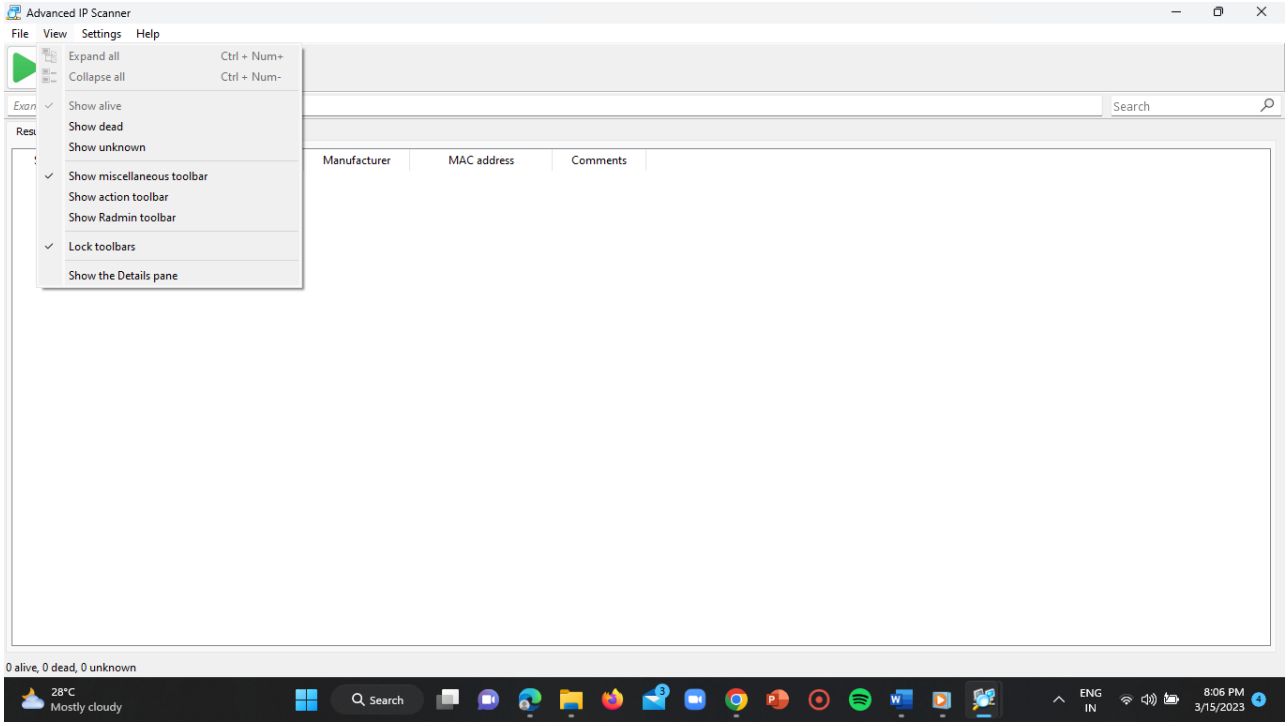
ST#IS#4899

STEP-4:

Now enter the IP address ranges in the IP address input bar of the application and click on scan.

STEP-5:

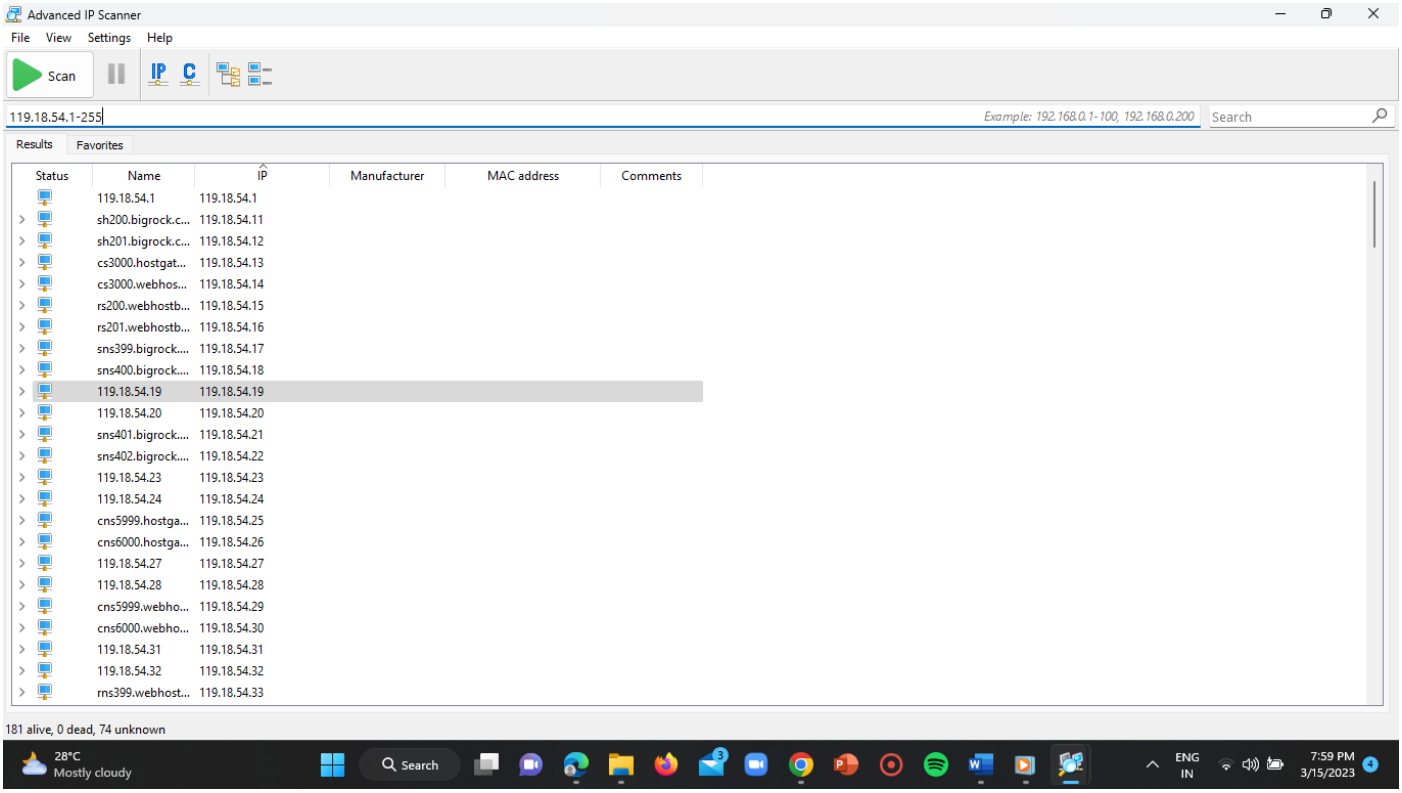
Make sure that in the view options only “show alive” option is enabled.



