

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.

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

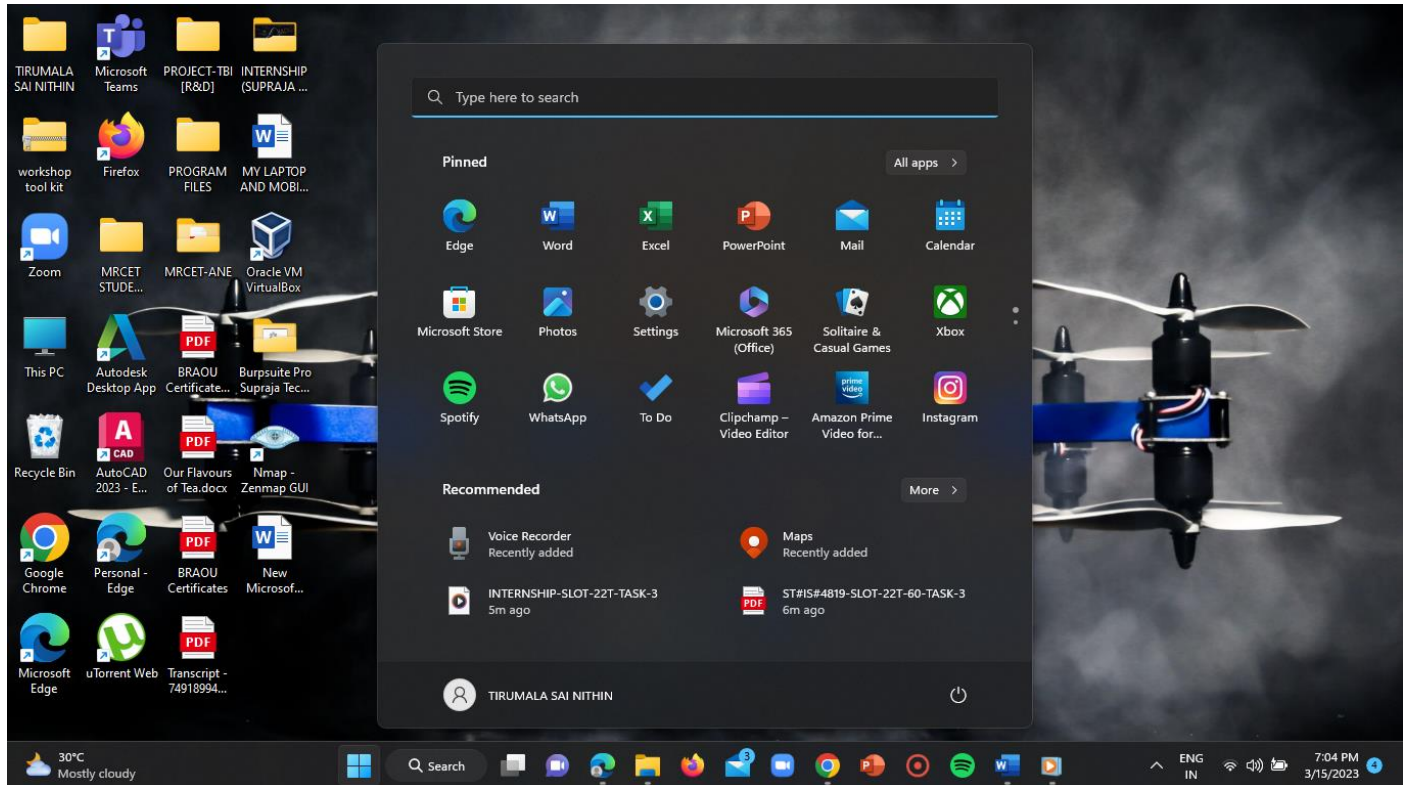
2) cmrec.ac.in

3) acc.edu.in

STEP-2:

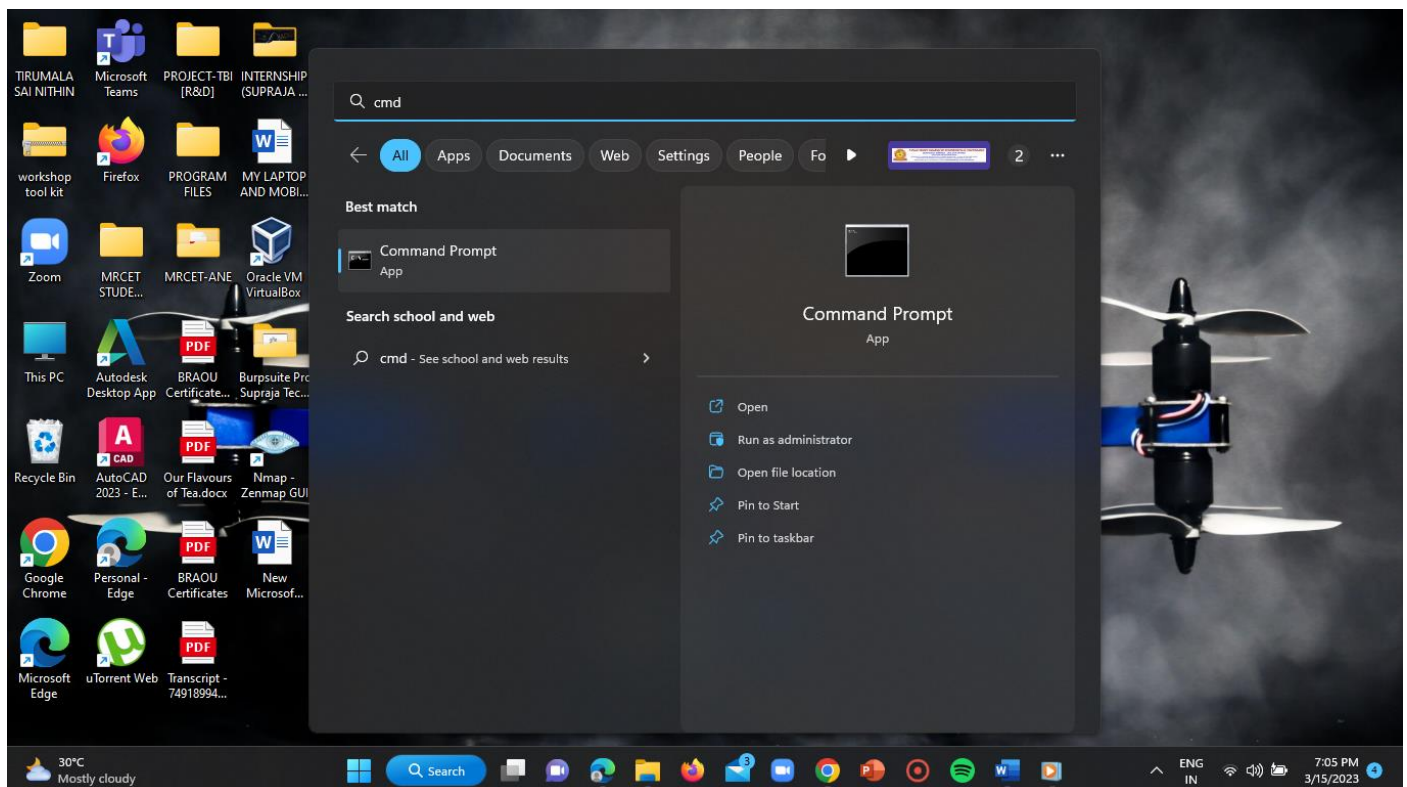
Now click on start.

ST#IS#4899



STEP-3:

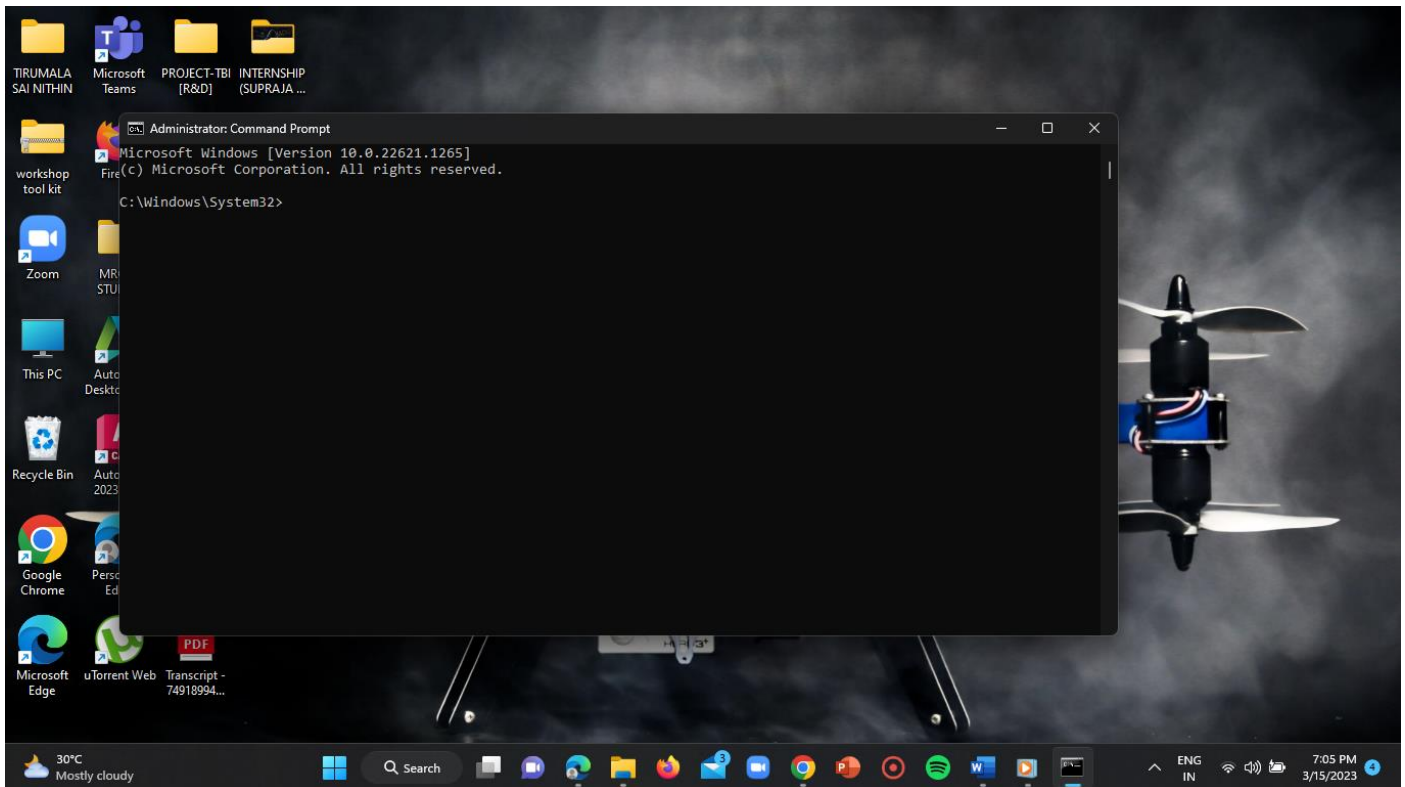
In the search bar enter "cmd".



