# TARGET: -

TASK – 3

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**

1. **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.**

1. **Gather the following details from the filtered IP addresses:**
   1. **Services**
   2. **Versions**
   3. **Banner Details**
   4. **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**

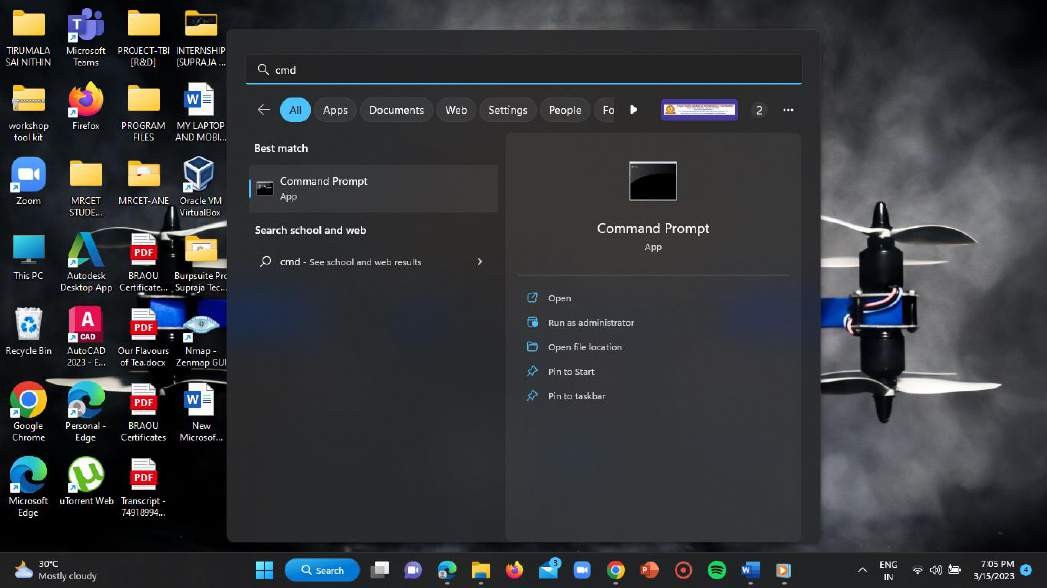
## STEP-2:

Now click on start.



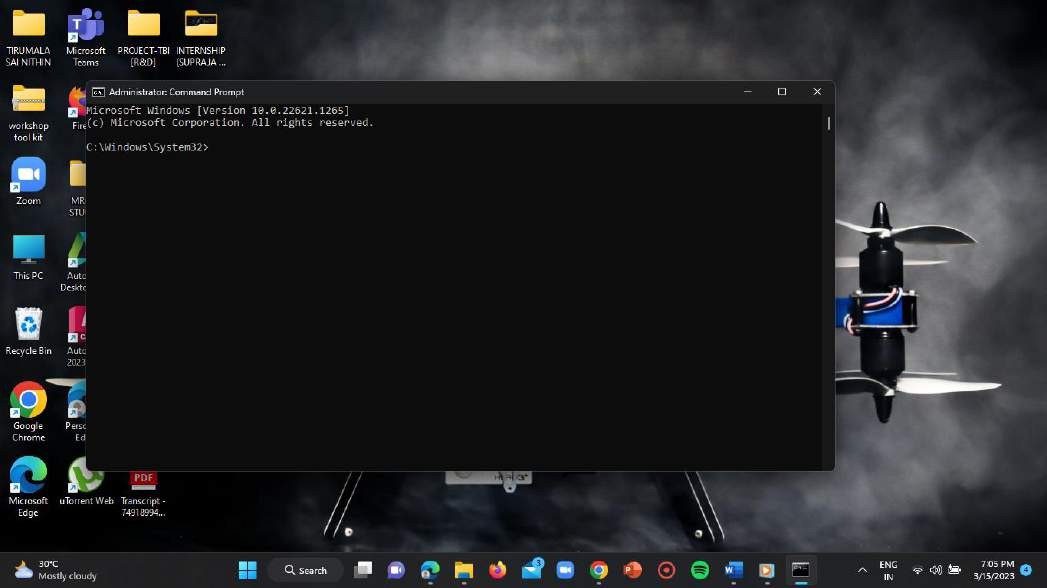
## STEP-3:

In the search bar enter “cmd”.



## STEP-4:

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



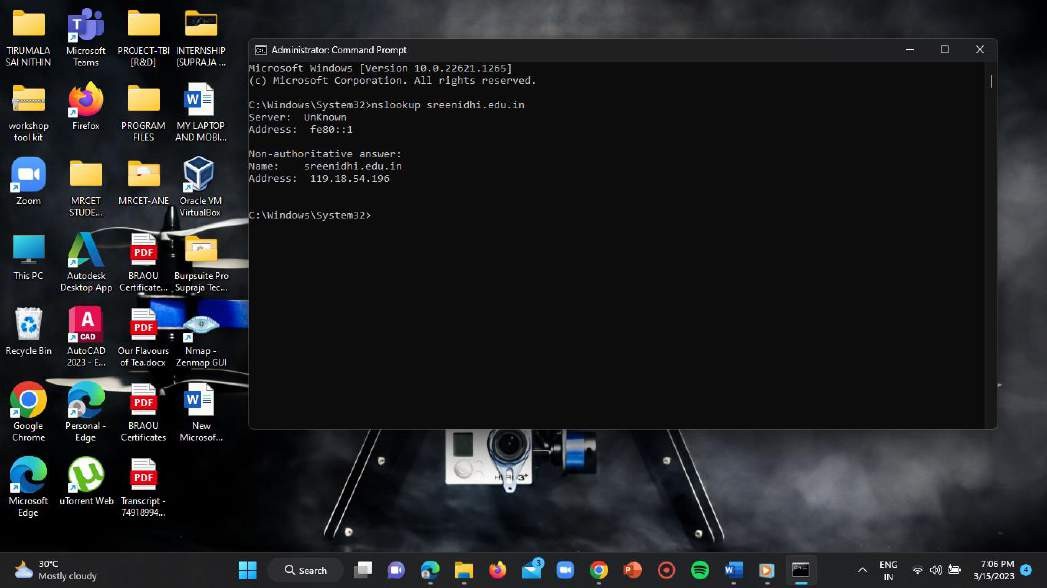
## STEP-5:

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

enter.