DOMAIN-1:

Range = 119.18.54.1-255

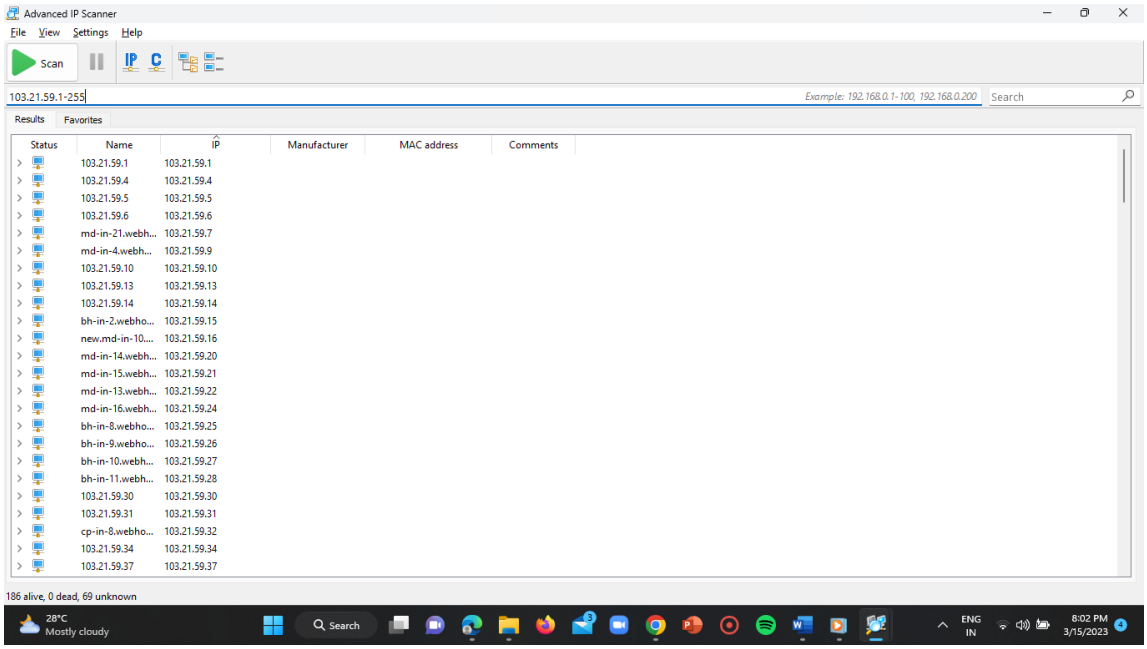
ST#IS#4899



NUMBER OF LIVE PORTS = 181

DOMAIN-2:

Range = 103.21.59.1-255

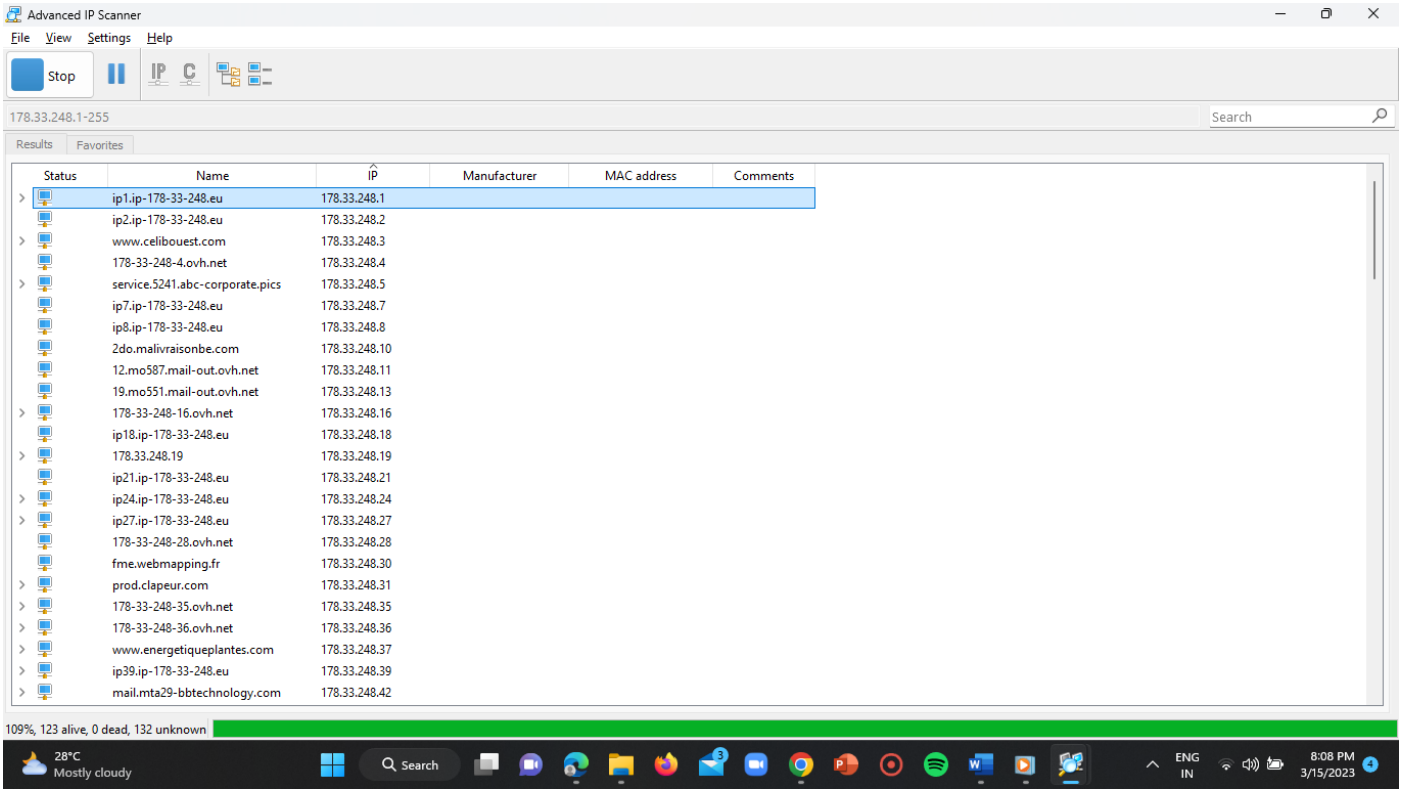


NUMBER OF LIVE PORTS = 186

DOMAIN-3:

Range = 178.33.248.1-255

ST#IS#4899



NUMBER OF LIVE PORTS = 123

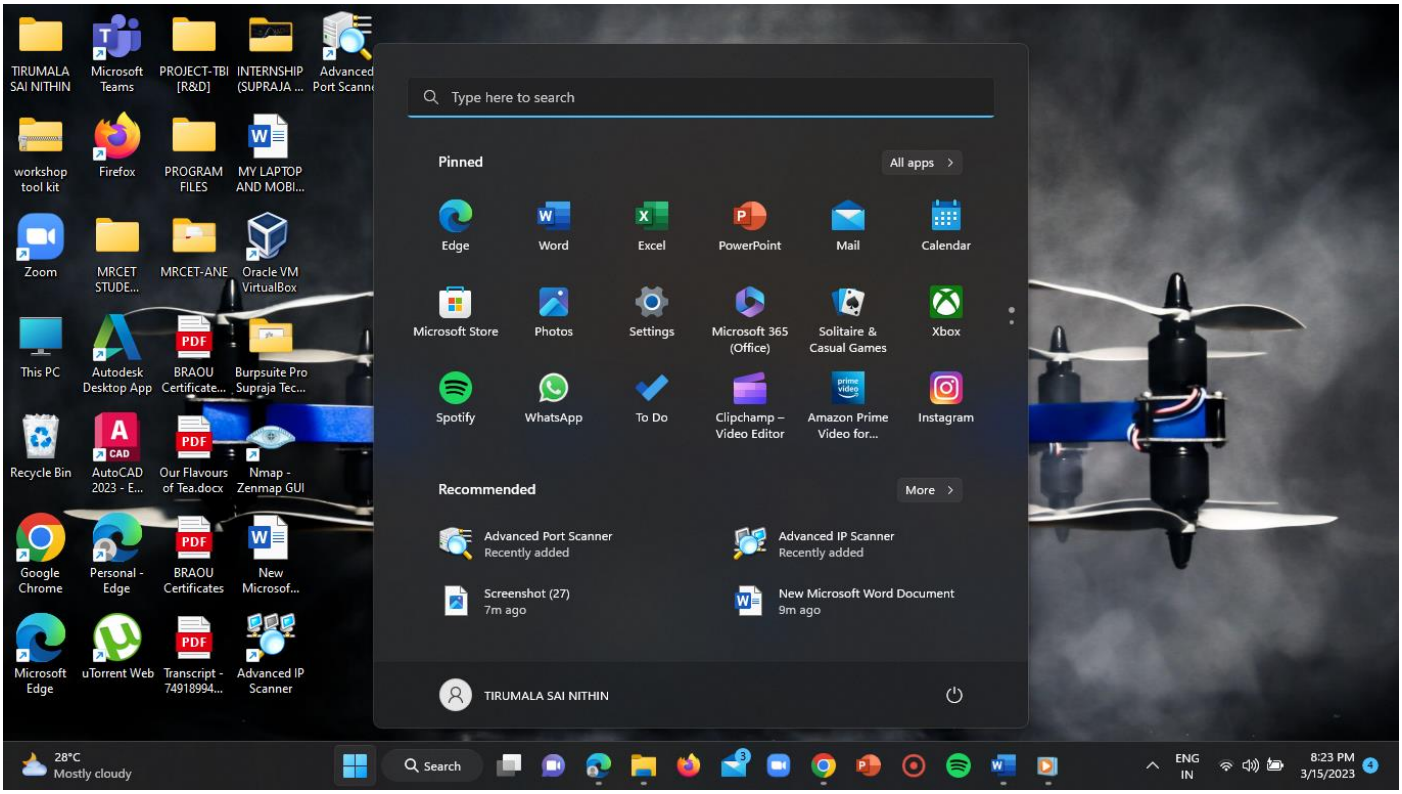
<u>ANSWER-2</u>:

➔ Filtering the IP addresses which are having the ports (22,80,3306) open from the scanned domain IP addresses.

