**TASK – 1**

**TARGET**:-

Collect the following details from the given IP addresses using OSINT/foot printing techniques:

1. Domain Name
2. Registrar and hosting organisation of the website.
3. Hosting web server and OS.
4. C0 – hosted website list.

**SYNOPSIS:-**

In this task we have performed footprinting technique using OSINT or other footprinting techniques on the provided target IP addresses. Footprinting is the very first step/phase in both hacking and ethical hacking where the required data to gain and maintain access on a particular domain will be collected. This technique/phase is mainly used to find out the vulnerabilities present in the respective target domains. Vulnerabilities are the loop holes by which a hacker can gain and maintain the access on the target domain and by this the hacker can have the unauthorised access of the sensitive data of the domain. In this task we have collected the data regarding.

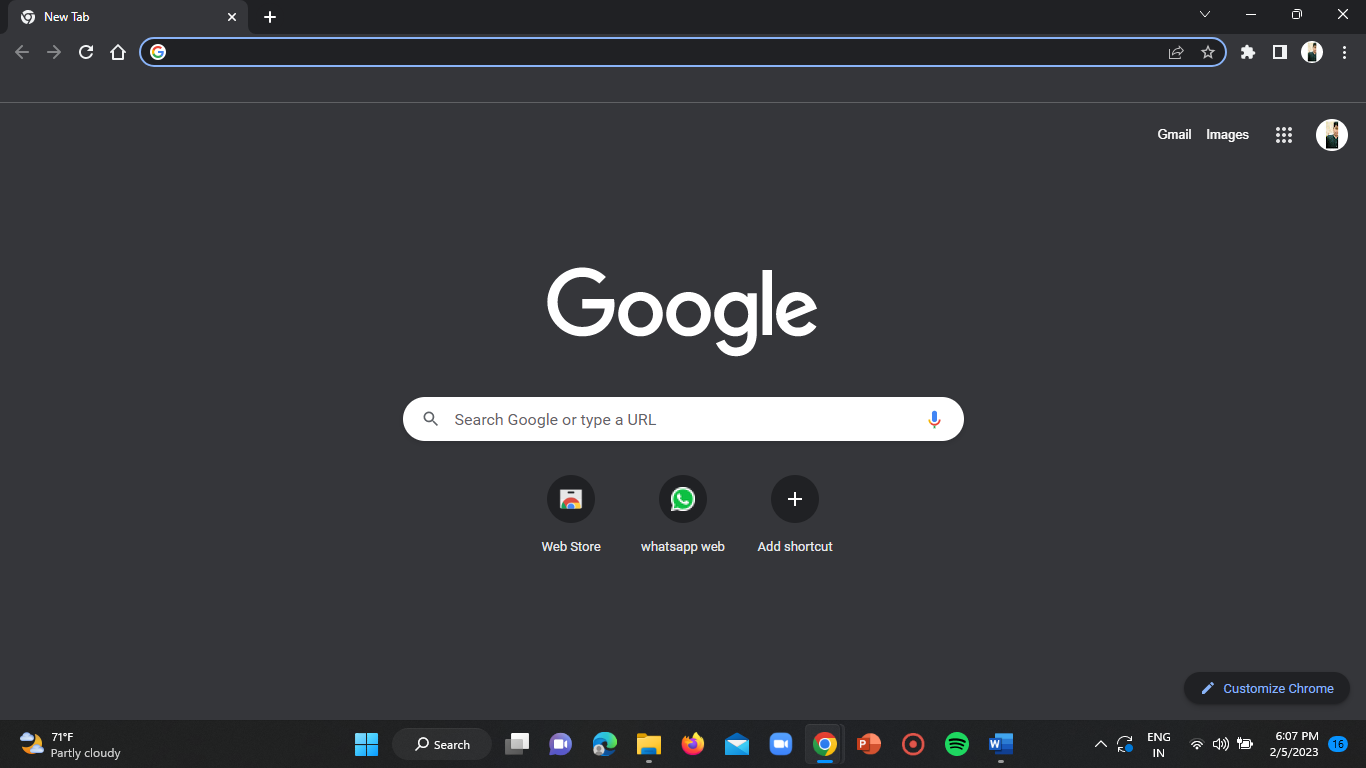
1. DOMAIN NAME OF THE IP ADDRESS.
2. REGISTRAR OF THE DOMAIN.
3. HOSTING ORGANISATION OF THE DOMAIN.
4. HOSTING WEB SERVER AND OS OF THE DOMAIN.
5. CO – HOSTED WEBSITES OF THE DOMAIN.