STEP-4:

ST#IS#4899

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



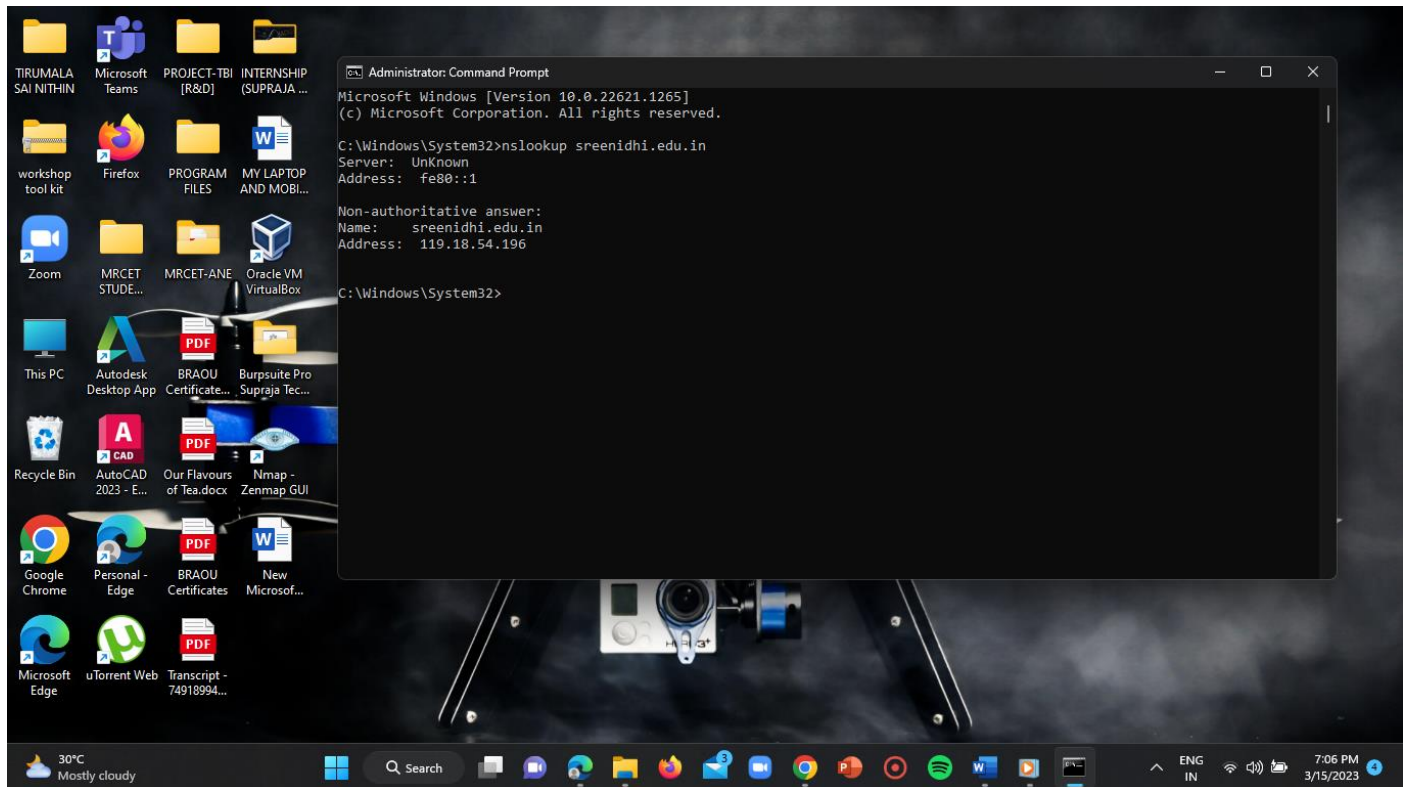
STEP-5:

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

For DOMAIN-1:

Type= nslookup sreenidhi.edu.in

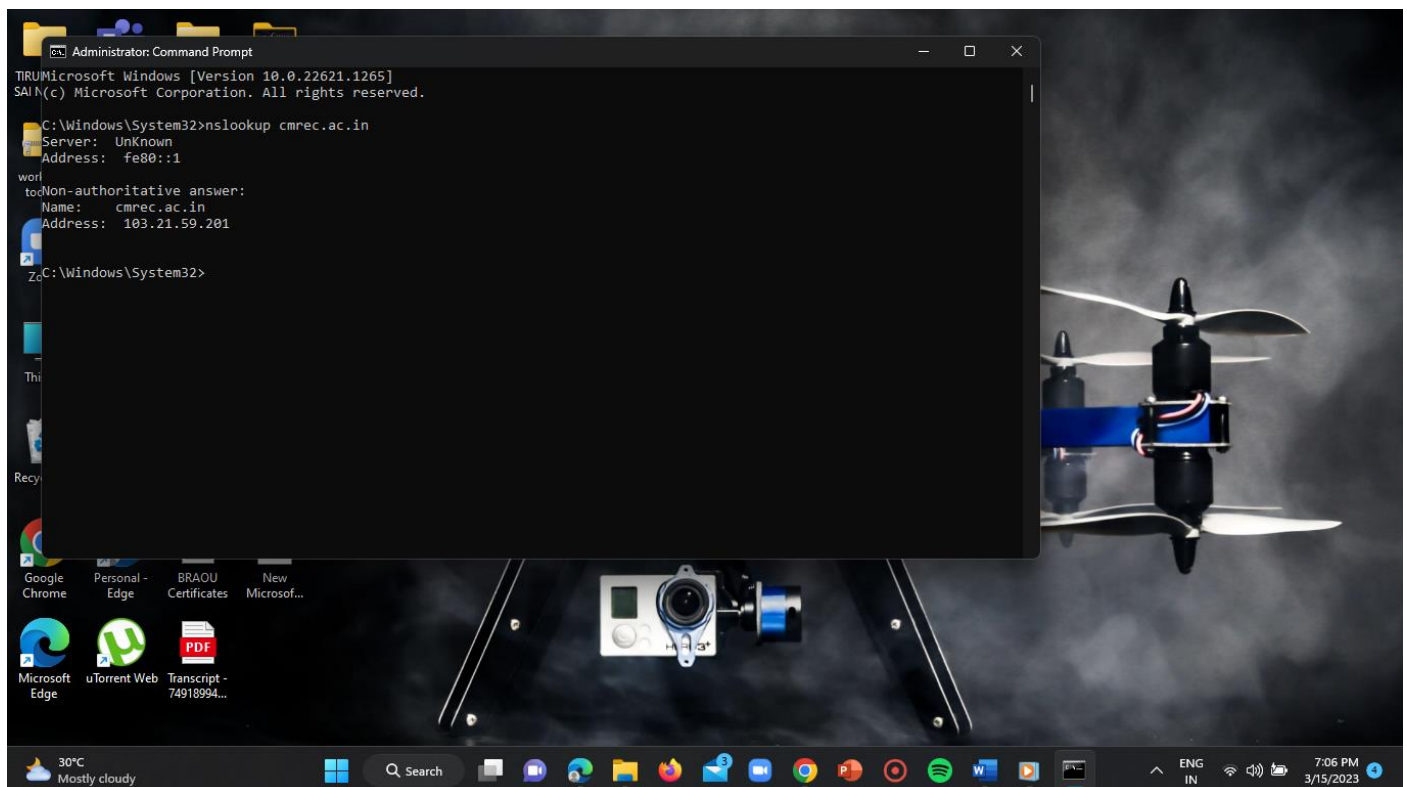
ST#IS#4899



IP ADDRESS = 119.18.54.196

For DOMAIN-2:

Type= nslookup cmrec.ac.in

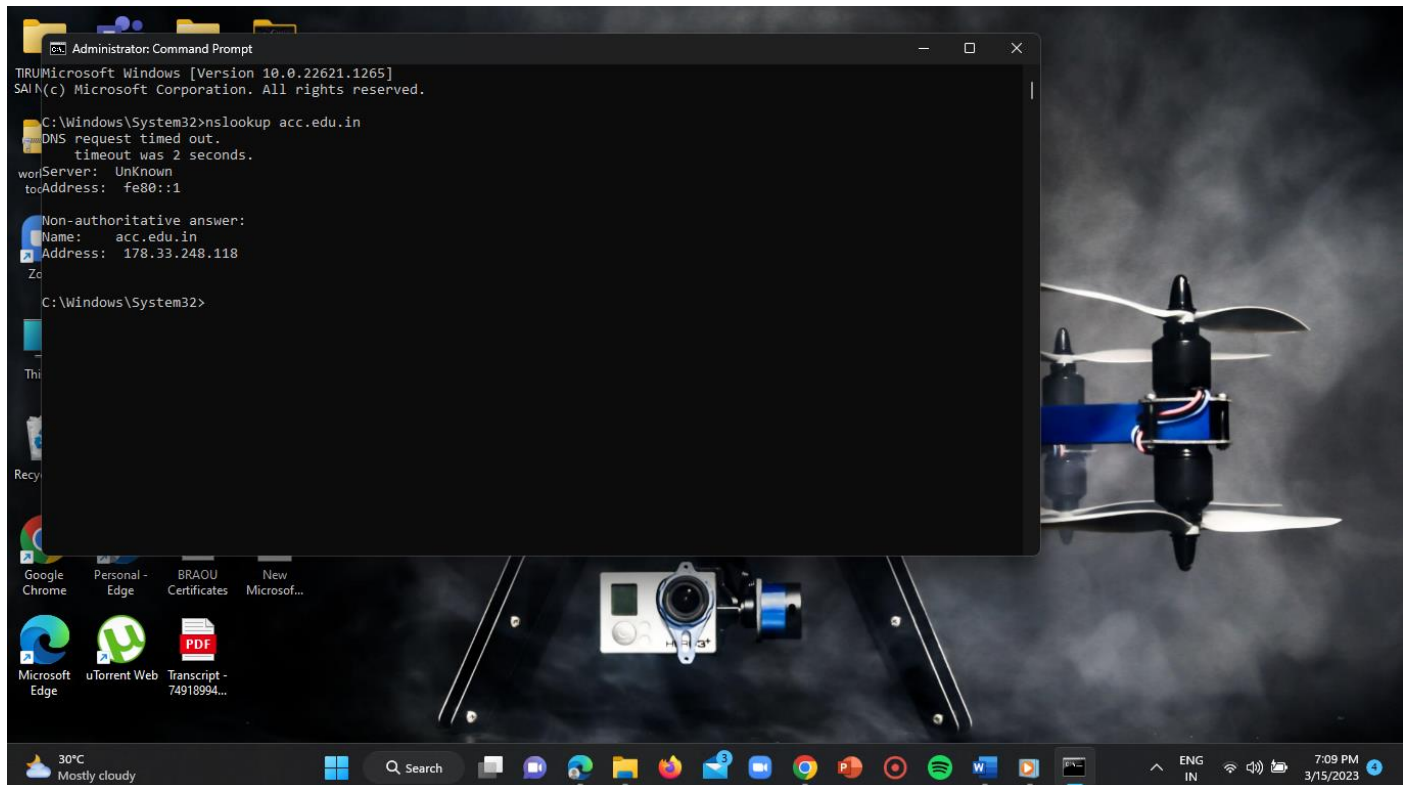


IP ADDRESS = 103.21.59.201

For DOMAIN-3:

ST#IS#4899

Type= nslookup acc.edu.in

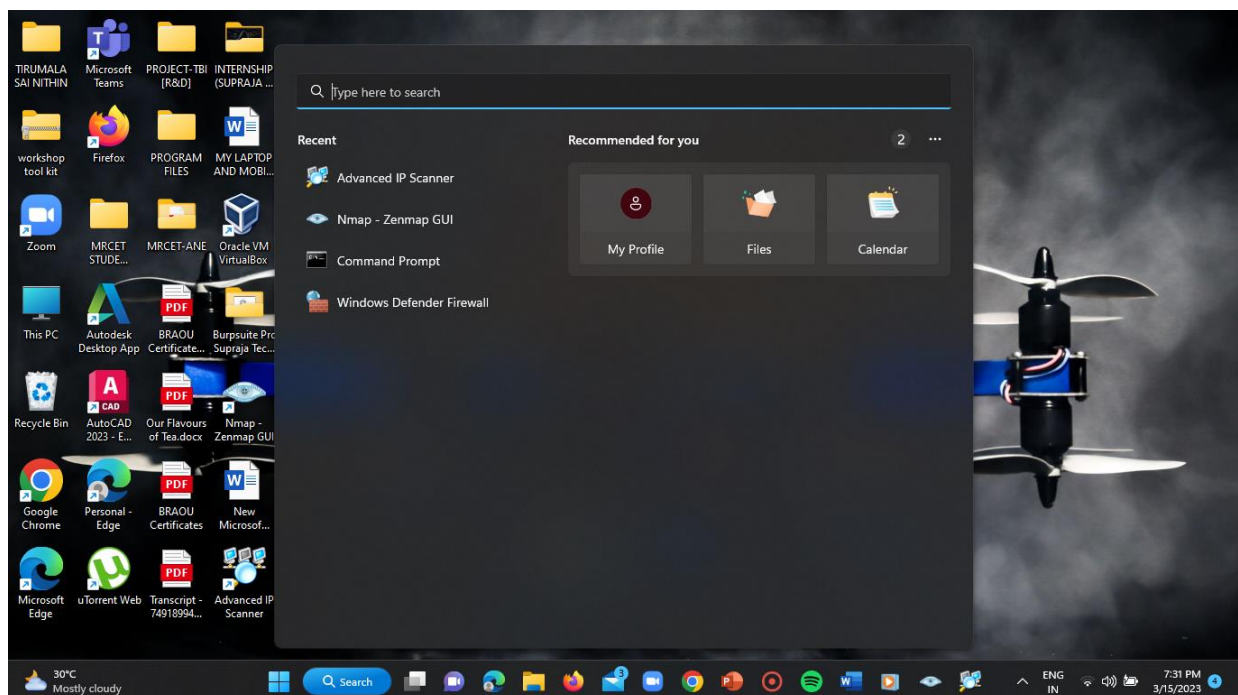


IP ADDRESS = 178.33.248.118

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

STEP-1:

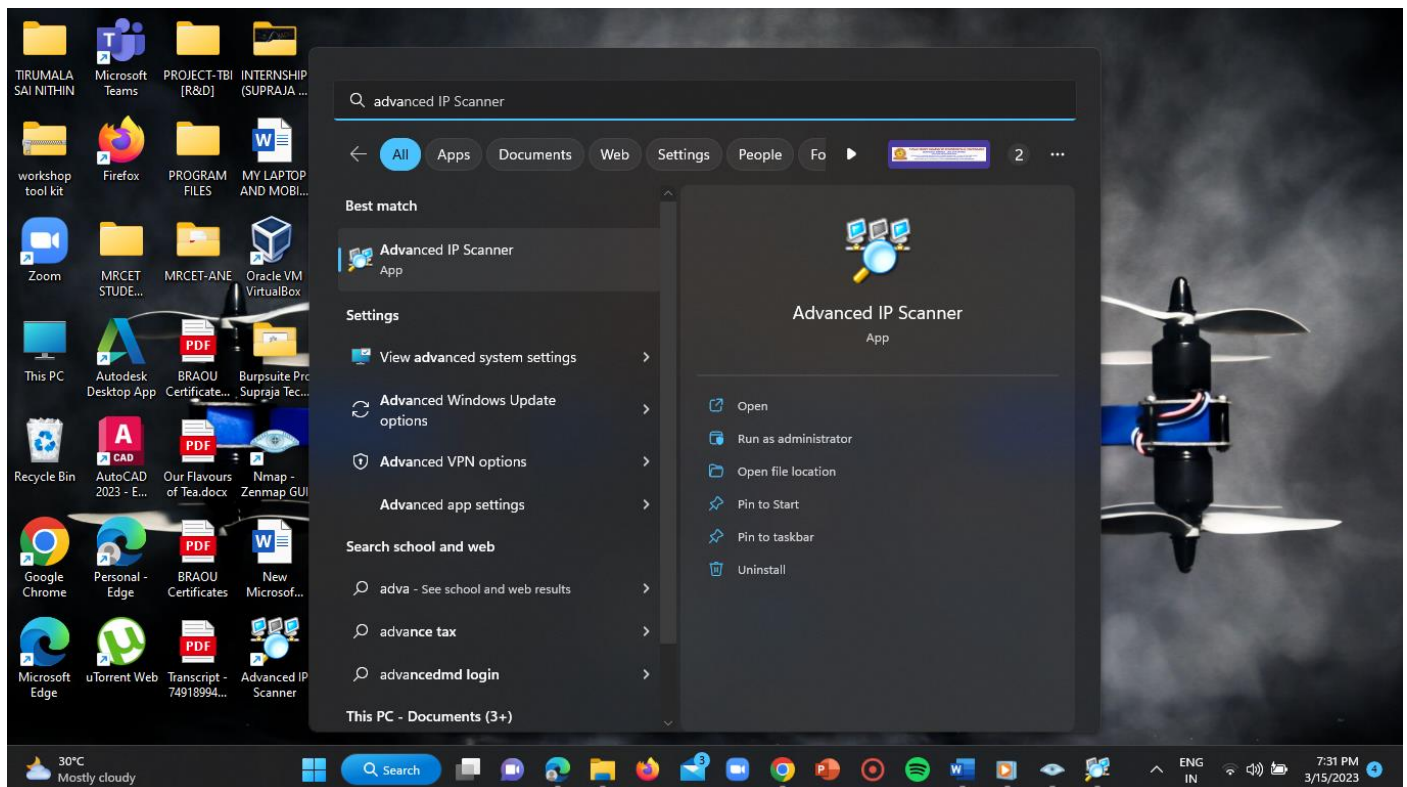
Click on start button.