STEP-1:

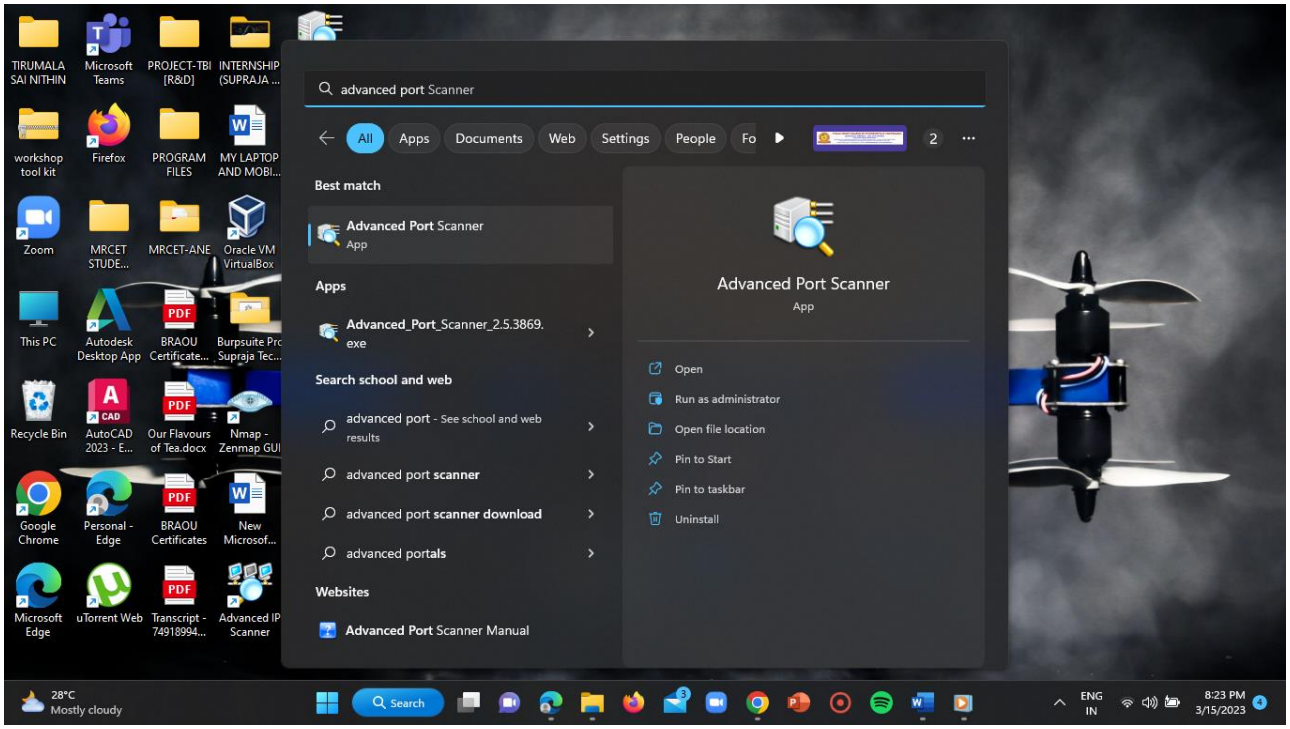
Click on start.

ST#IS#4899



STEP-2:

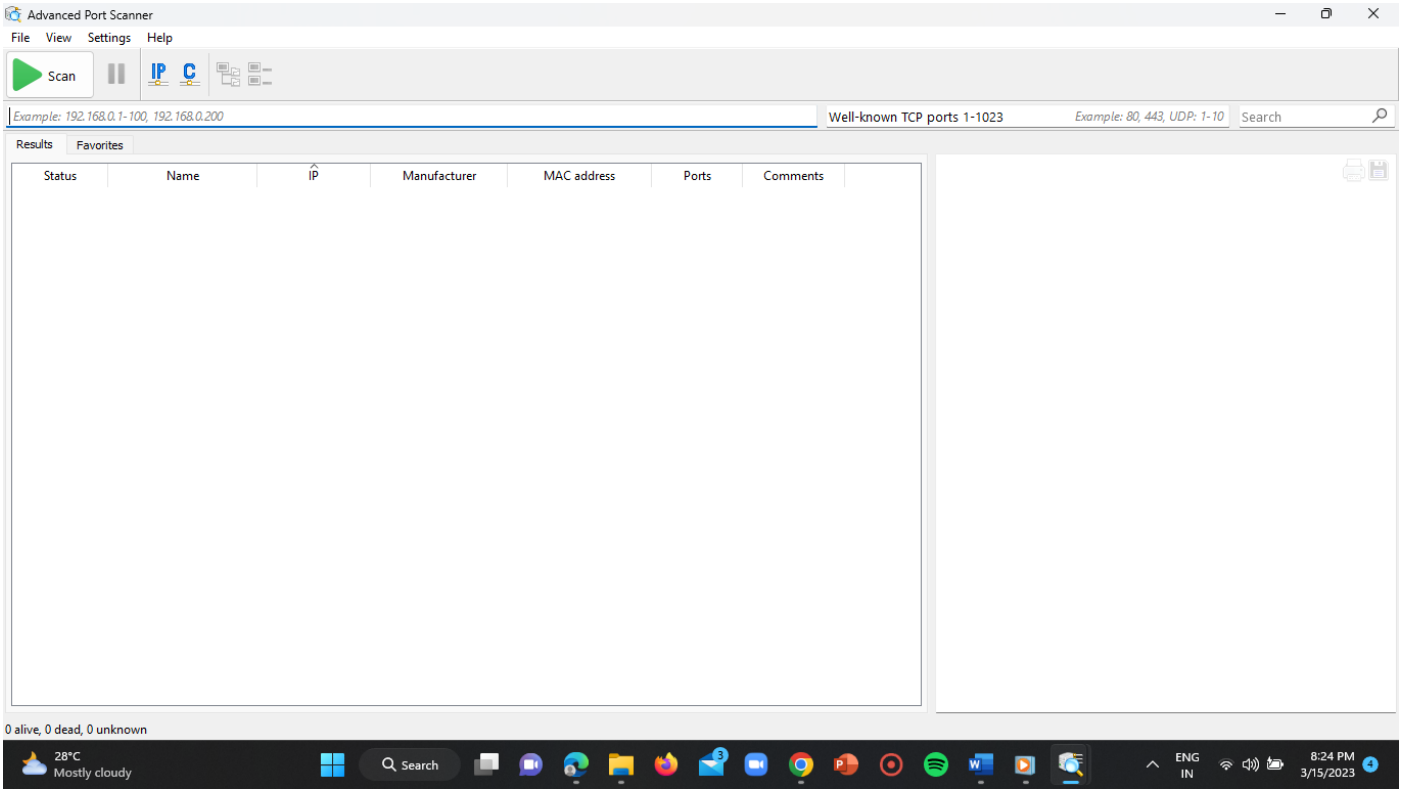
Type “advanced port scanner” in the search bar.