**1)DOMAIN NAMES :-**

**TOOL USED :- “SHODAN.IO”**

**Step-1:**

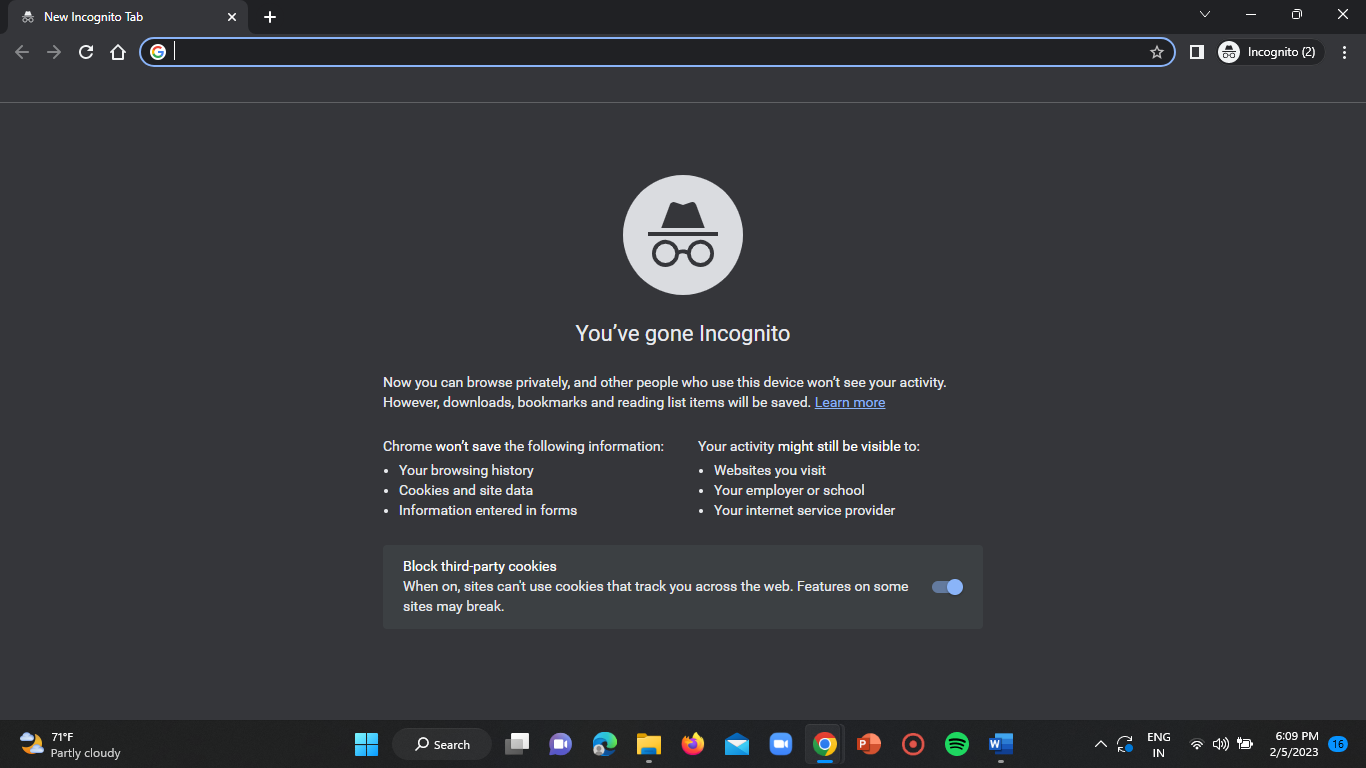
Open google chrome.



**Step-2:**

Open an incognito window.

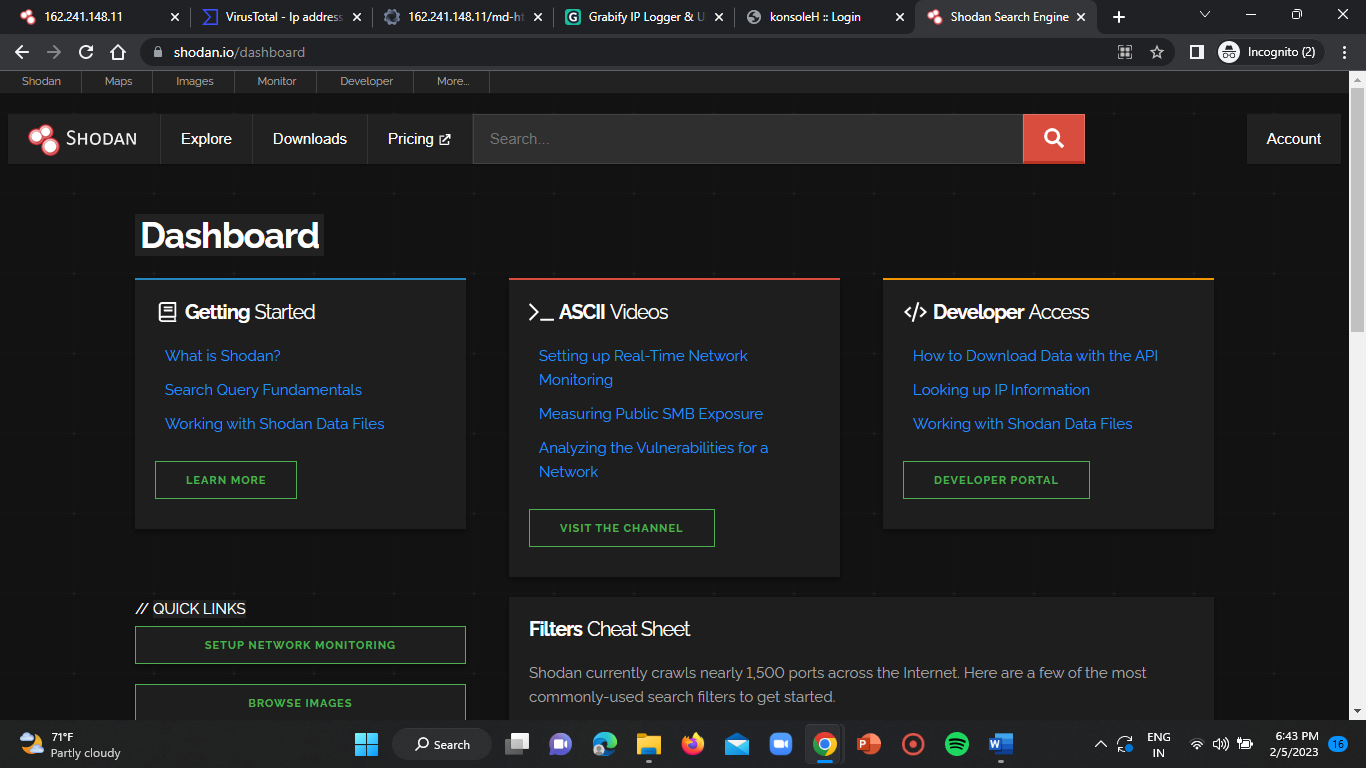
Use the shortcut = ctrl+shift+n



**Step-3:**

In the search bar enter the link of shodan webpage and signup or login to your shodan account.