STEP-2:

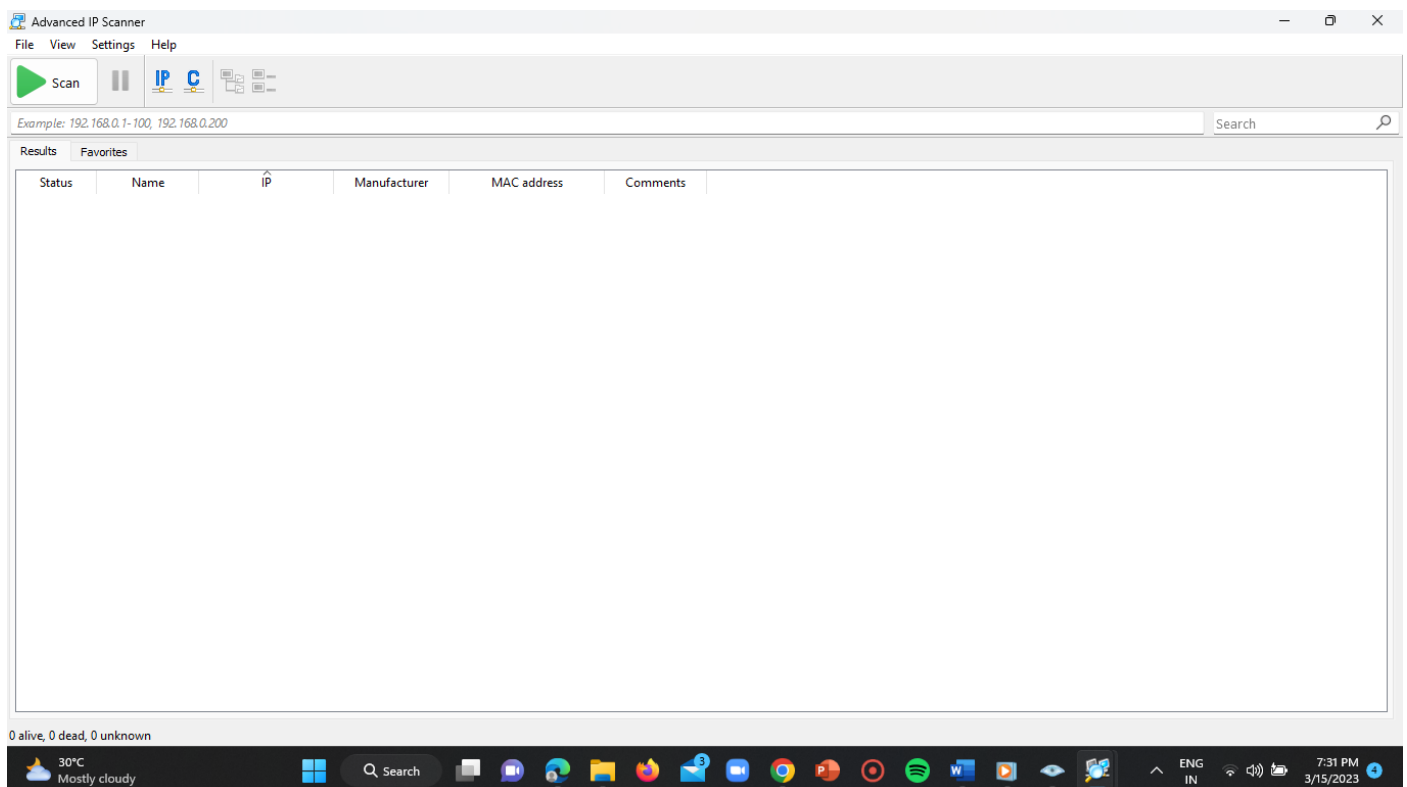
ST#IS#4899

In the search bar type “advanced IP scanner”.



STEP-3:

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



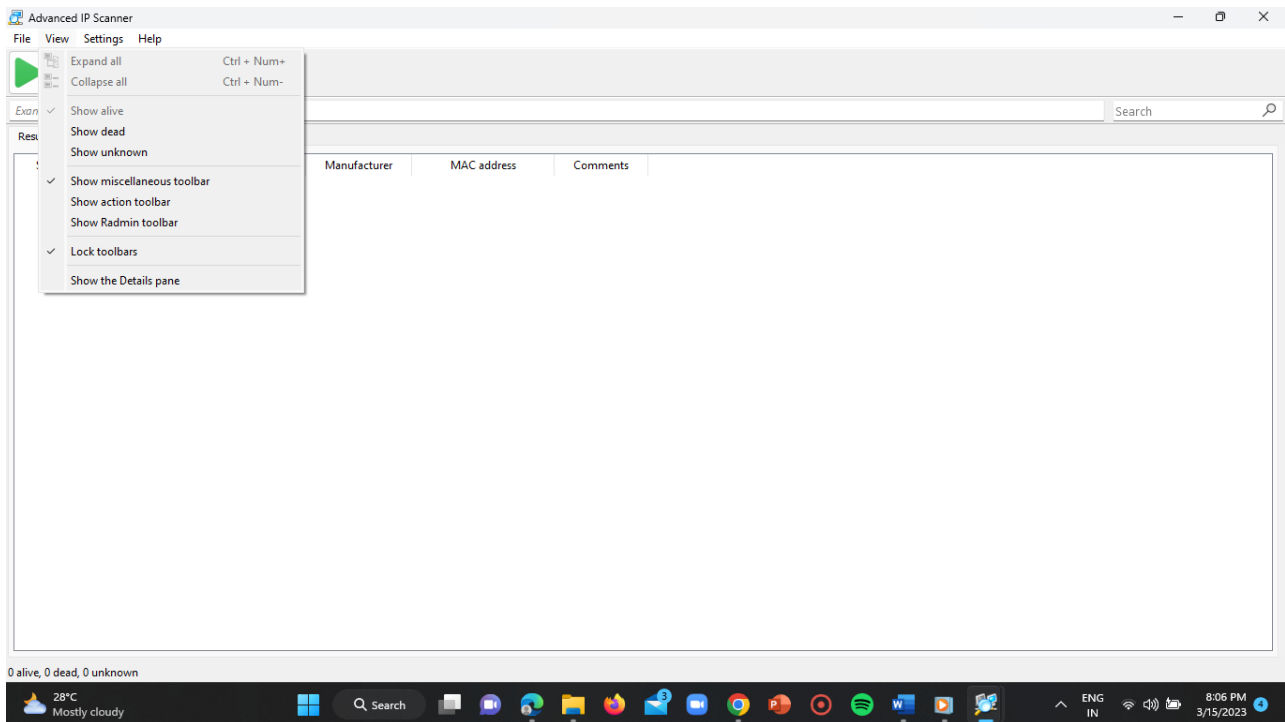
ST#IS#4899

STEP-4:

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

STEP-5:

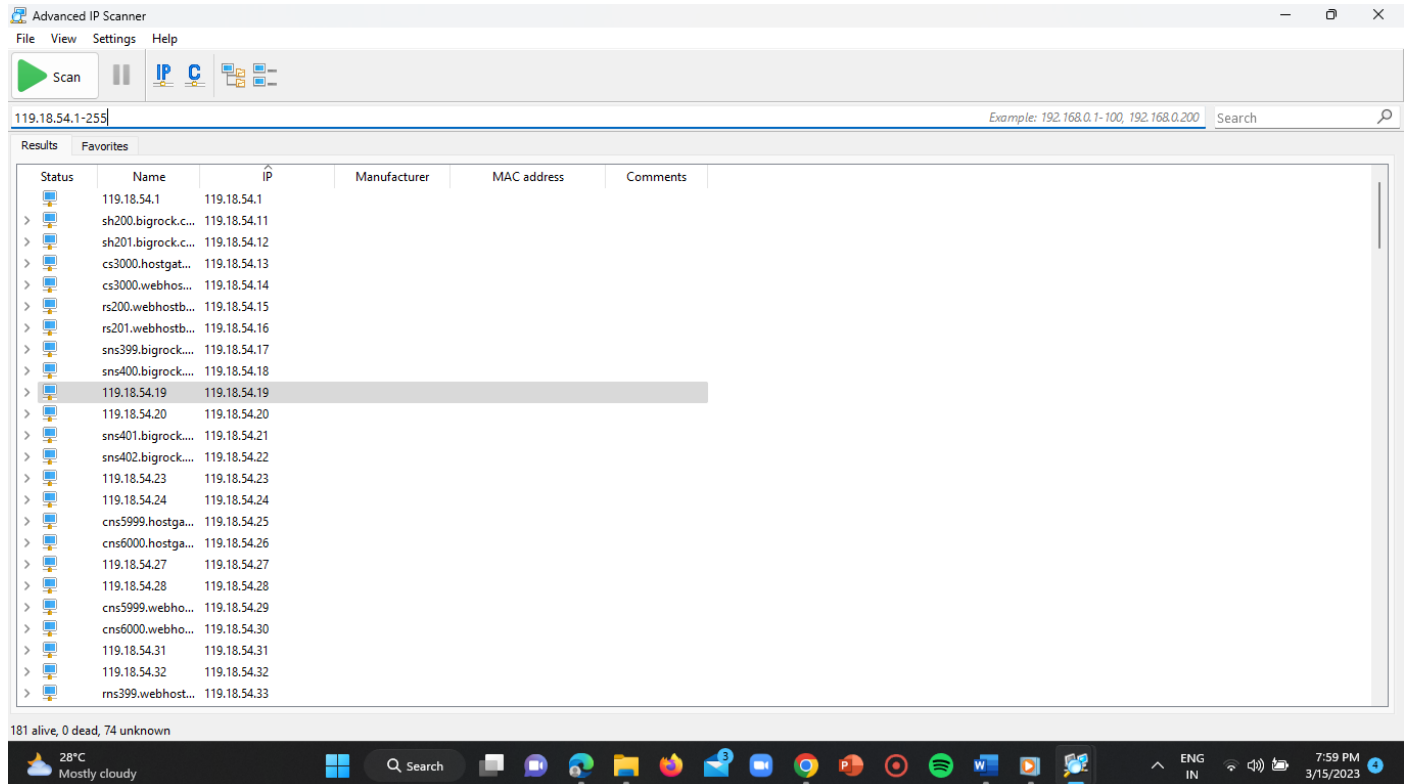
Make sure that in the view options only “show alive” option is enabled.