STEP-3:

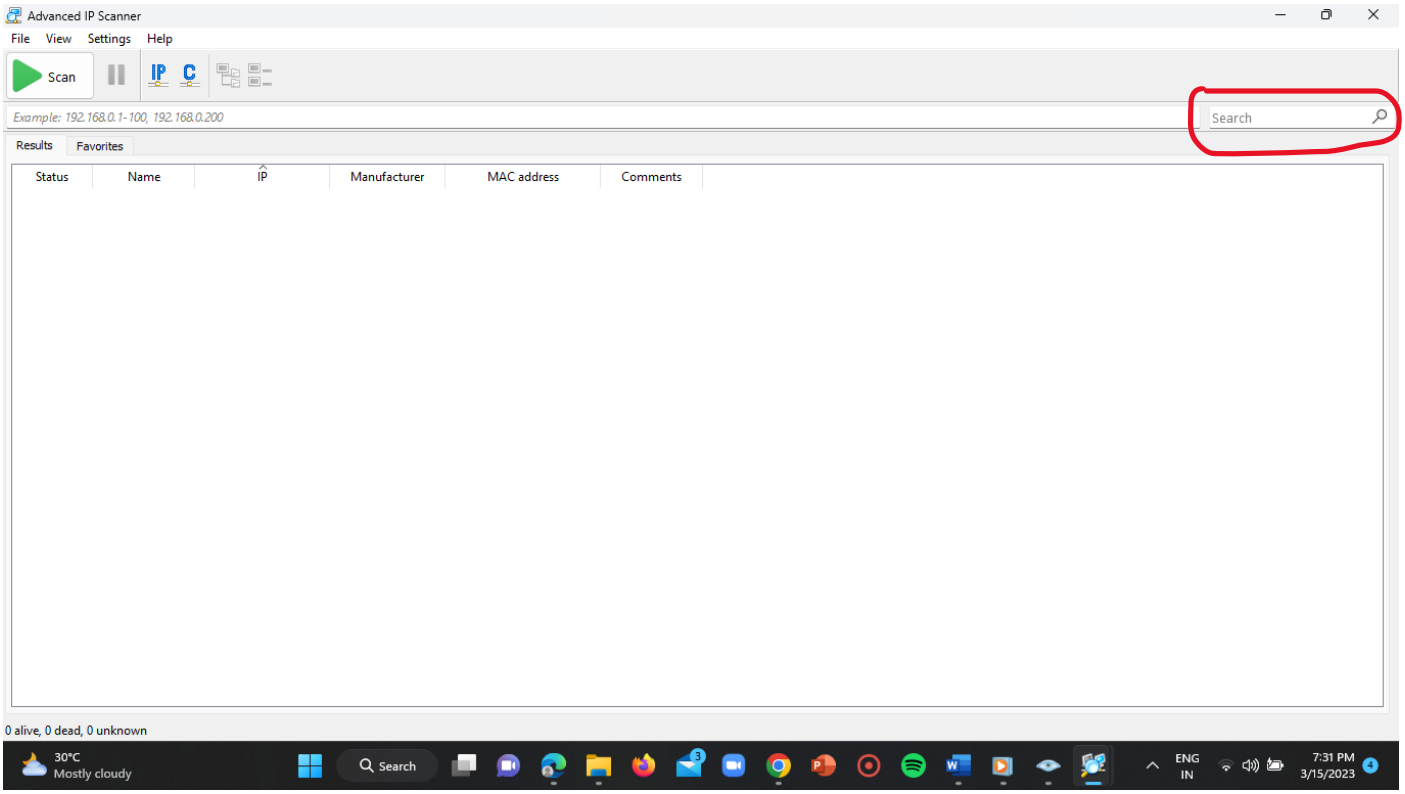
Open it in the ‘ADMINISTRATOR MODE’ by clicking on “run as administrator” and scan the target IP addresses.

ST#IS#4899



STEP-4:

Click on the search bar on the right corner of the advanced IP scanner.

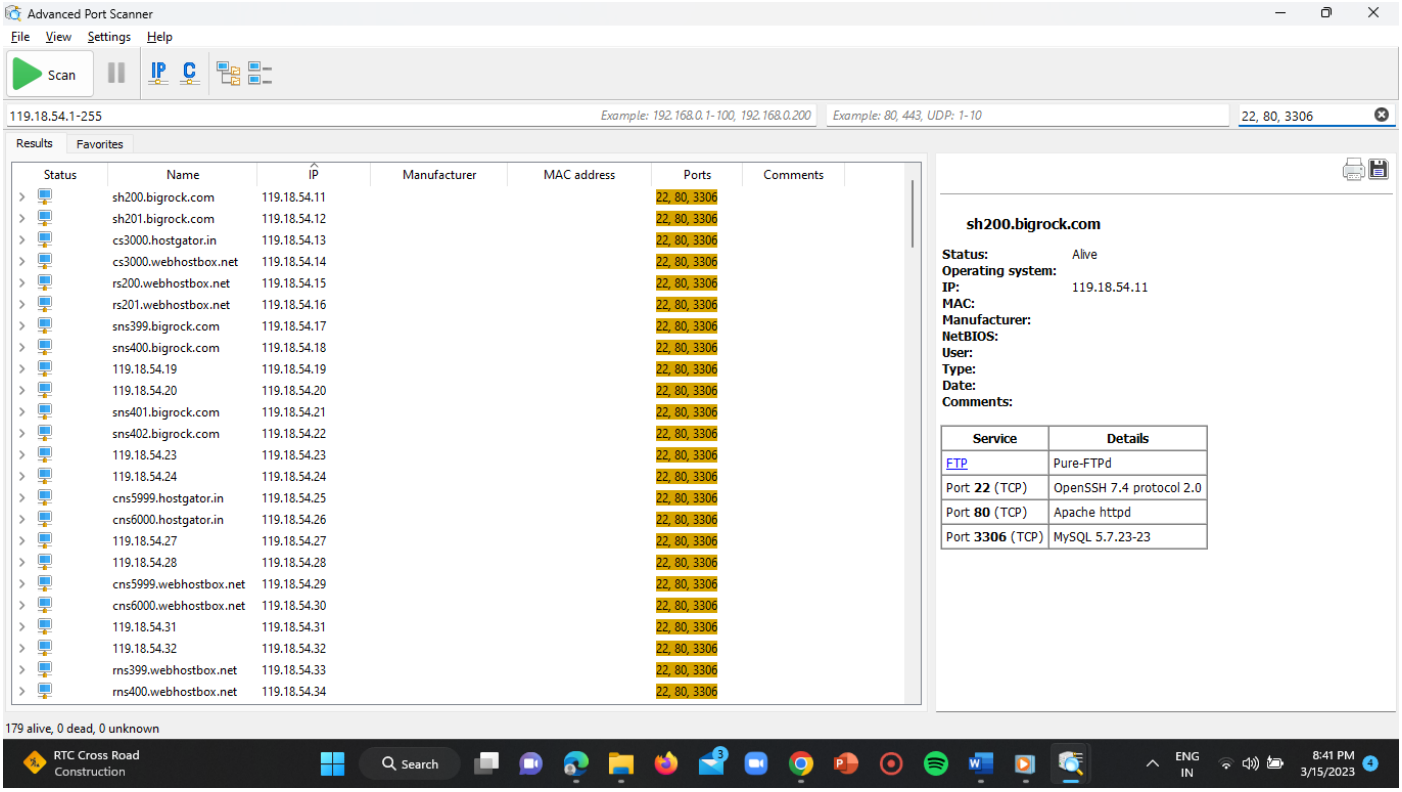


STEP-5:

ST#IS#4899

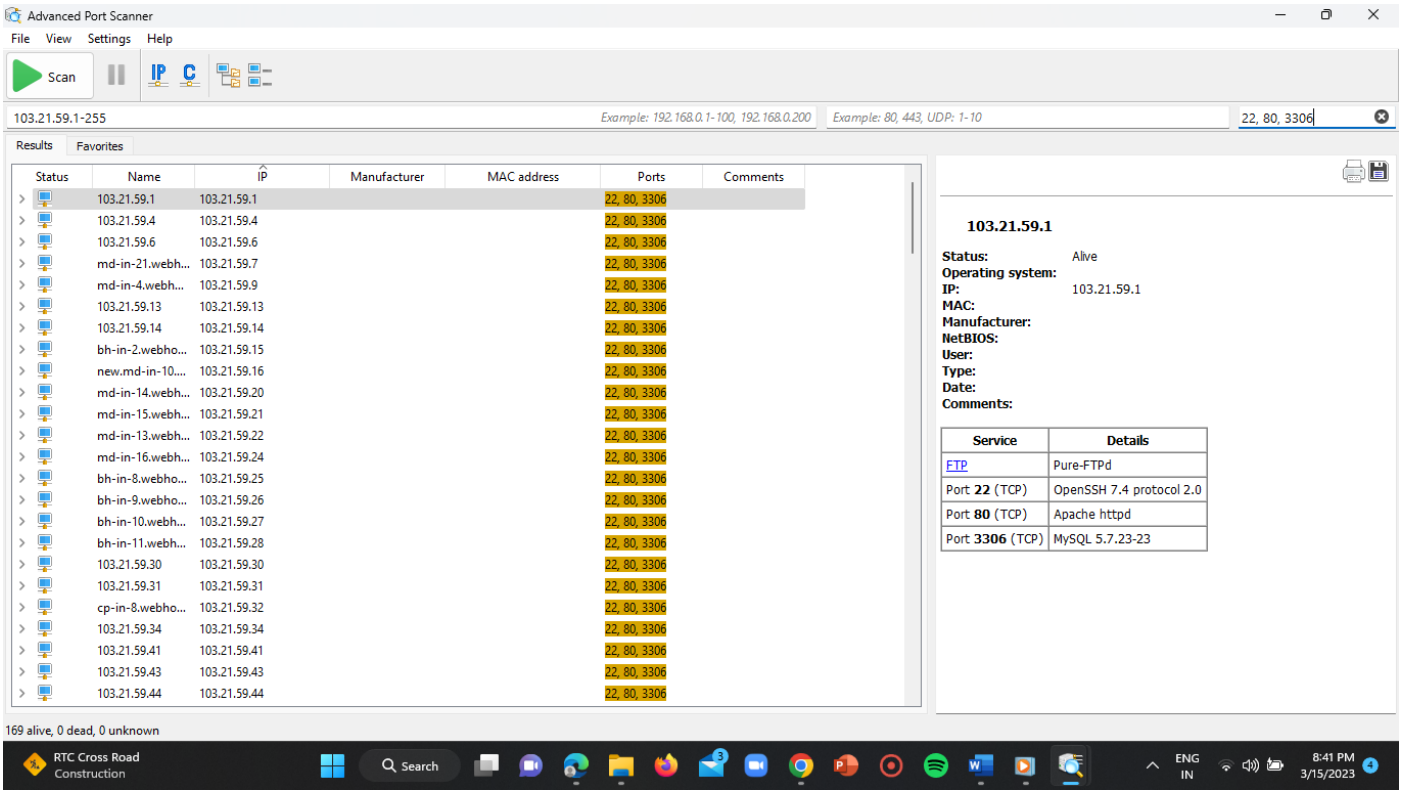
Now enter the port numbers = “22, 80, 3306” in the search bar and click on enter.

DOMAIN-1:



NUMBER OF PORTS = 179

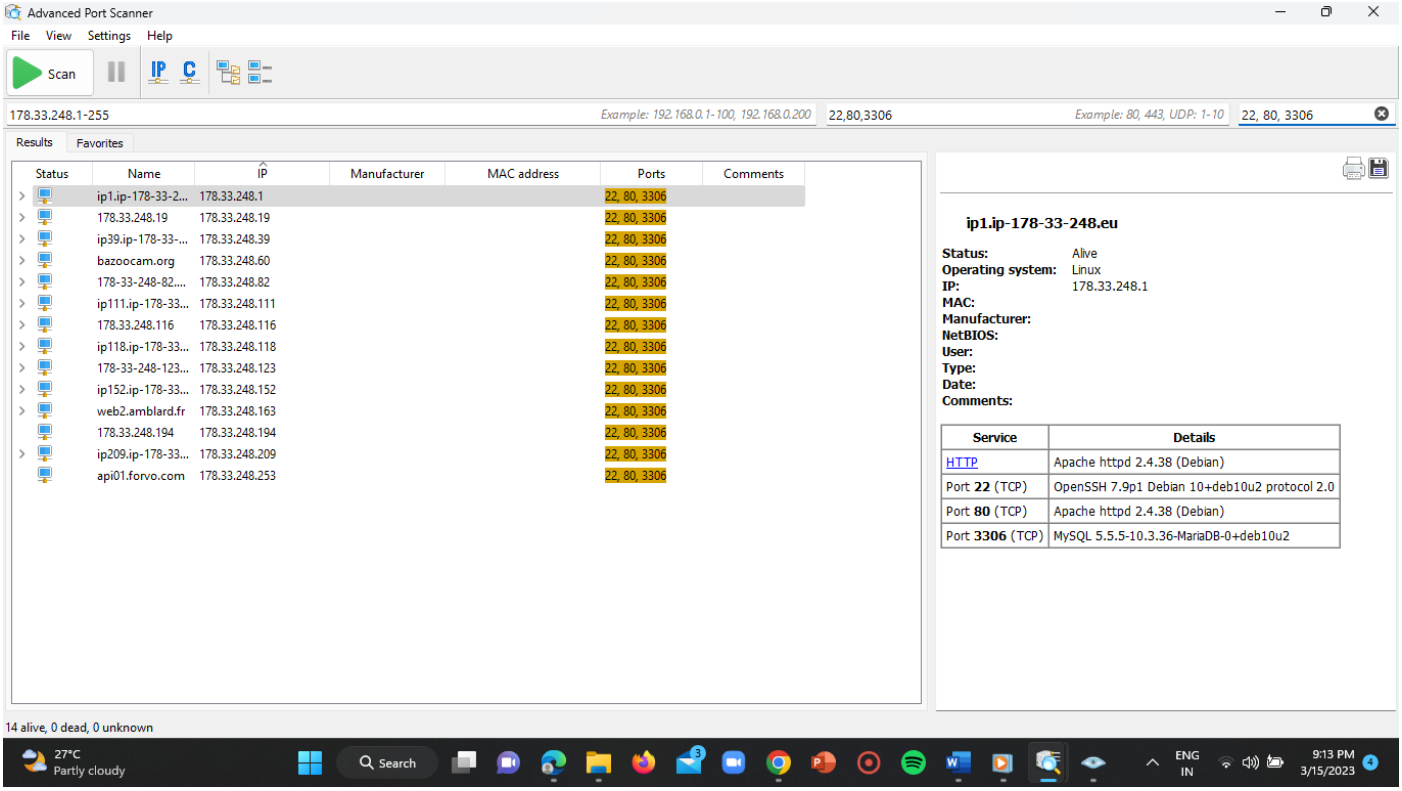
DOMAIN-2:



ST#IS#4899

NUMBER OF PORTS = 169

DOMAIN-3:



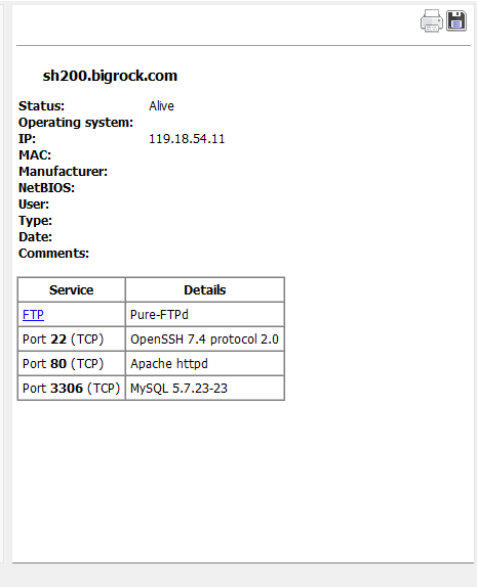
NUMBER OF PORTS = 14

<u>ANSWER-3</u>:

➔ Gathering the services and version details from the filtered ports with and without usage of the VPN.