**For DOMAIN-1:**

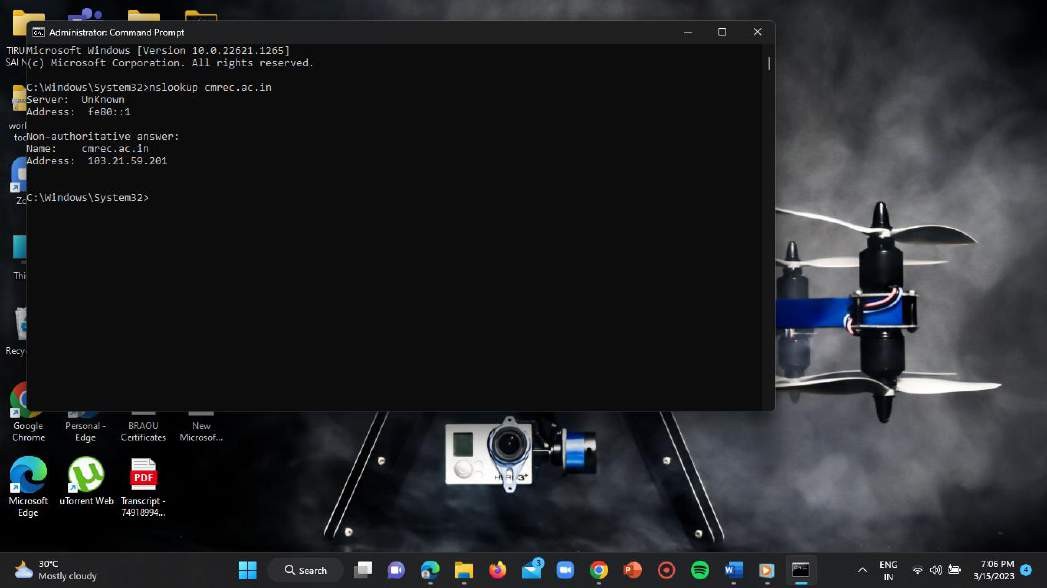
Type= nslookup sreenidhi.edu.in



**IP ADDRESS = 119.18.54.196**

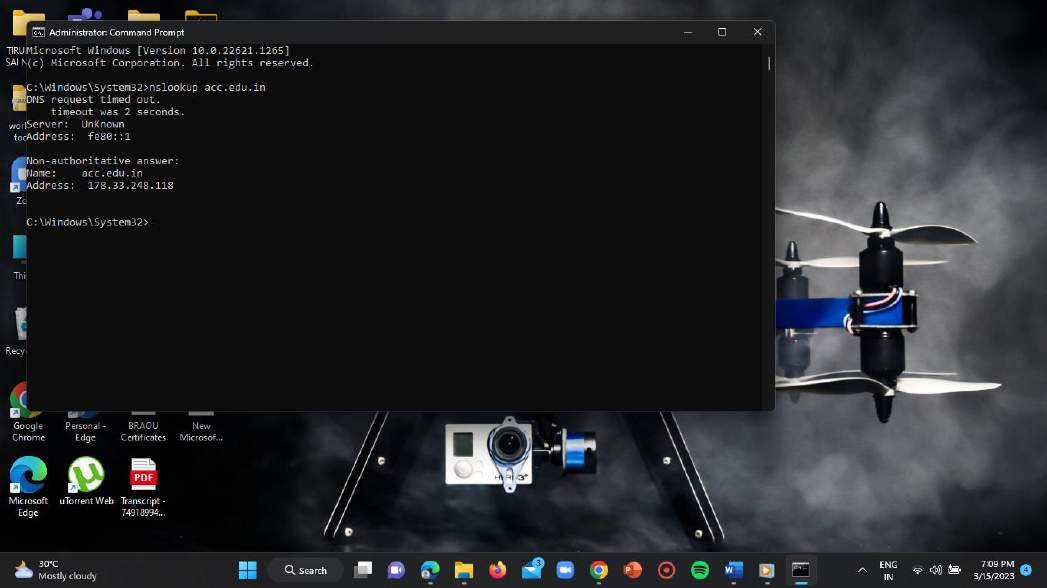
**For DOMAIN-2:**

Type= nslookup cmrec.ac.in



**IP ADDRESS = 103.21.59.201 For DOMAIN-3:**

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.



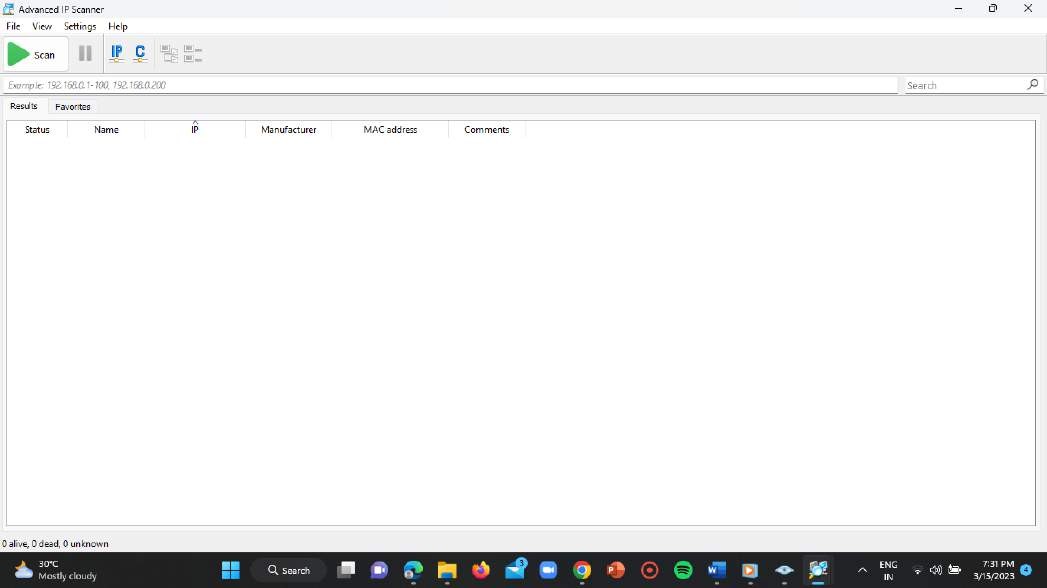
## STEP-2:

In the search bar type “advanced IP scanner”.