Link: <https://www.shodan.io/>

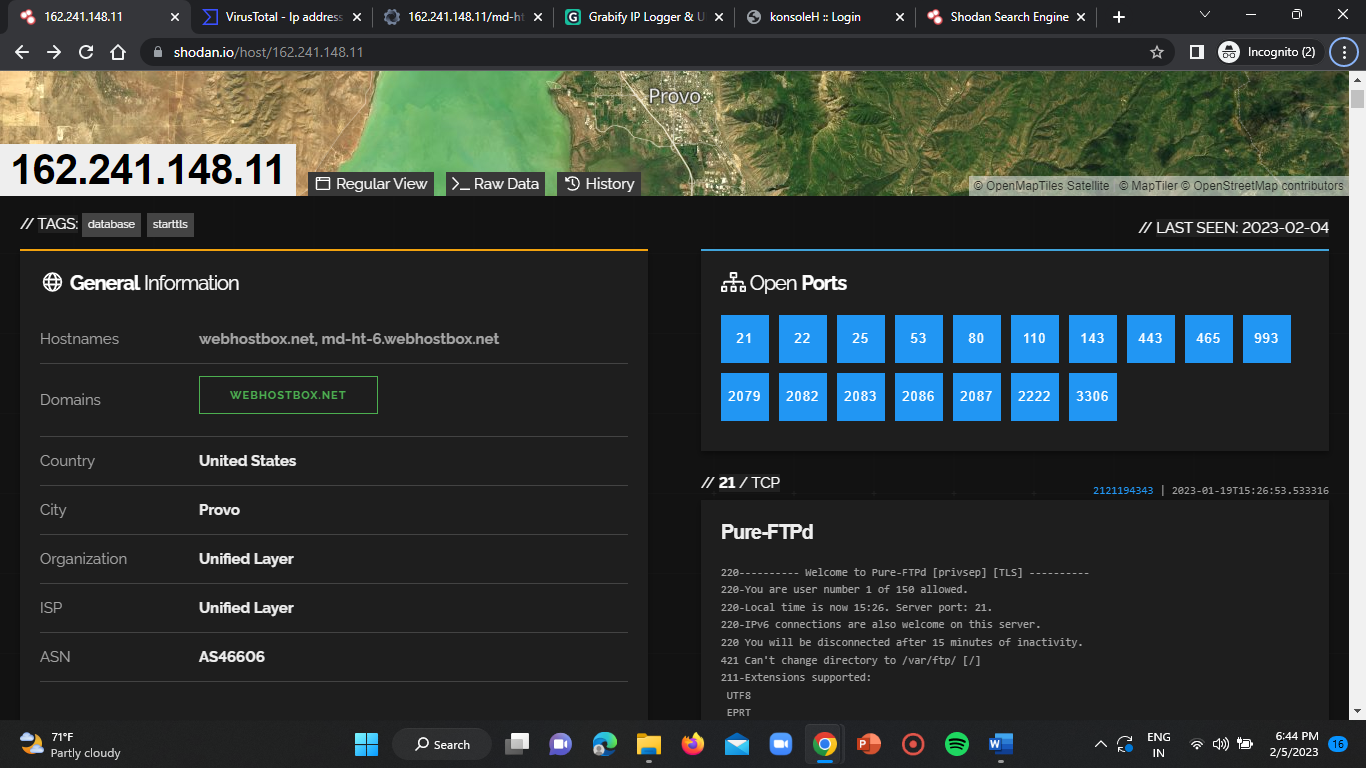


**Step-5:**

Enter the target URL in the search bar and click on enter.