<u>WITHOUT VPN</u>:

DOMAIN-1:



ST#IS#4899

DOMAIN-2:

103.21.59.1

Status: Alive
Operating system:
IP: 103.21.59.1
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	Pure-FTPd
Port **22** (TCP)	OpenSSH 7.4 protocol 2.0
Port **80** (TCP)	Apache httpd
Port **3306** (TCP)	MySQL 5.7.23-23

DOMAIN-3:

ip1.ip-178-33-248.eu

Status: Alive
Operating system: Linux
IP: 178.33.248.1
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
HTTP	Apache httpd 2.4.38 (Debian)
Port **22** (TCP)	OpenSSH 7.9p1 Debian 10+deb10u2 protocol 2.0
Port **80** (TCP)	Apache httpd 2.4.38 (Debian)
Port **3306** (TCP)	MySQL 5.5.5-10.3.36-MariaDB-0+deb10u2

<u>WITH VPN</u>:

DOMAIN-1:

119.18.54.1

Status: Alive
Operating system:
IP: 119.18.54.1
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	
Port **22** (TCP)	
Port **80** (TCP)	
Port **3306** (TCP)	

sh201.bigrock.com

Status: Alive
Operating system:
IP: 119.18.54.12
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	Pure-FTPd
Port **22** (TCP)	
Port **80** (TCP)	
Port **3306** (TCP)	

rs200.webhostbox.net

Status: Alive
Operating system:
IP: 119.18.54.15
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	Pure-FTPd
Port **22** (TCP)	OpenSSH 7.4 protocol 2.0
Port **80** (TCP)	
Port **3306** (TCP)	

119.18.54.146

Status: Alive
Operating system:
IP: 119.18.54.146
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	
Port **22** (TCP)	OpenSSH 7.4 protocol 2.0
Port **80** (TCP)	
Port **3306** (TCP)	

ST#IS#4899

DOMAIN-2:

103.21.59.1

Status: Alive
Operating system:
IP: 103.21.59.1
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	Pure-FTPd
Port **22** (TCP)	OpenSSH 7.4 protocol 2.0
Port **80** (TCP)	Apache httpd
Port **3306** (TCP)	

103.21.59.2

Status: Alive
Operating system:
IP: 103.21.59.2
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	
Port **22** (TCP)	
Port **80** (TCP)	
Port **3306** (TCP)	

md-in-21.webhostbox.net

Status: Alive
Operating system:
IP: 103.21.59.7
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	Pure-FTPd
Port **22** (TCP)	
Port **80** (TCP)	
Port **3306** (TCP)	

md-in-4.webhostbox.net

Status: Alive
Operating system:
IP: 103.21.59.9
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	Pure-FTPd
Port **22** (TCP)	OpenSSH 7.4 protocol 2.0
Port **80** (TCP)	
Port **3306** (TCP)	

103.21.59.81

Status: Alive
Operating system:
IP: 103.21.59.81
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	Pure-FTPd
Port **22** (TCP)	
Port **80** (TCP)	nginx 1.17.6
Port **3306** (TCP)	

103.21.59.99

Status: Alive
Operating system:
IP: 103.21.59.99
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	Pure-FTPd
Port **22** (TCP)	
Port **80** (TCP)	
Port **3306** (TCP)	

103.21.59.195

Status: Alive
Operating system:
IP: 103.21.59.195
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	
Port **22** (TCP)	OpenSSH 7.4 protocol 2.0
Port **80** (TCP)	nginx 1.17.6
Port **3306** (TCP)	

103.21.59.82

Status: Alive
Operating system:
IP: 103.21.59.82
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	
Port **22** (TCP)	
Port **80** (TCP)	Apache httpd
Port **3306** (TCP)	

103.21.59.194

Status: Alive
Operating system:
IP: 103.21.59.194
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	
Port **22** (TCP)	OpenSSH 7.4 protocol 2.0
Port **80** (TCP)	Apache httpd
Port **3306** (TCP)	

103.21.59.224

Status: Alive
Operating system:
IP: 103.21.59.224
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	
Port **22** (TCP)	
Port **80** (TCP)	nginx 1.17.6
Port **3306** (TCP)	

DOMAIN-3:

ST#IS#4899

ip1.ip-178-33-248.eu

Status: Alive
Operating system: Linux
IP: 178.33.248.1
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
HTTP	Apache httpd 2.4.38 (Debian)
FTP	
Port **22** (TCP)	OpenSSH 7.9p1 Debian 10+deb10u2 protocol 2.0
Port **80** (TCP)	Apache httpd 2.4.38 (Debian)
Port **3306** (TCP)	

ip2.ip-178-33-248.eu

Status: Alive
Operating system:
IP: 178.33.248.2
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	
Port **22** (TCP)	
Port **80** (TCP)	
Port **3306** (TCP)	

www.celibouest.com

Status: Alive
Operating system: Linux
IP: 178.33.248.3
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	ftp
Port **22** (TCP)	OpenSSH 7.9p1 Debian 10+deb10u2 protocol 2.0
Port **80** (TCP)	Apache httpd
Port **3306** (TCP)	

178.33.248.16

Status: Alive
Operating system:
IP: 178.33.248.16
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
HTTP	403 Forbidden (Apache)
FTP	
Port **22** (TCP)	
Port **80** (TCP)	
Port **3306** (TCP)	

ip18.ip-178-33-248.eu

Status: Alive
Operating system: Windows
IP: 178.33.248.18
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
FTP	
Port **22** (TCP)	
Port **80** (TCP)	Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
Port **3306** (TCP)	