## STEP-3:

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

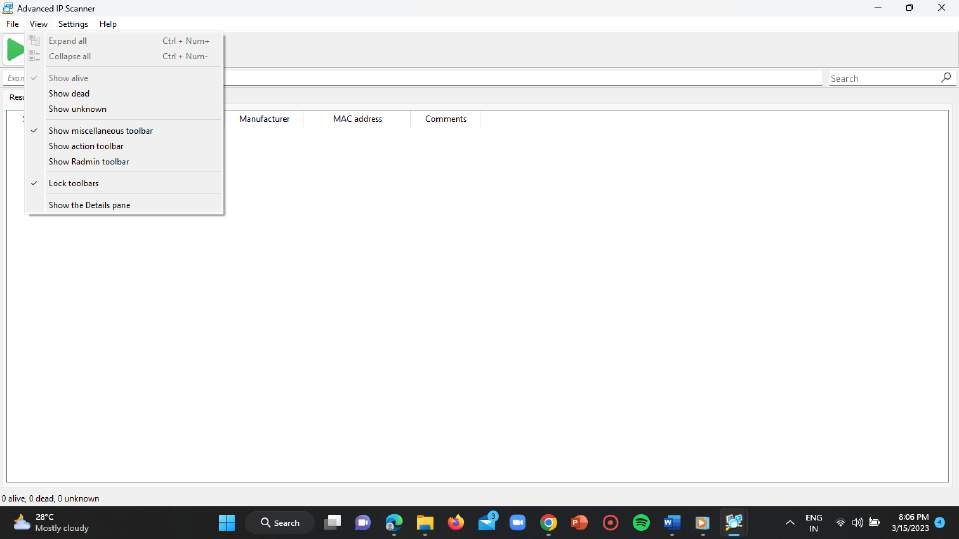


## STEP-4:

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

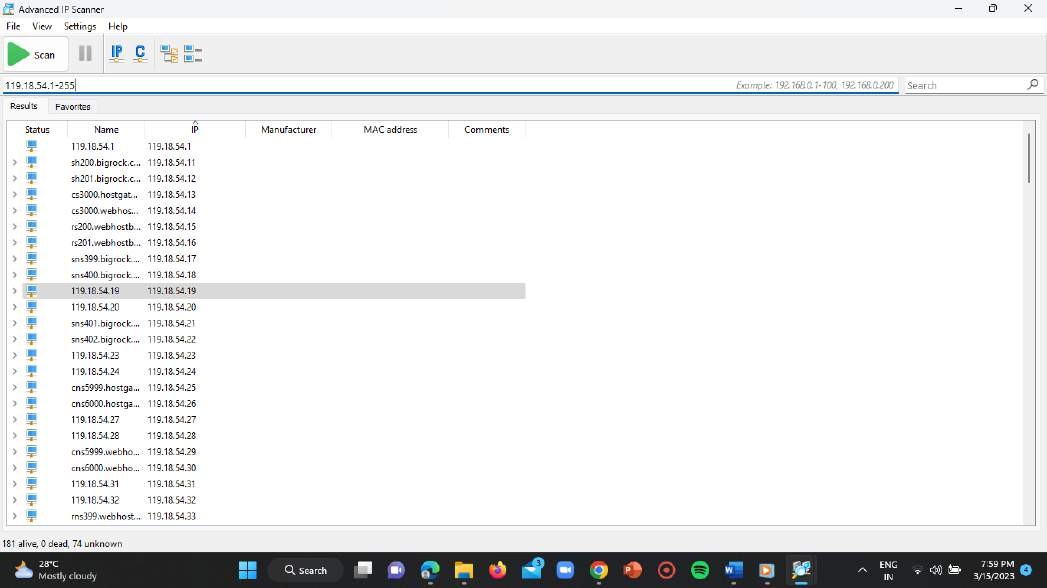
## STEP-5:

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



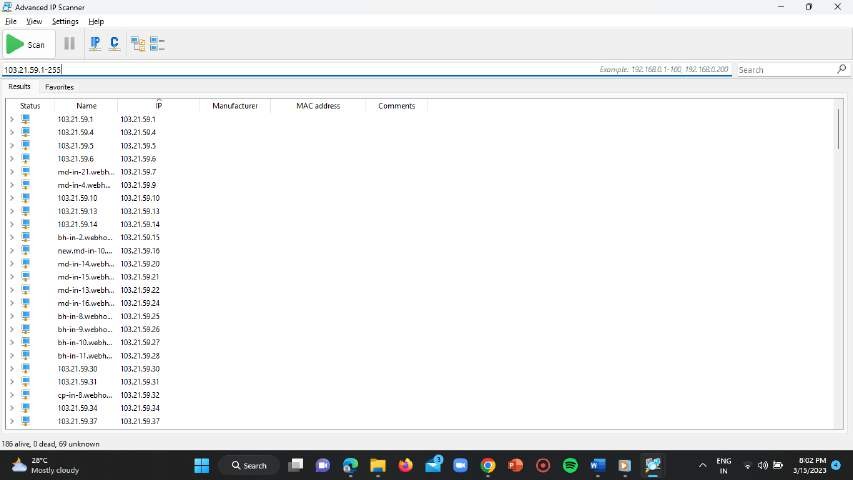
**DOMAIN-1:**

Range = 119.18.54.1-255



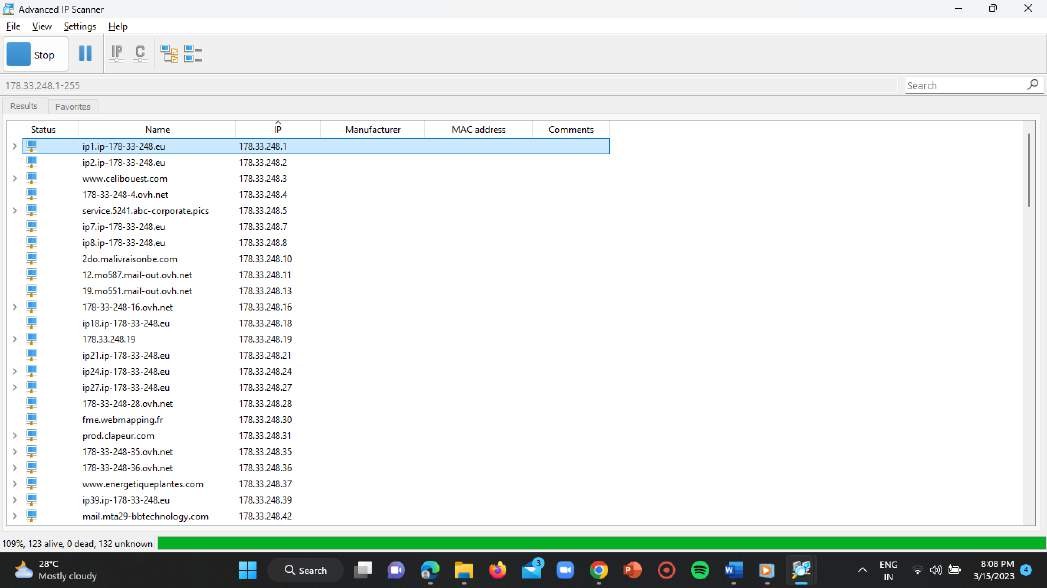
**NUMBER OF LIVE PORTS = 181 DOMAIN-2:**

Range = 103.21.59.1-255



**NUMBER OF LIVE PORTS = 186 DOMAIN-3:**

Range = 178.33.248.1-255

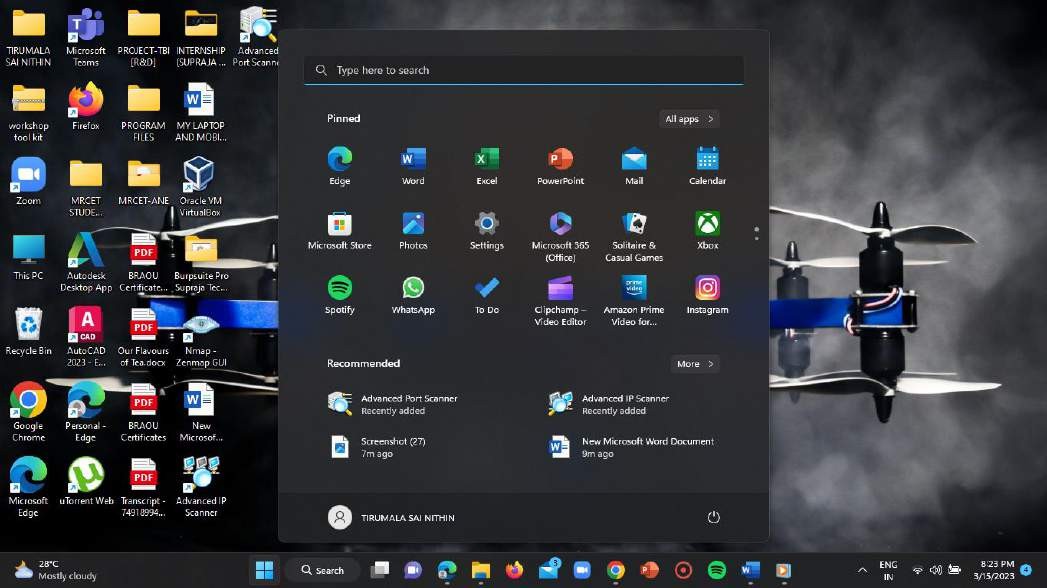


**NUMBER OF LIVE PORTS = 123 ANSWER-2:**

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

## STEP-1:

Click on start.



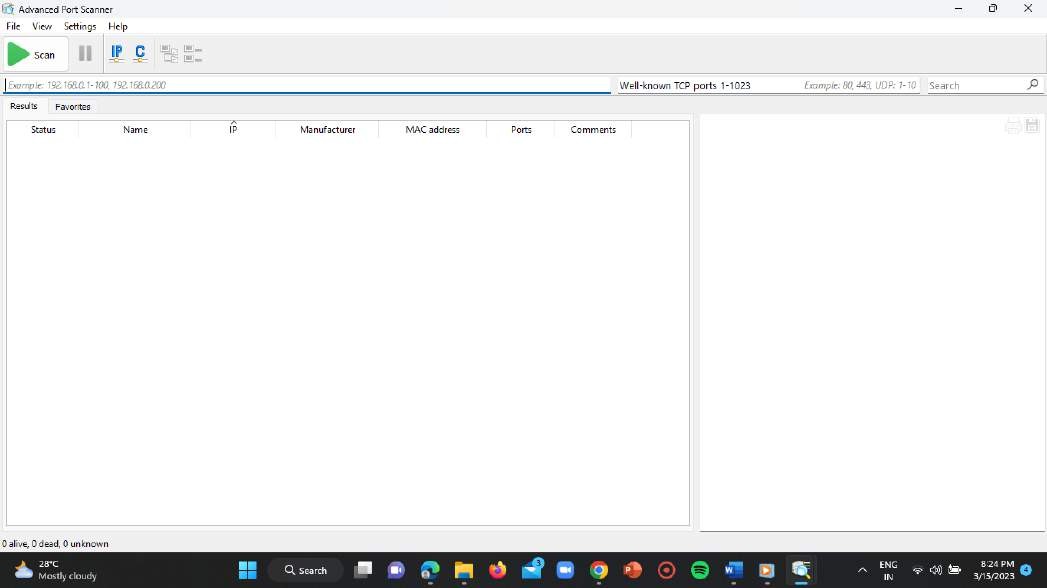
## STEP-2:

Type “advanced port scanner” in the search bar.