DOMAIN-1:

Range = 119.18.54.1-255

ST#IS#4899



Advanced IP Scanner

File View Settings Help

Scan

119.18.54.1-255

Example: 192.168.0.1-100, 192.168.0.200 Search

Status	Name	IP	Manufacturer	MAC address	Comments
>	119.18.54.1	119.18.54.1			
>	sh200.bigrock.c...	119.18.54.11			
>	sh201.bigrock.c...	119.18.54.12			
>	cs3000.hostgat...	119.18.54.13			
>	cs3000.webhos...	119.18.54.14			
>	rs200.webhostb...	119.18.54.15			
>	rs201.webhostb...	119.18.54.16			
>	sns399.bigrock...	119.18.54.17			
>	sns400.bigrock...	119.18.54.18			
>	119.18.54.19	119.18.54.19			
>	119.18.54.20	119.18.54.20			
>	sns401.bigrock...	119.18.54.21			
>	sns402.bigrock...	119.18.54.22			
>	119.18.54.23	119.18.54.23			
>	119.18.54.24	119.18.54.24			
>	cns5999.hostga...	119.18.54.25			
>	cns6000.hostga...	119.18.54.26			
>	119.18.54.27	119.18.54.27			
>	119.18.54.28	119.18.54.28			
>	cns5999.webho...	119.18.54.29			
>	cns6000.webho...	119.18.54.30			
>	119.18.54.31	119.18.54.31			
>	119.18.54.32	119.18.54.32			
>	rms399.webhost...	119.18.54.33			

181 alive, 0 dead, 74 unknown

28°C Mostly cloudy

Search

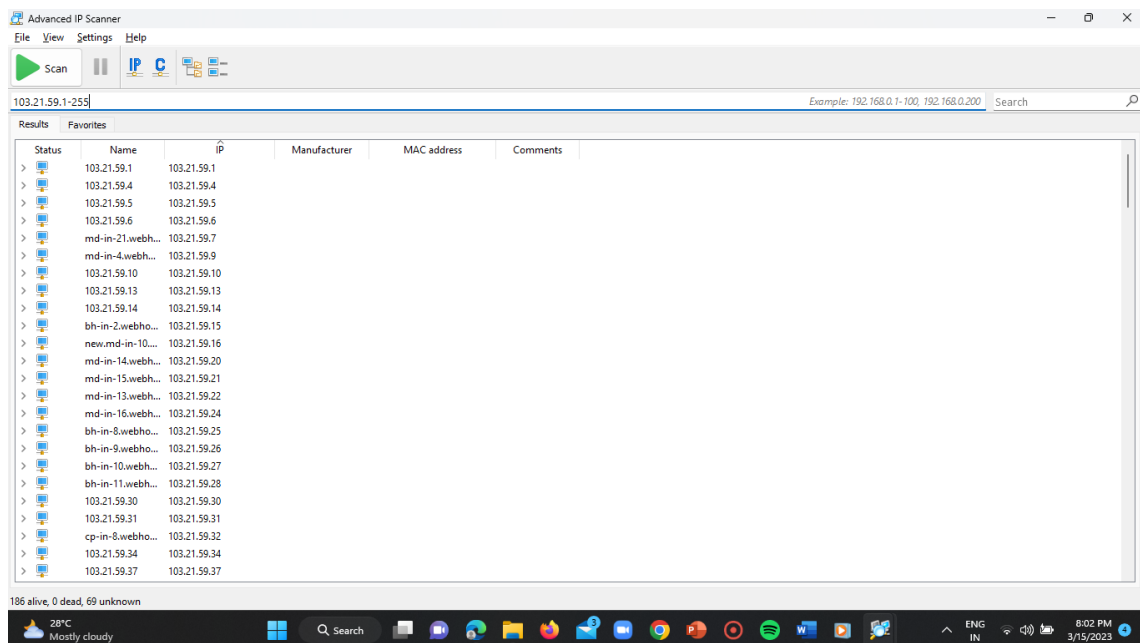
ENG IN

7:59 PM 3/15/2023

NUMBER OF LIVE PORTS = 181

DOMAIN-2:

Range = 103.21.59.1-255



Advanced IP Scanner

File View Settings Help

Scan

103.21.59.1-255

Example: 192.168.0.1-100, 192.168.0.200 Search

Status	Name	IP	Manufacturer	MAC address	Comments
>	103.21.59.1	103.21.59.1			
>	103.21.59.4	103.21.59.4			
>	103.21.59.5	103.21.59.5			
>	103.21.59.6	103.21.59.6			
>	md-in-21.webh...	103.21.59.7			
>	md-in-4.webh...	103.21.59.9			
>	103.21.59.10	103.21.59.10			
>	103.21.59.13	103.21.59.13			
>	103.21.59.14	103.21.59.14			
>	bh-in-2.webho...	103.21.59.15			
>	new.md-in-10...	103.21.59.16			
>	md-in-14.webh...	103.21.59.20			
>	md-in-15.webh...	103.21.59.21			
>	md-in-13.webh...	103.21.59.22			
>	md-in-16.webh...	103.21.59.24			
>	bh-in-8.webho...	103.21.59.25			
>	bh-in-9.webho...	103.21.59.26			
>	bh-in-10.webh...	103.21.59.27			
>	bh-in-11.webh...	103.21.59.28			
>	103.21.59.30	103.21.59.30			
>	103.21.59.31	103.21.59.31			
>	cp-in-8.webho...	103.21.59.32			
>	103.21.59.34	103.21.59.34			
>	103.21.59.37	103.21.59.37			

186 alive, 0 dead, 69 unknown

28°C Mostly cloudy

Search

ENG IN

8:02 PM 3/15/2023

NUMBER OF LIVE PORTS = 186

DOMAIN-3:

Range = 178.33.248.1-255

ST#IS#4899

Advanced IP Scanner

File View Settings Help

Stop

178.33.248.1-255

Results Favorites

Status	Name	IP	Manufacturer	MAC address	Comments
>	ip1.ip-178-33-248.eu	178.33.248.1			
>	ip2.ip-178-33-248.eu	178.33.248.2			
>	www.celibouest.com	178.33.248.3			
>	178-33-248-4.ovh.net	178.33.248.4			
>	service.5241.abc-corporate.pics	178.33.248.5			
>	ip7.ip-178-33-248.eu	178.33.248.7			
>	ip8.ip-178-33-248.eu	178.33.248.8			
>	2do.malivraisonbe.com	178.33.248.10			
>	12.mo587.mail-out.ovh.net	178.33.248.11			
>	19.mo551.mail-out.ovh.net	178.33.248.13			
>	178-33-248-16.ovh.net	178.33.248.16			
>	ip18.ip-178-33-248.eu	178.33.248.18			
>	178.33.248.19	178.33.248.19			
>	ip21.ip-178-33-248.eu	178.33.248.21			
>	ip24.ip-178-33-248.eu	178.33.248.24			
>	ip27.ip-178-33-248.eu	178.33.248.27			
>	178-33-248-28.ovh.net	178.33.248.28			
>	fme.webmapping.fr	178.33.248.30			
>	prod.clapeur.com	178.33.248.31			
>	178-33-248-35.ovh.net	178.33.248.35			
>	178-33-248-36.ovh.net	178.33.248.36			
>	www.energetiqueplantes.com	178.33.248.37			
>	ip39.ip-178-33-248.eu	178.33.248.39			
>	mail.mta29-bbtechnology.com	178.33.248.42			

109%, 123 alive, 0 dead, 132 unknown

28°C Mostly cloudy

ENG IN 8:08 PM 3/15/2023

NUMBER OF LIVE PORTS = 123

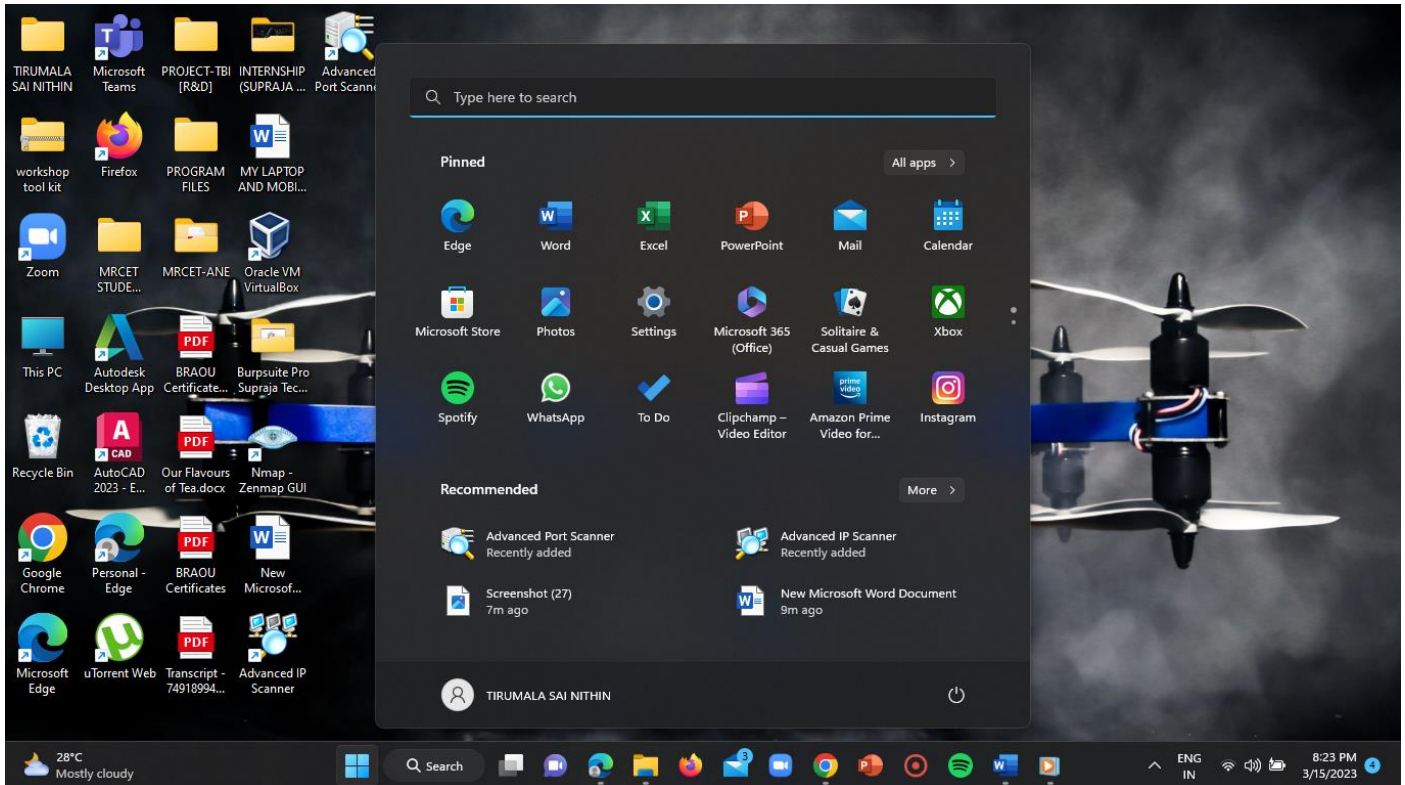
ANSWER-2:

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

STEP-1:

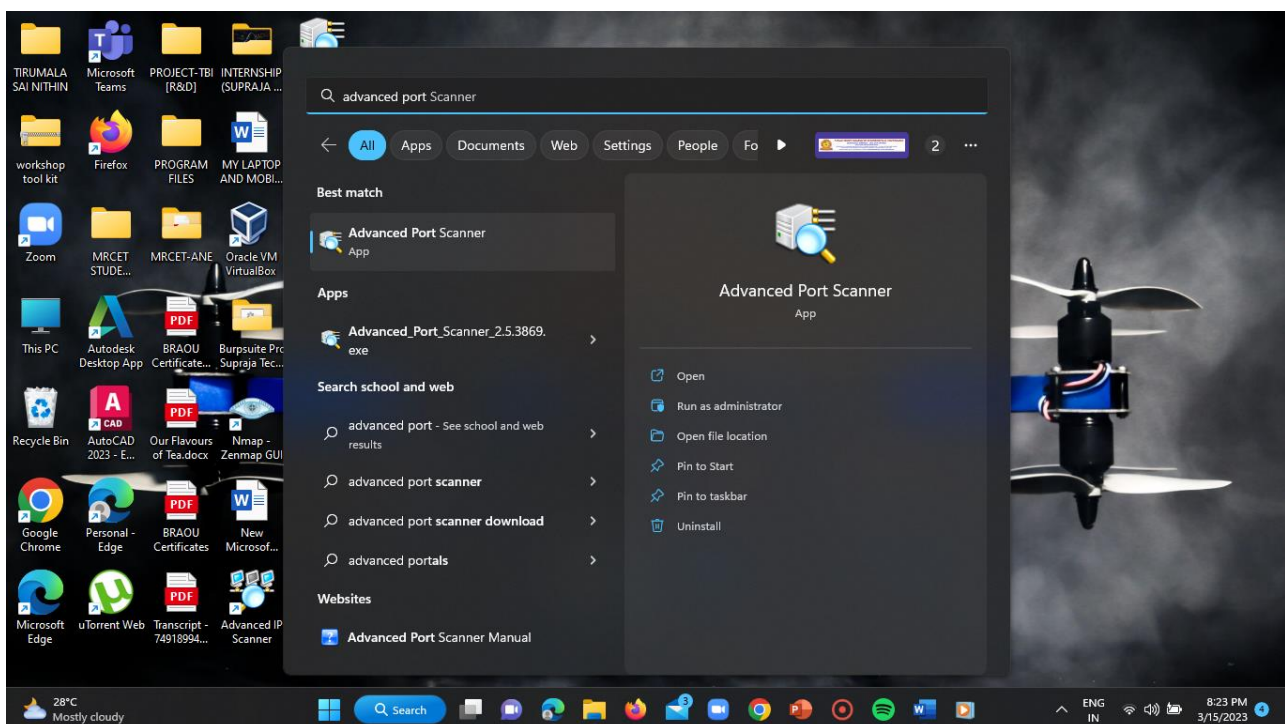
Click on start.

ST#IS#4899



STEP-2:

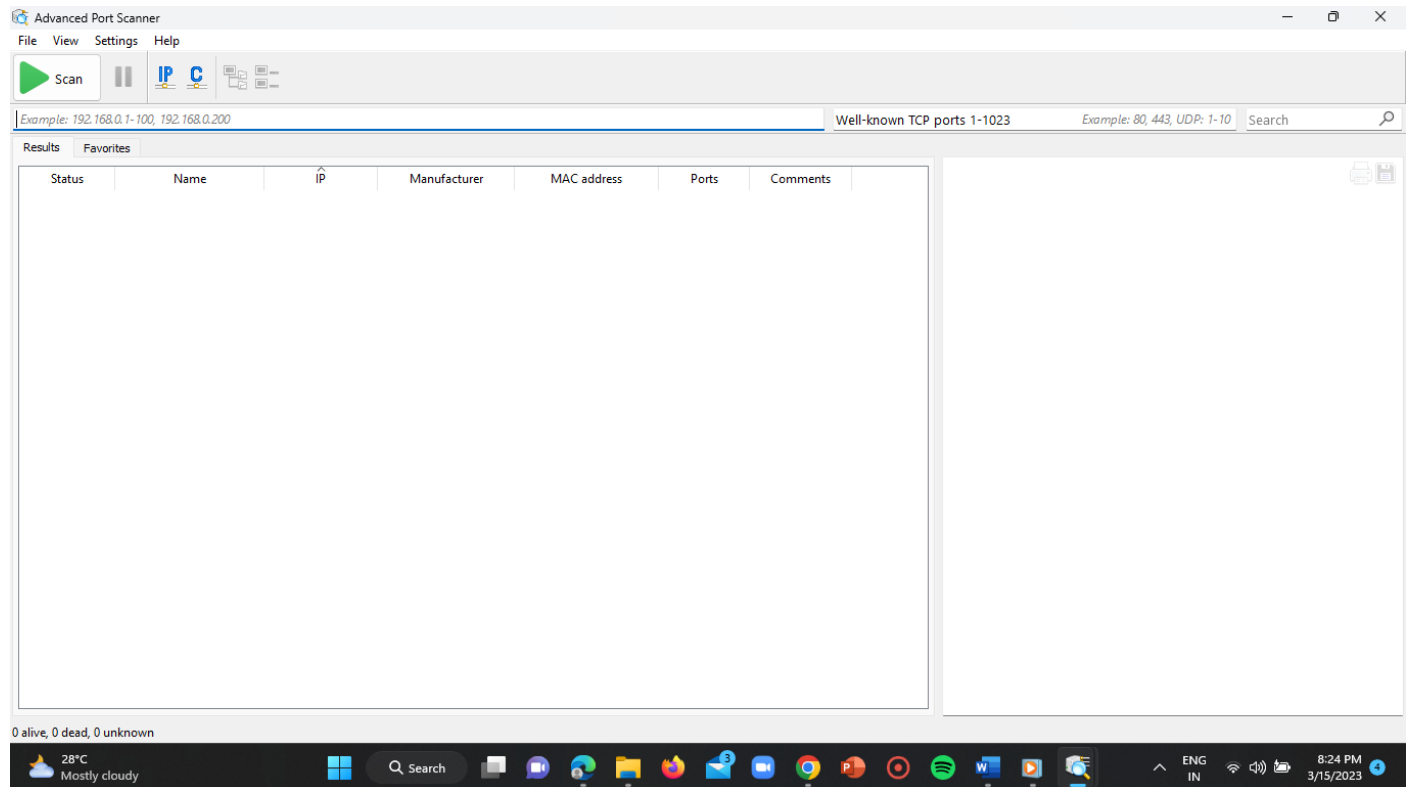
Type “advanced port scanner” in the search bar.



STEP-3:

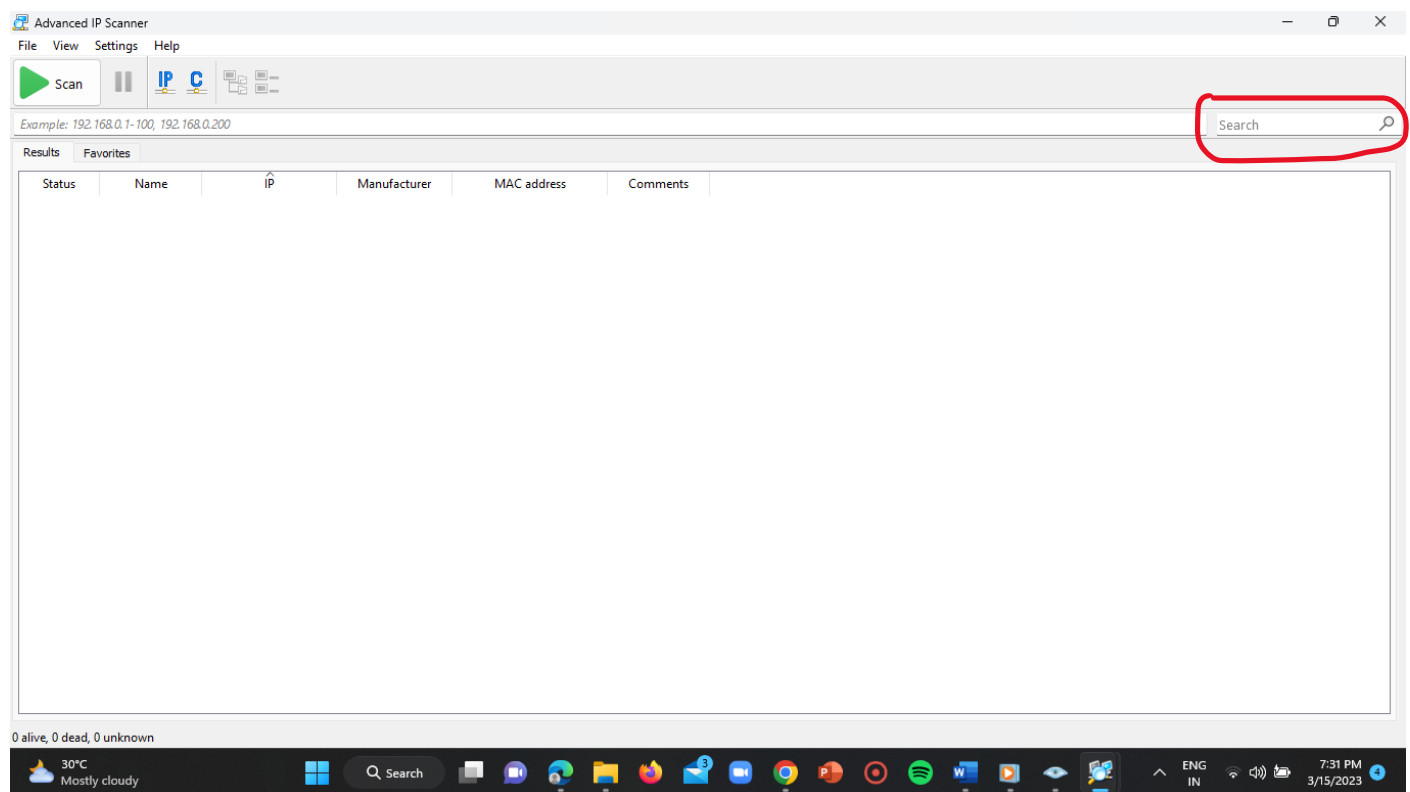
Open it in the ‘ADMINISTRATOR MODE’ by clicking on “run as administrator” and scan the target IP addresses.