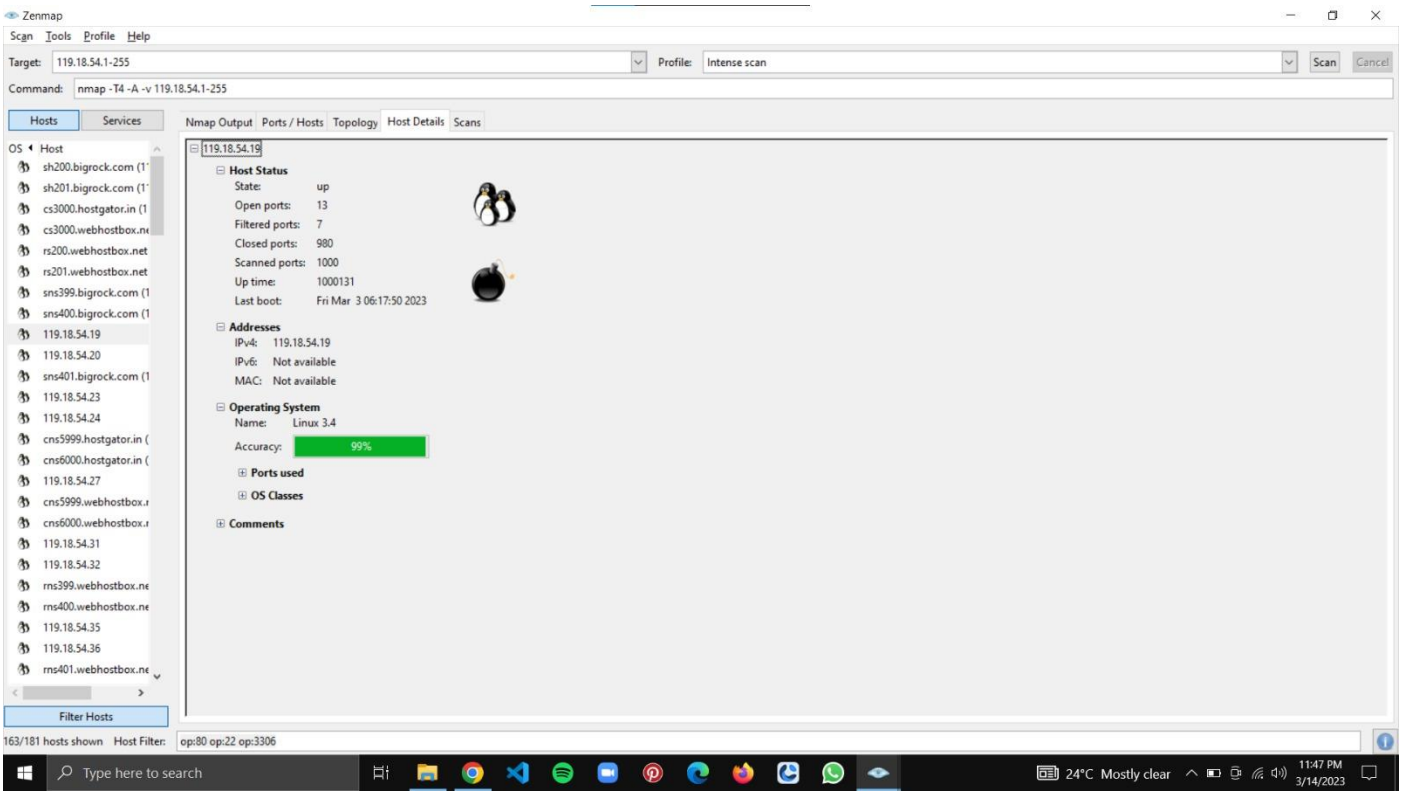
ip251.ip-178-33-248.eu

Status: Alive
Operating system:
IP: 178.33.248.251
MAC:
Manufacturer:
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
HTTP	Apache HTTP Server Test Page powered by CentOS (Apache httpd 2.2.15 (CentOS))
FTP	
Port **22** (TCP)	OpenSSH 5.3 protocol 2.0
Port **80** (TCP)	Apache httpd 2.2.15 (CentOS)
Port **3306** (TCP)	

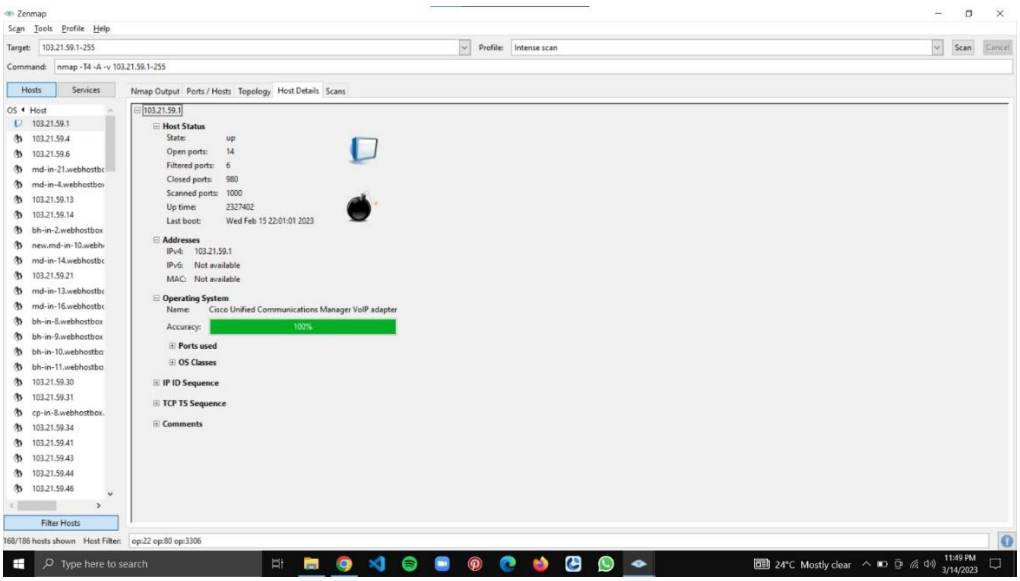
➔ Gathering the banner and operating system details of the filtered IP addresses of the target domains.

DOMAIN-1:



DOMAIN-2:

ST#IS#4899

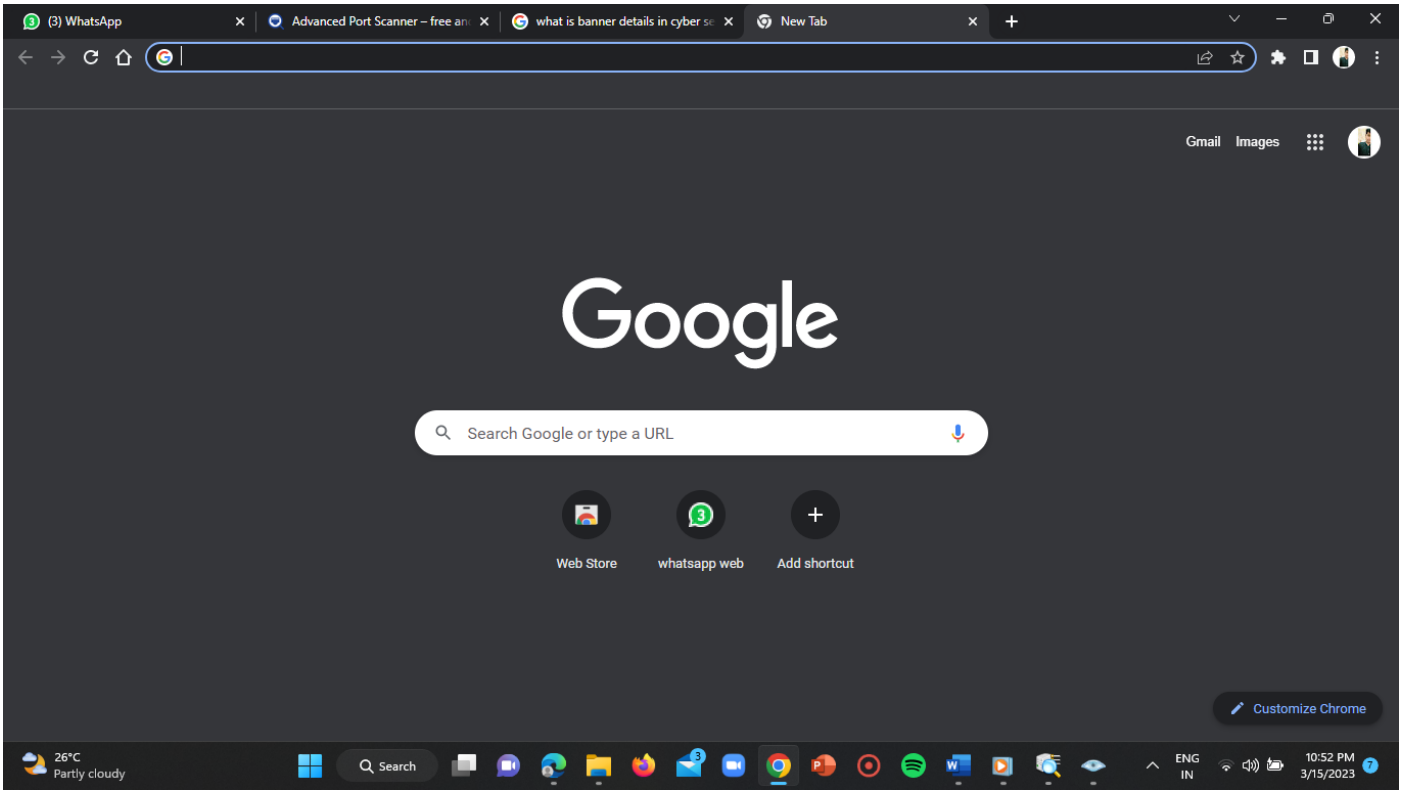


DOMAIN-3:

We have an alternative method to find the banner details of a target IP by using a site called “sitereport.netcraft.com” other than using the ‘n-map’.

STEP-1:

Open google chrome.