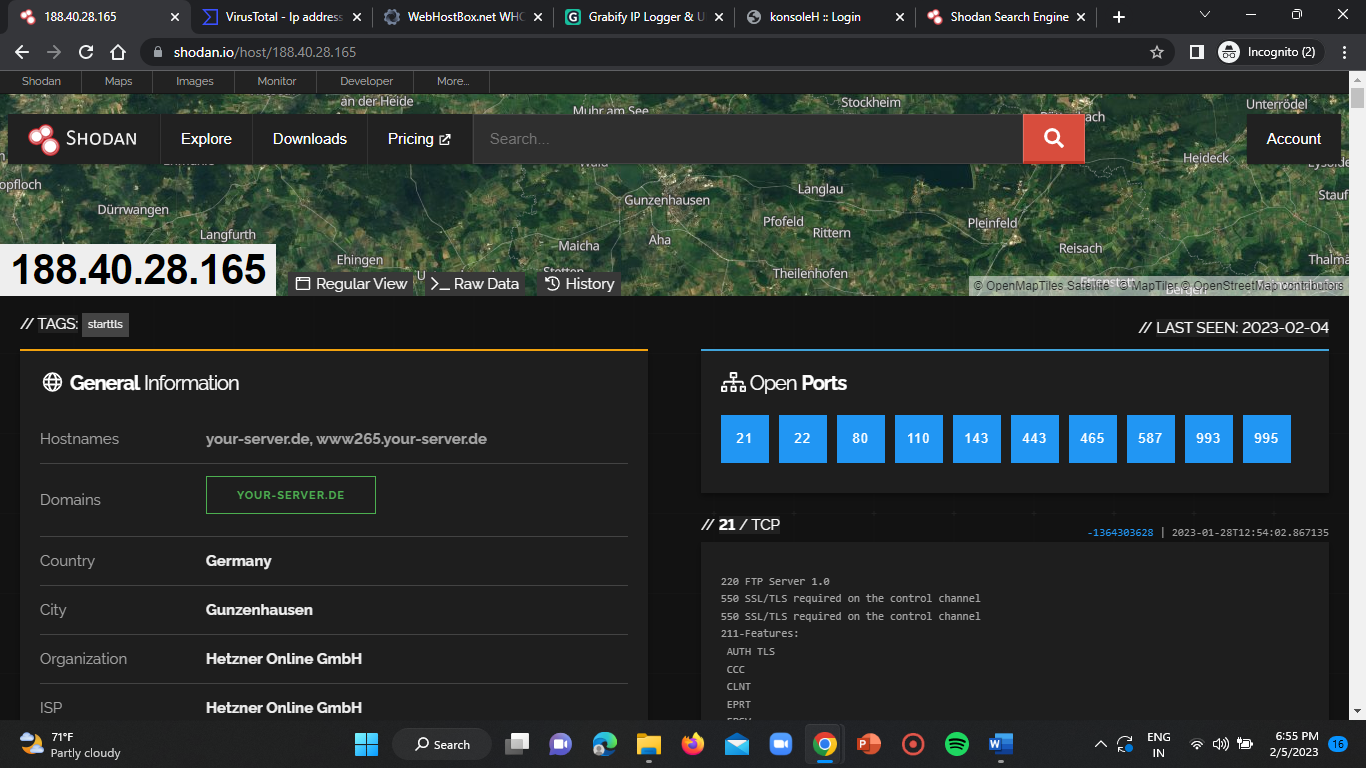
**IP ADDRESS-1:-** **“**webhostbox.net**”** (162.241.148.11)

LINK: <https://md-ht-6.webhostbox.net/>



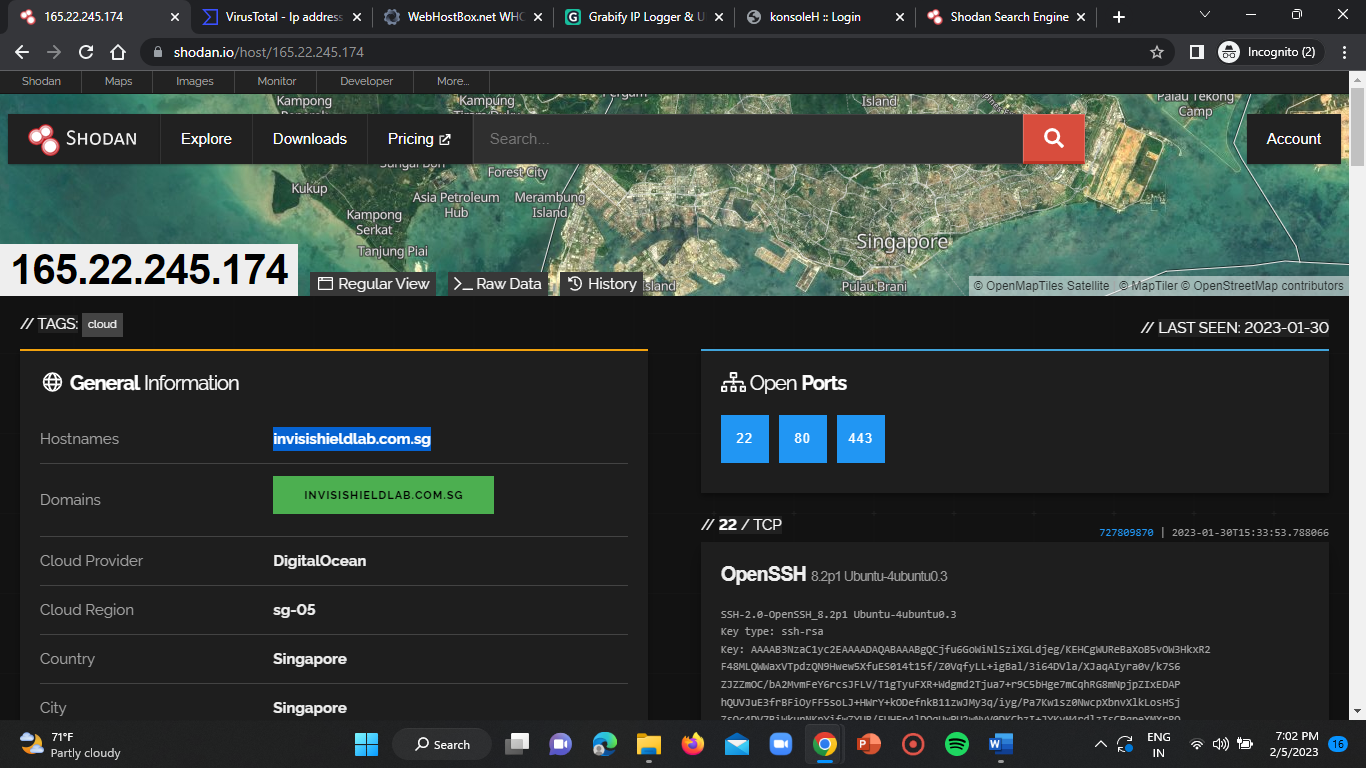
**IP ADDRESS-2:- “**your-server.de**”**(188.40.28.165)