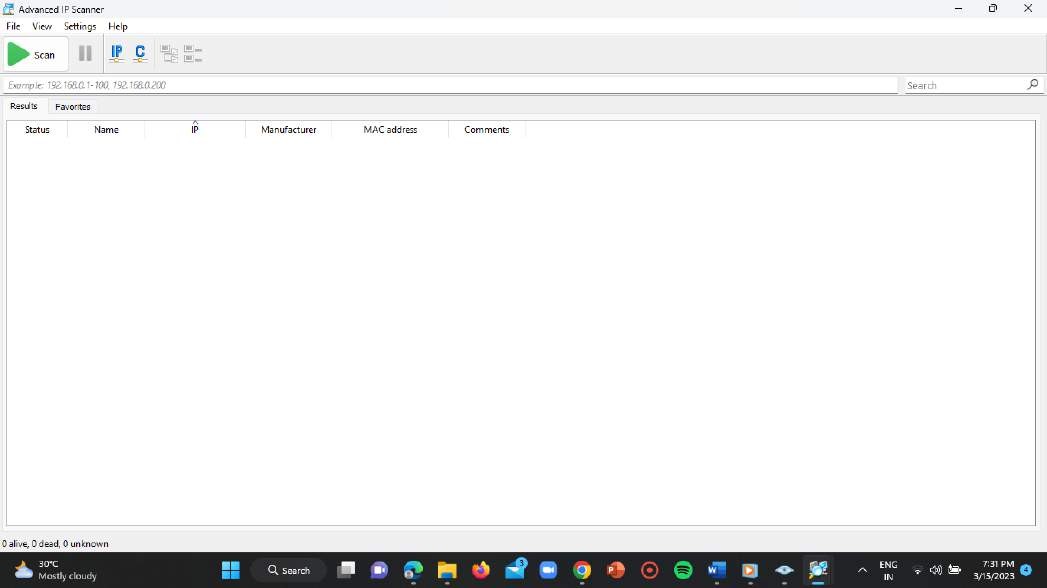
## STEP-3:

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



## STEP-4:

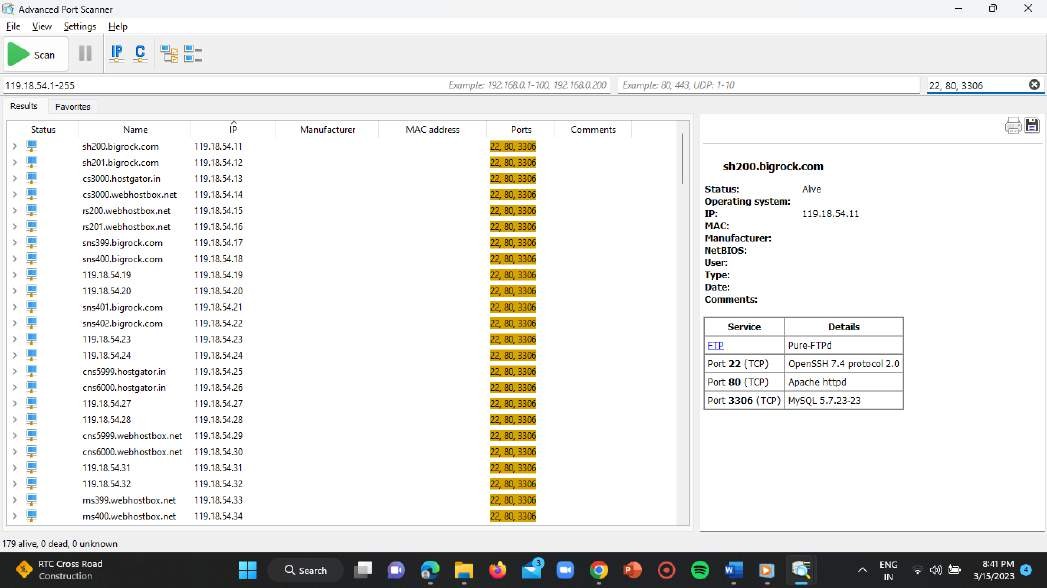
Click on the search bar on the right corner of the advanced IP scanner.



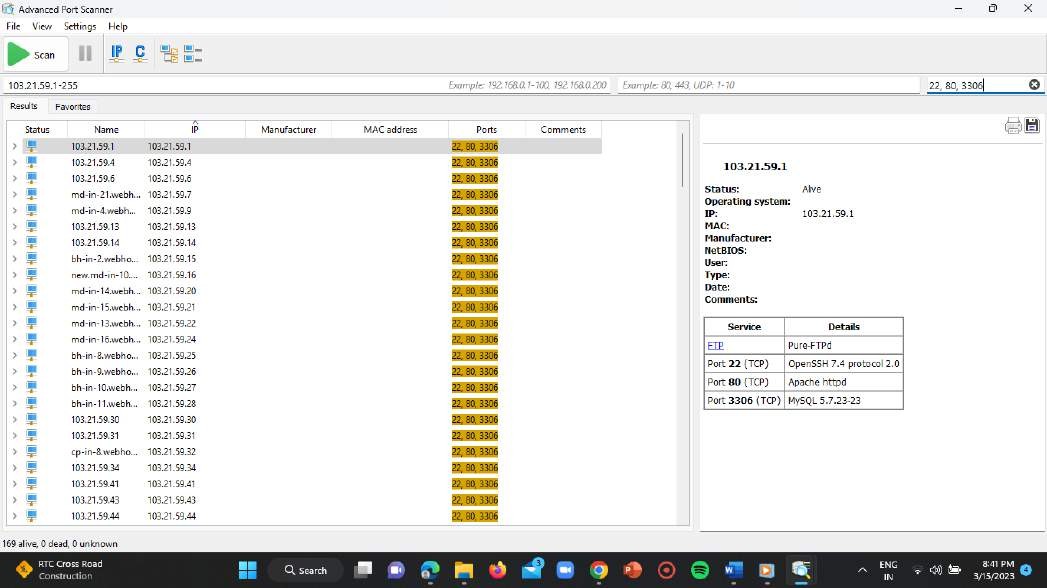
## STEP-5:

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

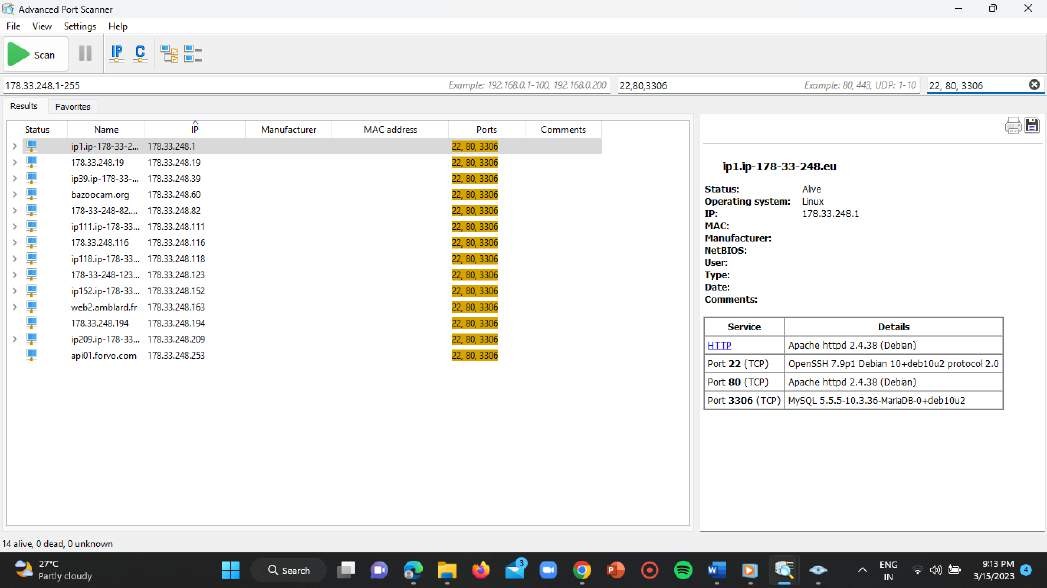
**DOMAIN-1:**



**NUMBER OF PORTS = 179 DOMAIN-2:**



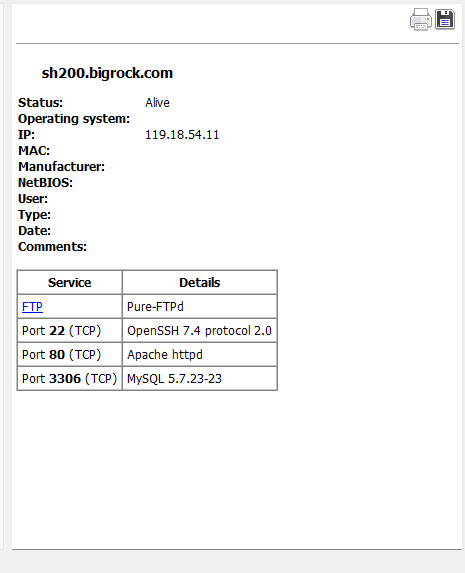
**NUMBER OF PORTS = 169 DOMAIN-3:**

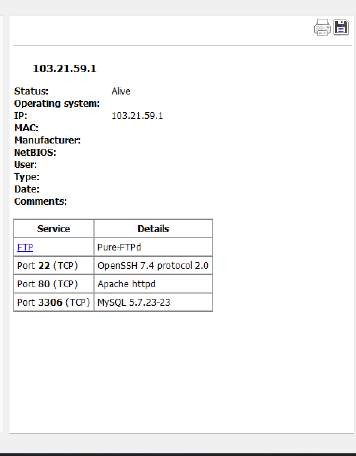


**NUMBER OF PORTS = 14 ANSWER-3:**

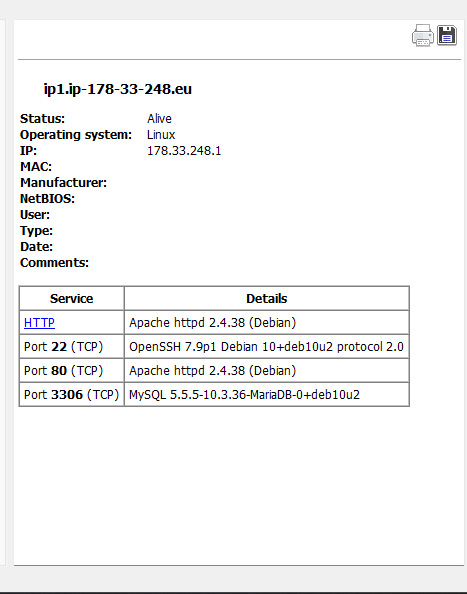
Gathering the services and version details from the filtered ports with and without usage of the VPN.

**WITHOUT VPN: DOMAIN-1:**

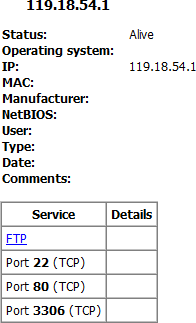


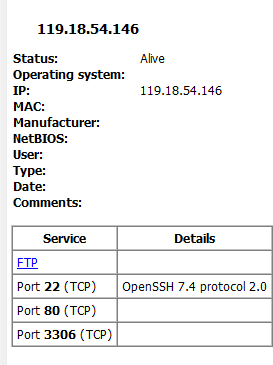
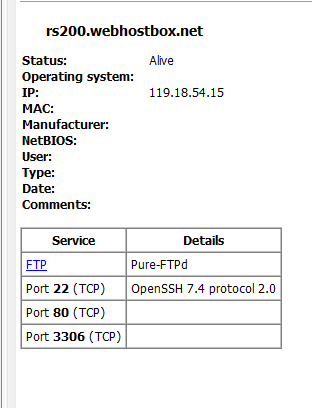
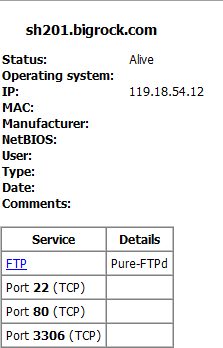