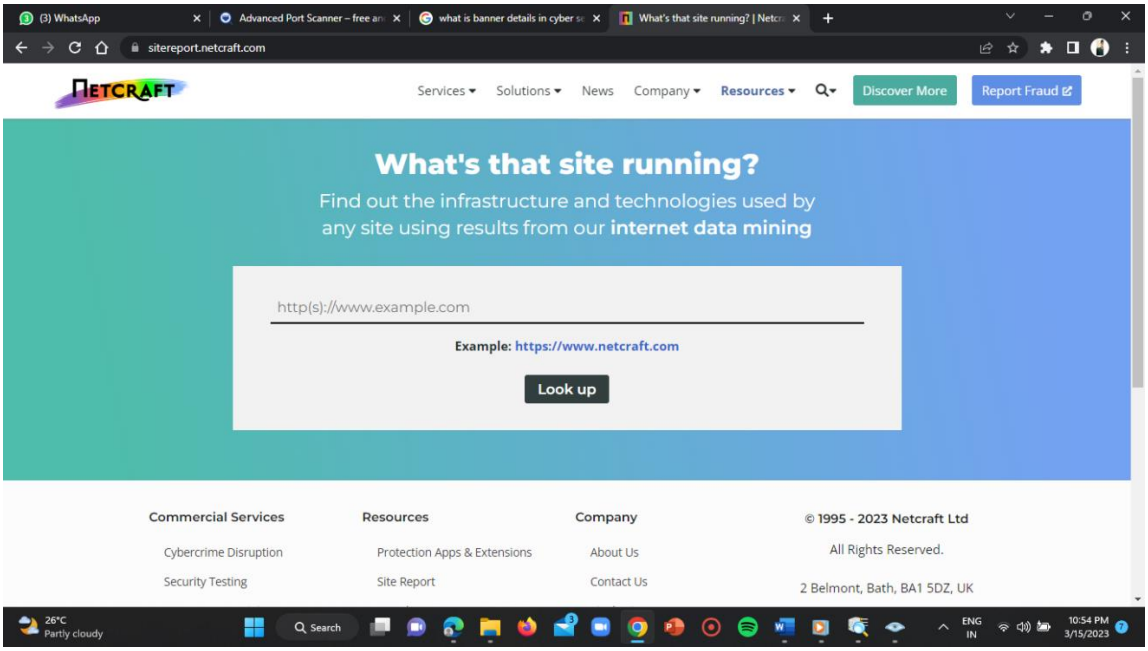


STEP-2:

Enter the link for the website i.e,

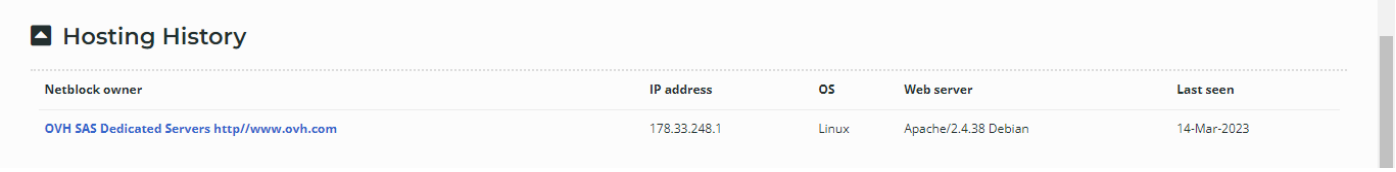
LINK = https://sitereport.netcraft.com/

ST#IS#4899



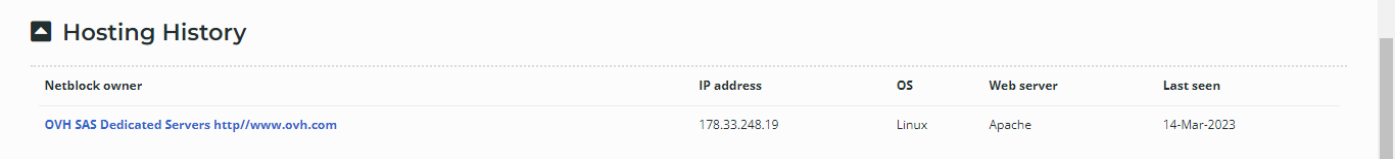
STEP-3:

Enter the filtered IP addresses in the search input bar in the homepage of the website.



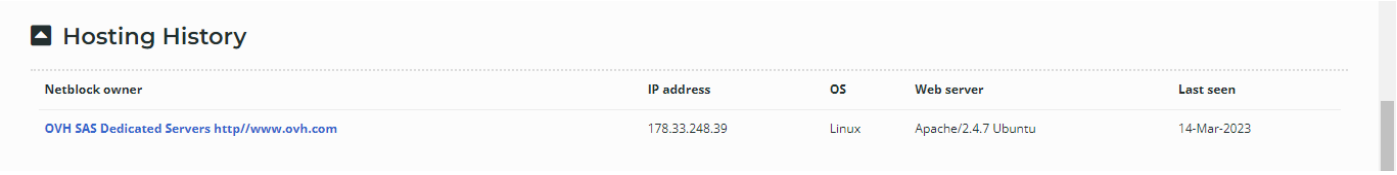
Hosting History

Netblock owner	IP address	OS	Web server	Last seen
OVH SAS Dedicated Servers http//www.ovh.com	178.33.248.1	Linux	Apache/2.4.38 Debian	14-Mar-2023



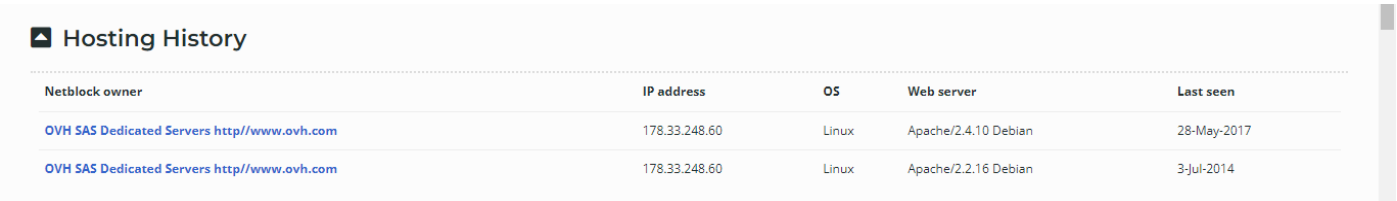
Hosting History

Netblock owner	IP address	OS	Web server	Last seen
OVH SAS Dedicated Servers http//www.ovh.com	178.33.248.19	Linux	Apache	14-Mar-2023



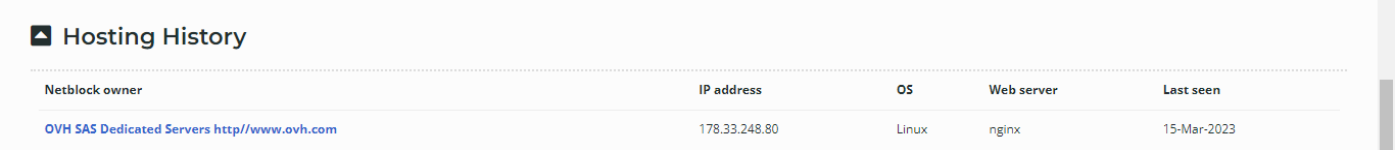
Hosting History

Netblock owner	IP address	OS	Web server	Last seen
OVH SAS Dedicated Servers http//www.ovh.com	178.33.248.39	Linux	Apache/2.4.7 Ubuntu	14-Mar-2023



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
OVH SAS Dedicated Servers http//www.ovh.com	178.33.248.60	Linux	Apache/2.4.10 Debian	28-May-2017
OVH SAS Dedicated Servers http//www.ovh.com	178.33.248.60	Linux	Apache/2.2.16 Debian	3-Jul-2014



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
OVH SAS Dedicated Servers http//www.ovh.com	178.33.248.80	Linux	nginx	15-Mar-2023

Conclusion:

A port number is a way to identify a specific process to which an internet or other network message is to be forwarded when it arrives at a server.

Ports are needed so that traffic coming from different applications on different sources can simultaneously reach the same host.

Here in this task I've used the below mentioned tools:

1) nslookup
2) advanced IP scanner
3) advanced port scanner
4) nmap
5) proton VPN
6) netcraft