LINK: <https://www.shodan.io/domain/your-server.de>



**IP ADDRESS-3:- “invisishieldlab.com.sg”(**165.22.245.174**)**

LINK: <https://www.shodan.io/domain/invisishieldlab.com.sg>



**2)REGISTRAR AND HOSTING ORGANISATION OF THE WEBSITE:-**

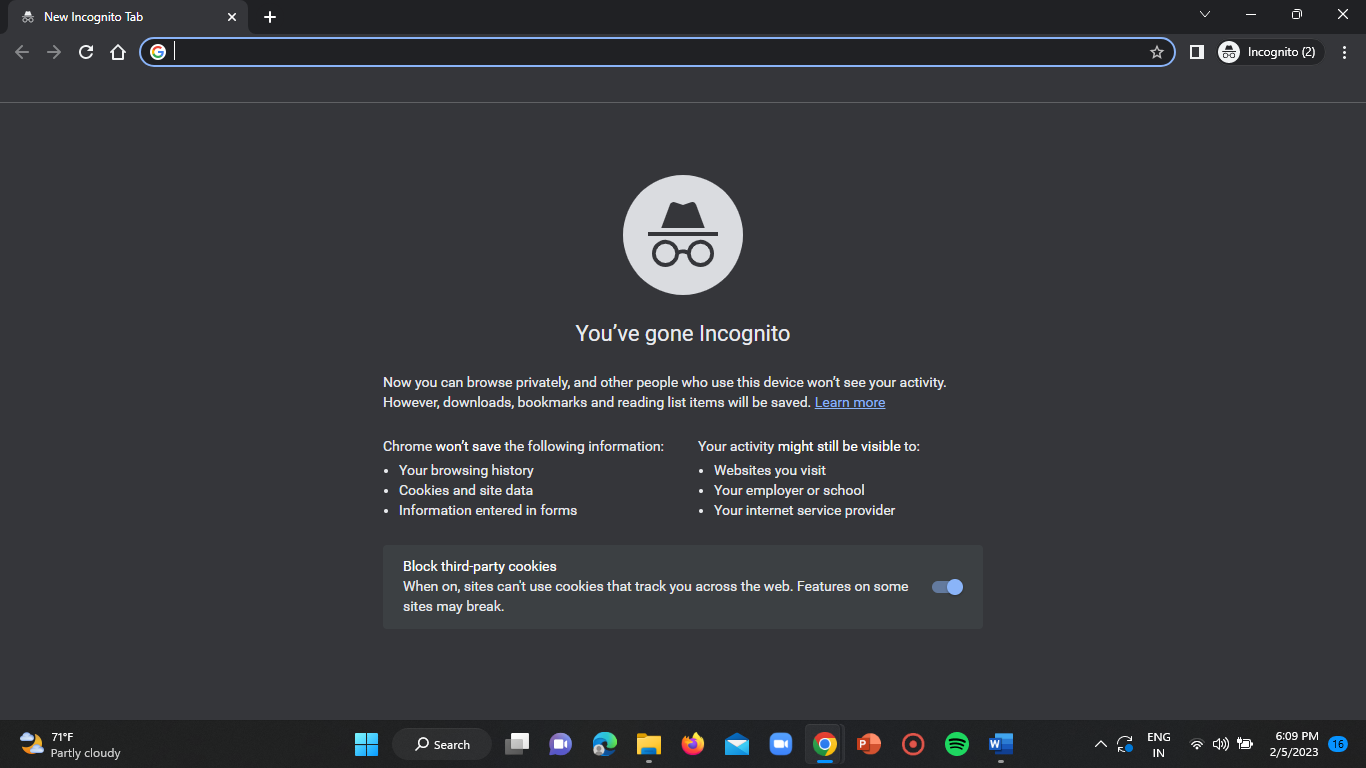
**TOOL USED:- “**WHOIS LOOKUP**”**

**LINK:** <https://whois.domaintools.com/>

**Step-1:**

Open an incognito window in the google chrome using the below mentioned shortcut key.