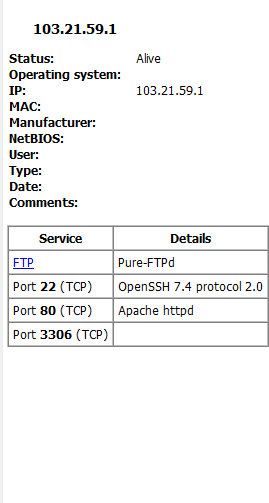
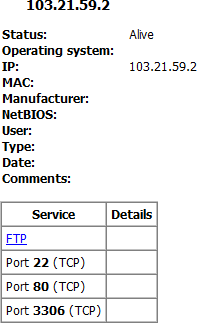
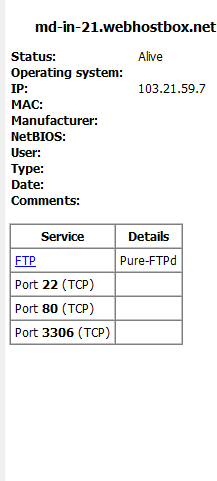
**DOMAIN-3:**

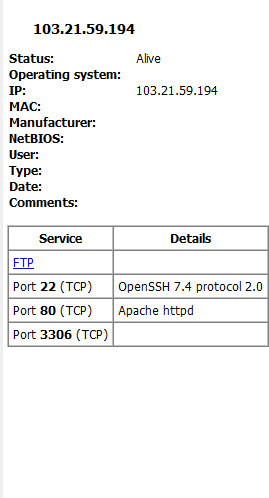
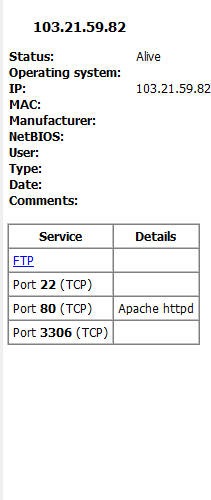
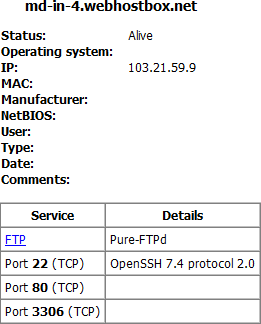


**WITH VPN: DOMAIN-1:**

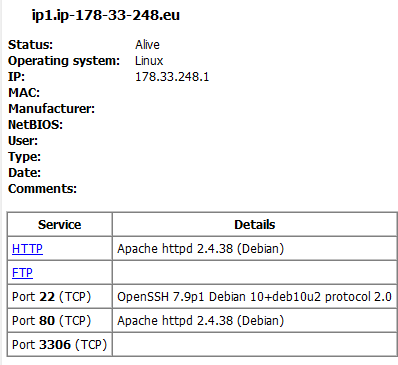


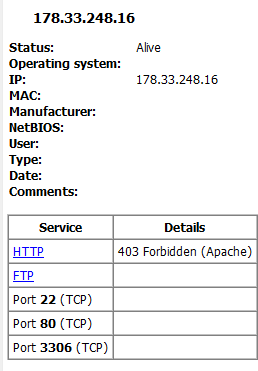
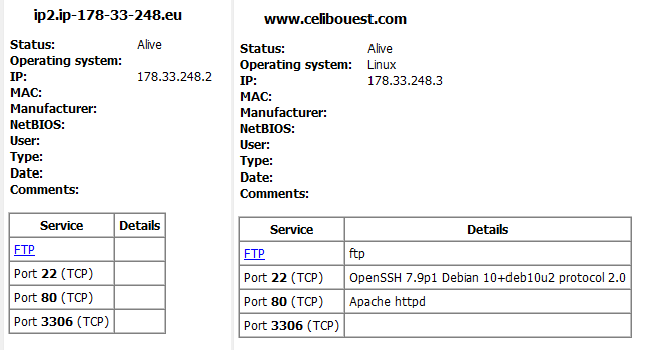