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:

Advanced Port Scanner

File View Settings Help

Scan

119.18.54.1-255 Example: 192.168.0.1-100, 192.168.0.200 Example: 80, 443, UDP: 1-10 22, 80, 3306

Status	Name	IP	Manufacturer	MAC address	Ports	Comments
>	sh200.bigrock.com	119.18.54.11			22, 80, 3306	
>	sh201.bigrock.com	119.18.54.12			22, 80, 3306	
>	cs3000.hostgator.in	119.18.54.13			22, 80, 3306	
>	cs3000.webhostbox.net	119.18.54.14			22, 80, 3306	
>	rs200.webhostbox.net	119.18.54.15			22, 80, 3306	
>	rs201.webhostbox.net	119.18.54.16			22, 80, 3306	
>	sns399.bigrock.com	119.18.54.17			22, 80, 3306	
>	sns400.bigrock.com	119.18.54.18			22, 80, 3306	
>	119.18.54.19	119.18.54.19			22, 80, 3306	
>	119.18.54.20	119.18.54.20			22, 80, 3306	
>	sns401.bigrock.com	119.18.54.21			22, 80, 3306	
>	sns402.bigrock.com	119.18.54.22			22, 80, 3306	
>	119.18.54.23	119.18.54.23			22, 80, 3306	
>	119.18.54.24	119.18.54.24			22, 80, 3306	
>	cns5999.hostgator.in	119.18.54.25			22, 80, 3306	
>	cns6000.hostgator.in	119.18.54.26			22, 80, 3306	
>	119.18.54.27	119.18.54.27			22, 80, 3306	
>	119.18.54.28	119.18.54.28			22, 80, 3306	
>	cns5999.webhostbox.net	119.18.54.29			22, 80, 3306	
>	cns6000.webhostbox.net	119.18.54.30			22, 80, 3306	
>	119.18.54.31	119.18.54.31			22, 80, 3306	
>	119.18.54.32	119.18.54.32			22, 80, 3306	
>	rms399.webhostbox.net	119.18.54.33			22, 80, 3306	
>	rms400.webhostbox.net	119.18.54.34			22, 80, 3306	

179 alive, 0 dead, 0 unknown

RTC Cross Road Construction

sh200.bigrock.com

Status: Alive

Operating system: 119.18.54.11

IP: 119.18.54.11

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

NUMBER OF PORTS = 179

DOMAIN-2:

Advanced Port Scanner

File View Settings Help

Scan

103.21.59.1-255 Example: 192.168.0.1-100, 192.168.0.200 Example: 80, 443, UDP: 1-10 22, 80, 3306

Status	Name	IP	Manufacturer	MAC address	Ports	Comments
>	103.21.59.1	103.21.59.1			22, 80, 3306	
>	103.21.59.4	103.21.59.4			22, 80, 3306	
>	103.21.59.6	103.21.59.6			22, 80, 3306	
>	md-in-21.webh...	103.21.59.7			22, 80, 3306	
>	md-in-4.webh...	103.21.59.9			22, 80, 3306	
>	103.21.59.13	103.21.59.13			22, 80, 3306	
>	103.21.59.14	103.21.59.14			22, 80, 3306	
>	bh-in-2.webho...	103.21.59.15			22, 80, 3306	
>	new.md-in-10...	103.21.59.16			22, 80, 3306	
>	md-in-14.webh...	103.21.59.20			22, 80, 3306	
>	md-in-15.webh...	103.21.59.21			22, 80, 3306	
>	md-in-13.webh...	103.21.59.22			22, 80, 3306	
>	md-in-16.webh...	103.21.59.24			22, 80, 3306	
>	bh-in-8.webho...	103.21.59.25			22, 80, 3306	
>	bh-in-9.webho...	103.21.59.26			22, 80, 3306	
>	bh-in-10.webh...	103.21.59.27			22, 80, 3306	
>	bh-in-11.webh...	103.21.59.28			22, 80, 3306	
>	103.21.59.30	103.21.59.30			22, 80, 3306	
>	103.21.59.31	103.21.59.31			22, 80, 3306	
>	cp-in-8.webho...	103.21.59.32			22, 80, 3306	
>	103.21.59.34	103.21.59.34			22, 80, 3306	
>	103.21.59.41	103.21.59.41			22, 80, 3306	
>	103.21.59.43	103.21.59.43			22, 80, 3306	
>	103.21.59.44	103.21.59.44			22, 80, 3306	

169 alive, 0 dead, 0 unknown

RTC Cross Road Construction

103.21.59.1

Status: Alive

Operating system: 103.21.59.1

IP: 103.21.59.1

MAC:

Manufacturer:

NetBIOS:

User:

Type:

Date:

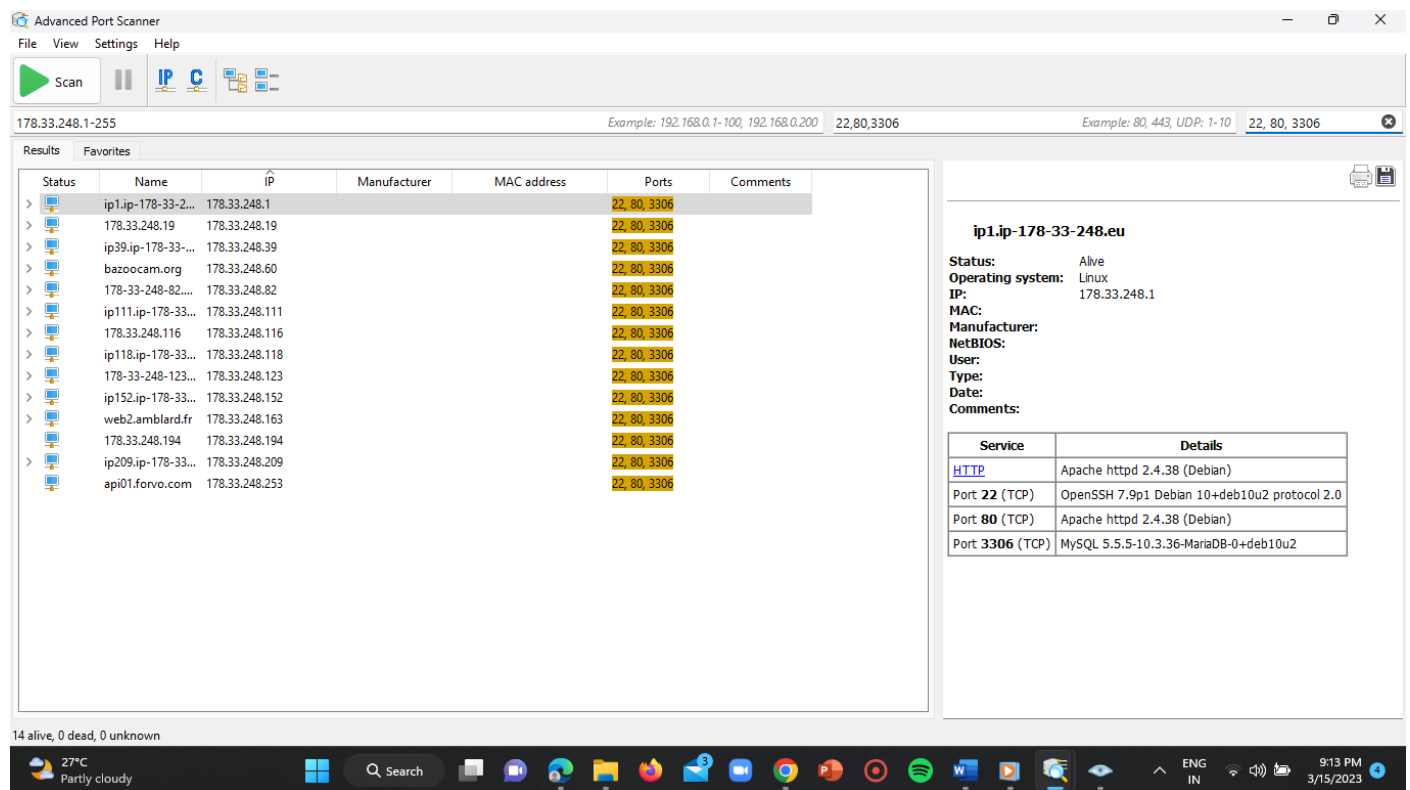
Comments:

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

ST#IS#4899

NUMBER OF PORTS = 169

DOMAIN-3:



Advanced Port Scanner

File View Settings Help

Scan

178.33.248.1-255 Example: 192.168.0.1-100, 192.168.0.200 22,80,3306 Example: 80, 443, UDP: 1-10 22, 80, 3306

Status	Name	IP	Manufacturer	MAC address	Ports	Comments
>	ip1.ip-178-33-2...	178.33.248.1			22, 80, 3306	
>	178.33.248.19	178.33.248.19			22, 80, 3306	
>	ip39.ip-178-33-...	178.33.248.39			22, 80, 3306	
>	bazoccam.org	178.33.248.60			22, 80, 3306	
>	178-33-248-82...	178.33.248.82			22, 80, 3306	
>	ip111.ip-178-33...	178.33.248.111			22, 80, 3306	
>	178.33.248.116	178.33.248.116			22, 80, 3306	
>	ip118.ip-178-33...	178.33.248.118			22, 80, 3306	
>	178-33-248-123...	178.33.248.123			22, 80, 3306	
>	ip152.ip-178-33...	178.33.248.152			22, 80, 3306	
>	web2.amblard.fr	178.33.248.163			22, 80, 3306	
>	178.33.248.194	178.33.248.194			22, 80, 3306	
>	ip209.ip-178-33...	178.33.248.209			22, 80, 3306	
>	api01.forvo.com	178.33.248.253			22, 80, 3306	