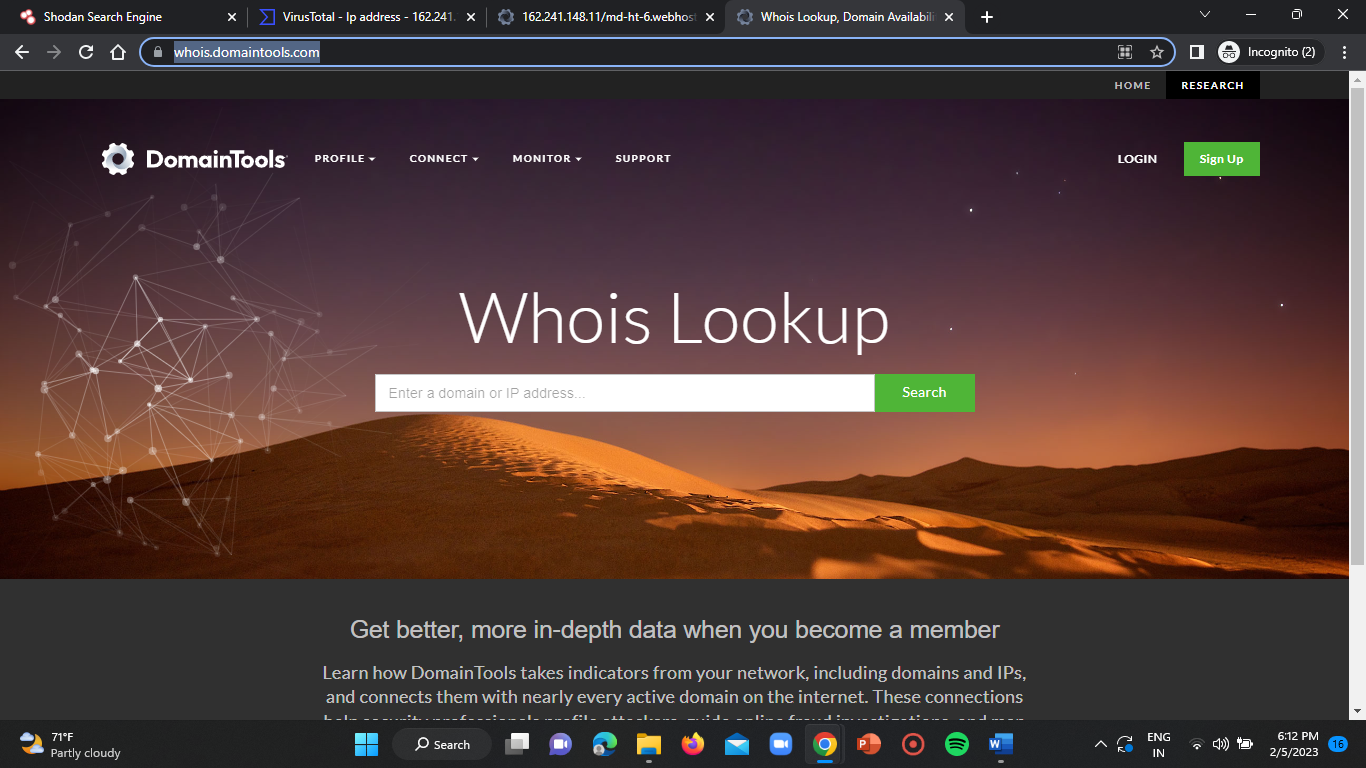
Shortcut = ctrl+shift+n



**Step-2:**

Enter the URL of the whoislookup website in the search bar and click on enter.

LINK: <https://whois.domaintools.com/>



**Step-3:**

Enter the respective domain name obtained in the above task in the search bar of the whoislookup home page.

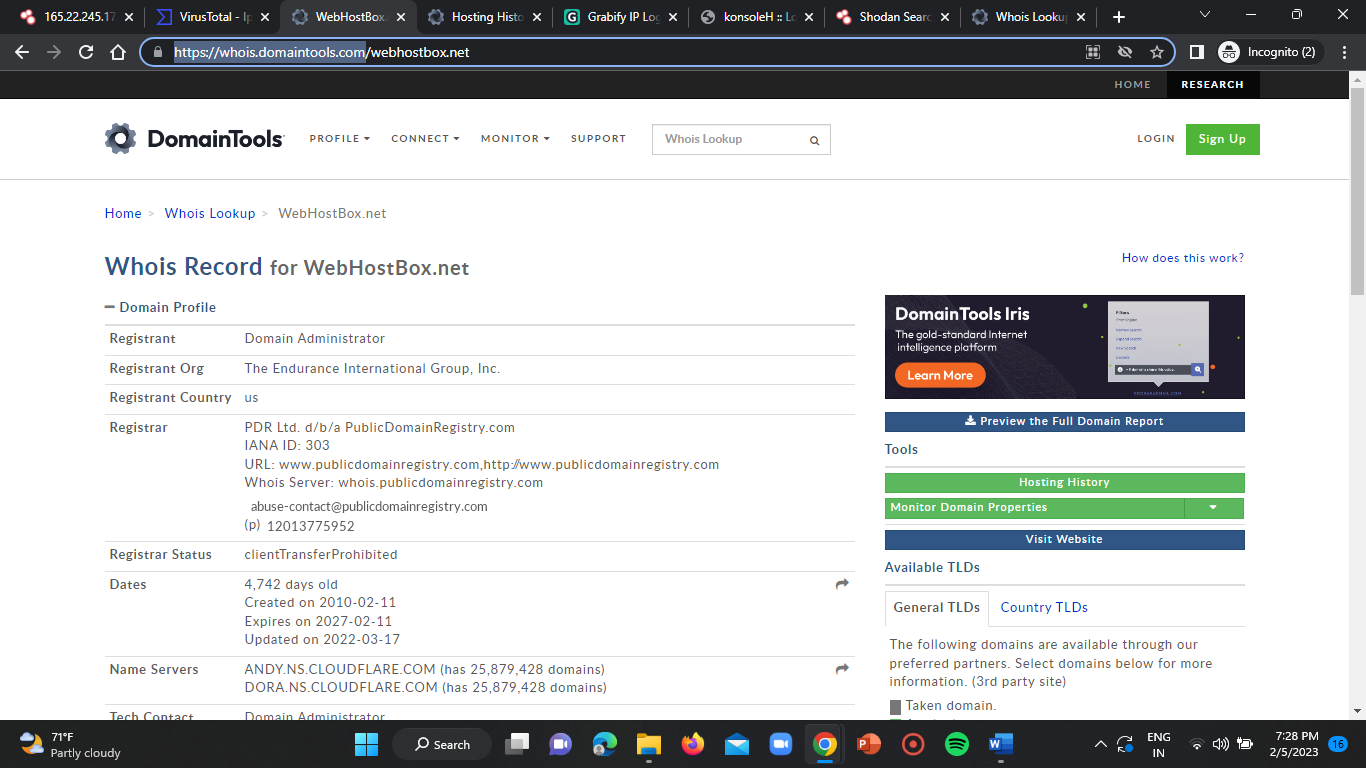
Then click on enter.