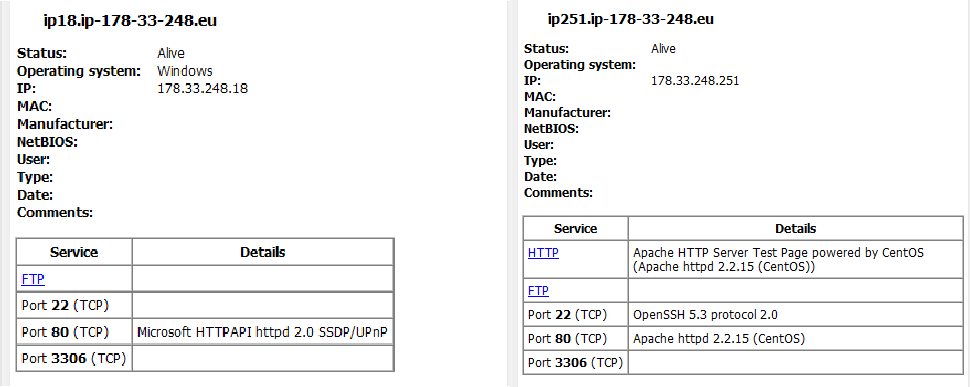
  



**DOMAIN-3:**

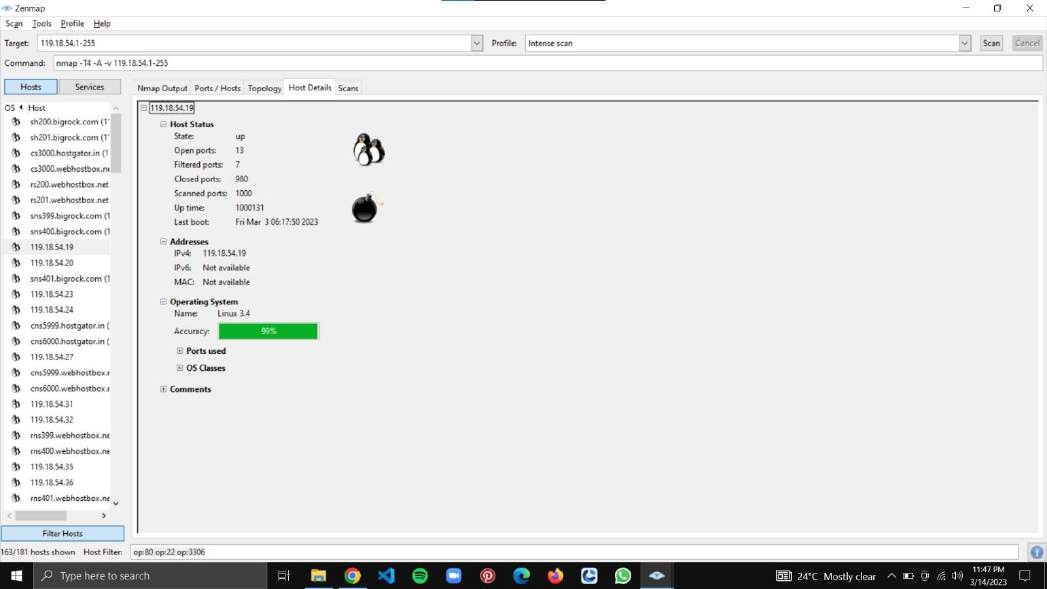




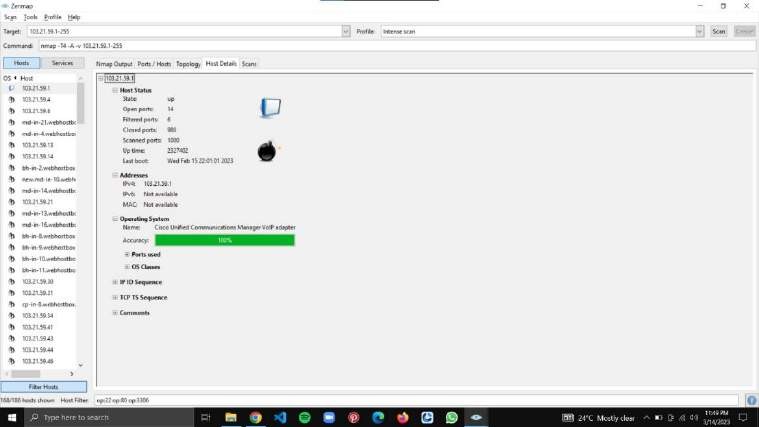


Gathering the banner and operating system details of the filtered IP addresses of the target domains.

**DOMAIN-1:**



**DOMAIN-2:**

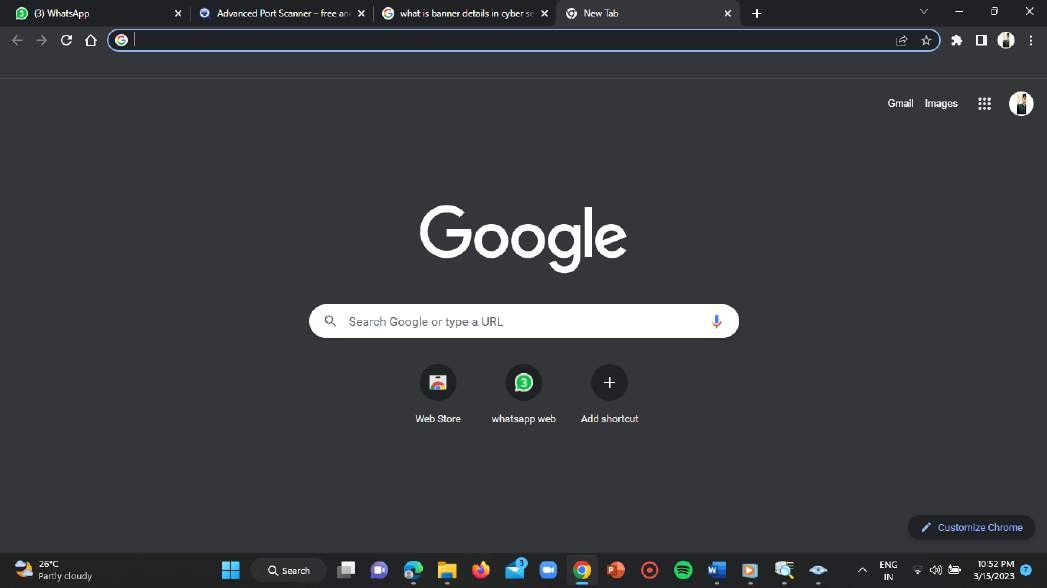


**DOMAIN-3:**

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:

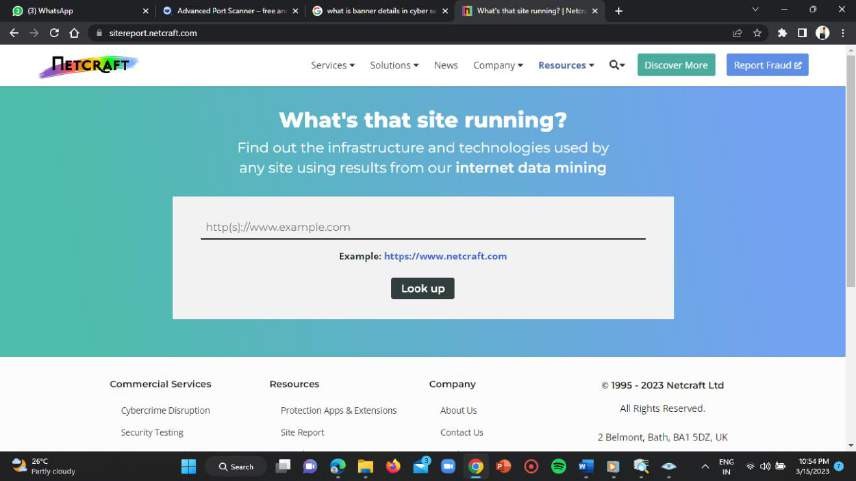
Open google chrome.



## STEP-2:

Enter the link for the website i.e,

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



## STEP-3:

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



# 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 6) netcraft
2. advanced IP scanner
3. advanced port scanner
4. nmap
5. proton VPN