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

14 alive, 0 dead, 0 unknown

27°C Partly cloudy

9:13 PM 3/15/2023

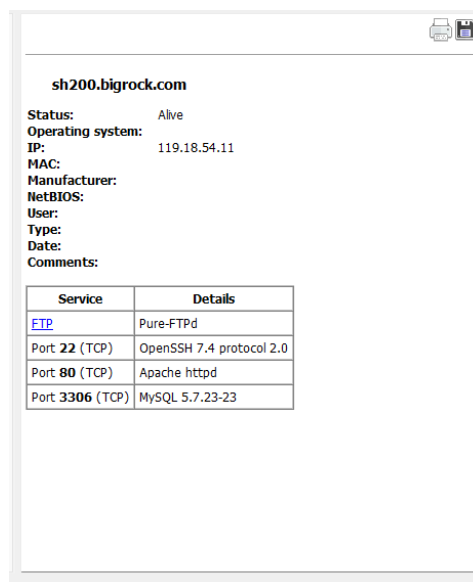
NUMBER OF PORTS = 14

ANSWER-3:

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

WITHOUT VPN:

DOMAIN-1:



sh200.bigrock.com

Status: Alive
Operating system: Linux
IP: 119.18.54.11
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

ST#IS#4899

DOMAIN-2:

103.21.59.1

Status: Alive

Operating system: 103.21.59.1

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

WITH VPN:

DOMAIN-1:

119.18.54.1

Status: Alive

Operating system: 119.18.54.1

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: 119.18.54.12

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: 119.18.54.15

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: 119.18.54.146

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:	ip2.ip-178-33-248.eu Status: Alive Operating system: Linux IP: 178.33.248.2 MAC: Manufacturer: NetBIOS: User: Type: Date: Comments:	www.cellbouest.com Status: Alive Operating system: Linux IP: 178.33.248.3 MAC: Manufacturer: NetBIOS: User: Type: Date: Comments:	178.33.248.16 Status: Alive Operating system: Linux IP: 178.33.248.16 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)	

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

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

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

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

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)	

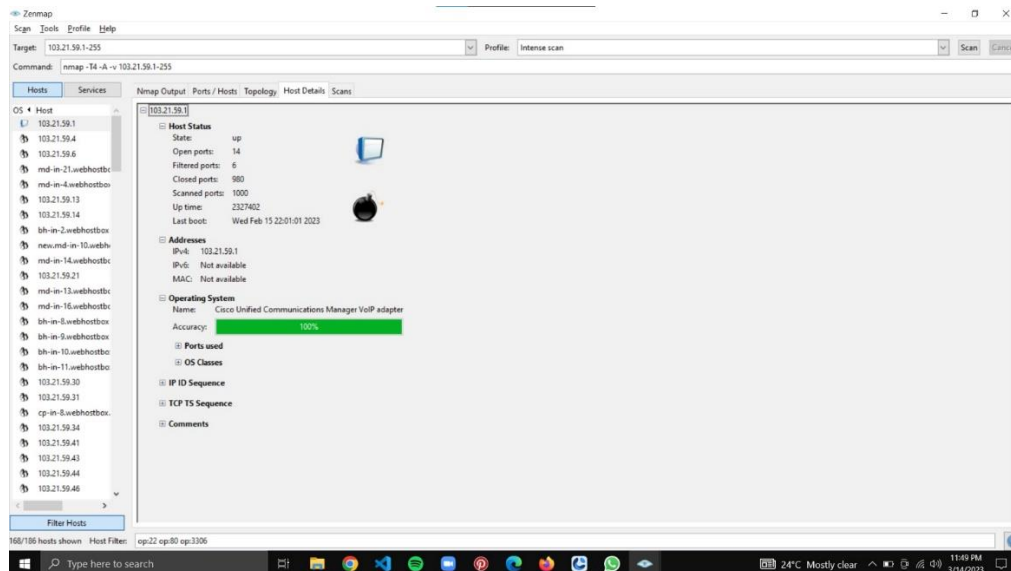
➔ Gathering the banner and operating system details of the filtered IP addresses of the target domains.

DOMAIN-1:

Zenmap interface showing a scan of 119.18.54.1-255. The scan command is nmap -T4 -A -v 119.18.54.1-255. The target is 119.18.54.1-255. The scan profile is Intense scan. The scan results show 13 open ports, 7 filtered ports, and 980 closed ports. The operating system is identified as Linux 3.4 with 99% accuracy. The ports used are 22, 80, and 3306.

DOMAIN-2:

ST#IS#4899

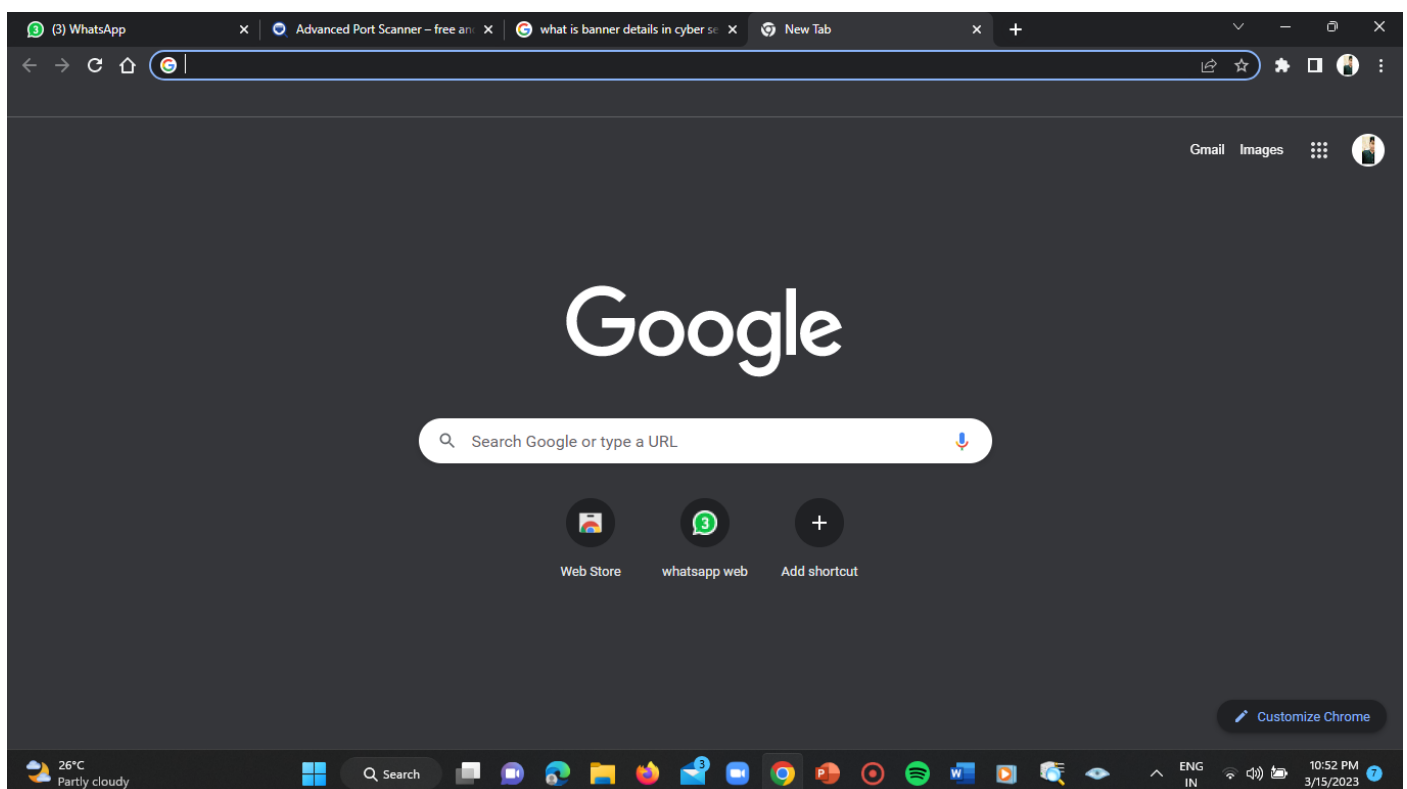


DOMAIN-3:

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.

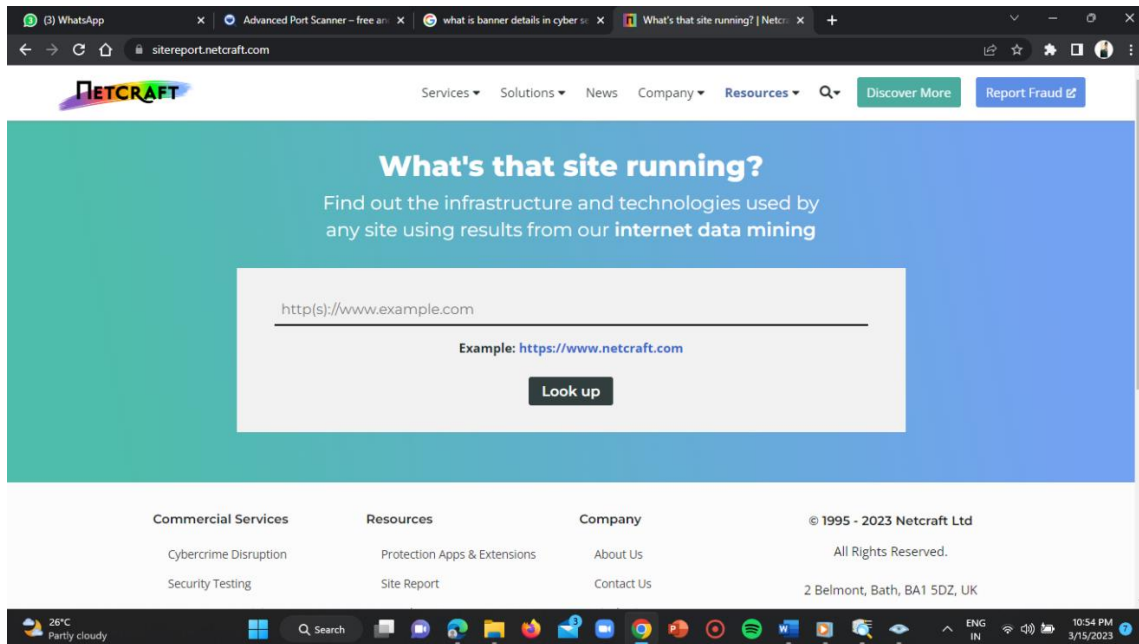


STEP-2:

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