You will be displayed the registrar and organisation details of the domain.

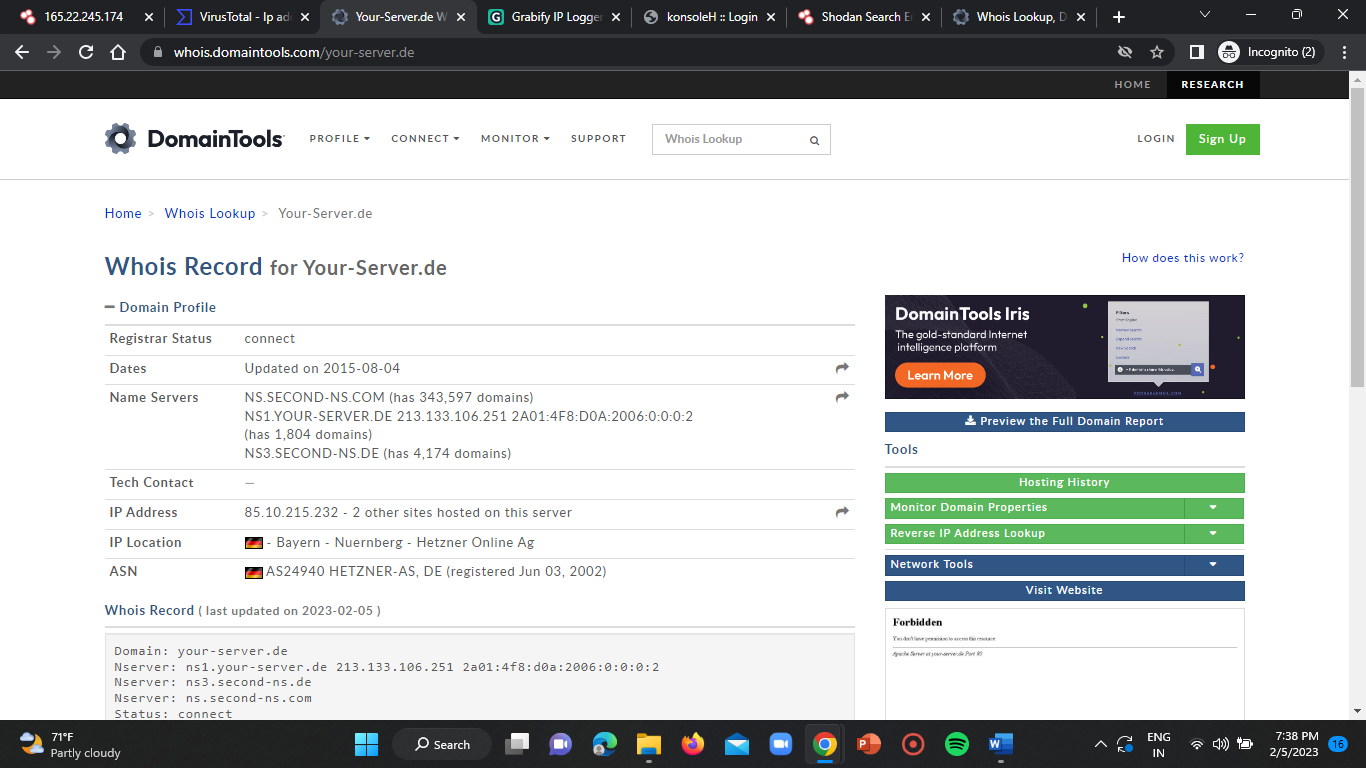
**IP ADDRESS-1:-** (162.241.148.11)

**Registrar =** PDR ltd.

**Hosting organisation =** The Endurance International Group, Inc.



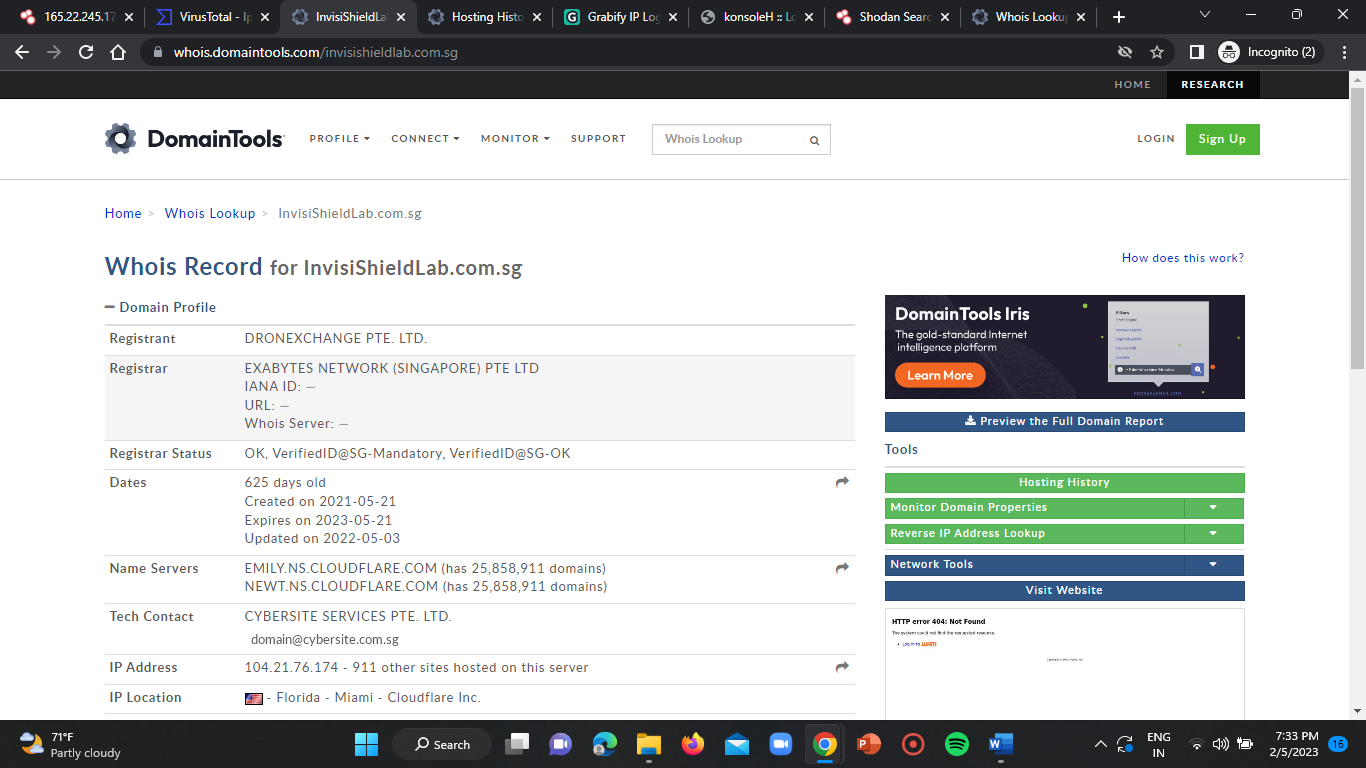
**IP ADDRESS-2:-** (188.40.28.165)



**IP ADDRESS-3:- (**165.22.245.174**)**

**Registrar =** EXABYTES NETWORK (SINGAPORE) PTE LTD

**Hosting organisation =** DRONEXCHANGE PTE. LTD.

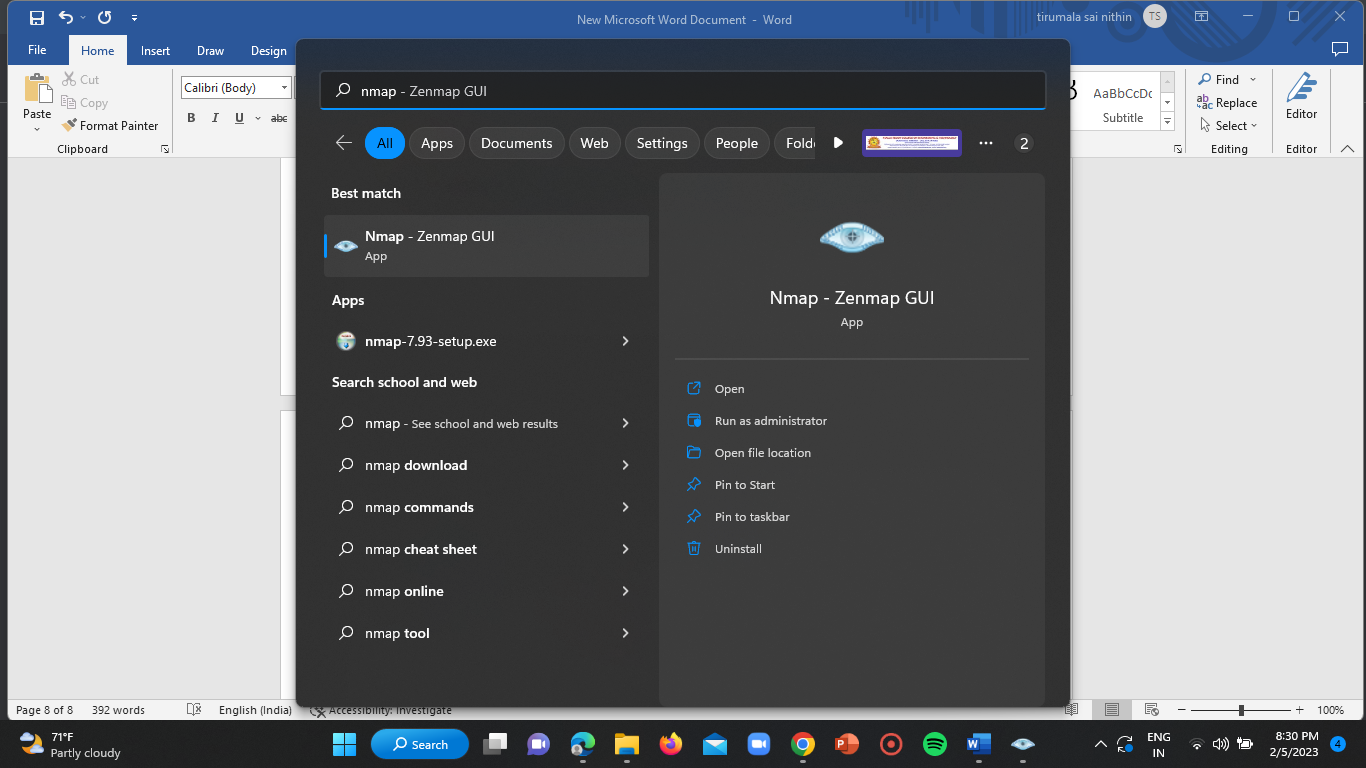
****

**3)HOSTING WEB SERVER AND OPERATING SYSTEM:-**

**TOOL USED:- “** NMAP-ZENMAP GUI **”**

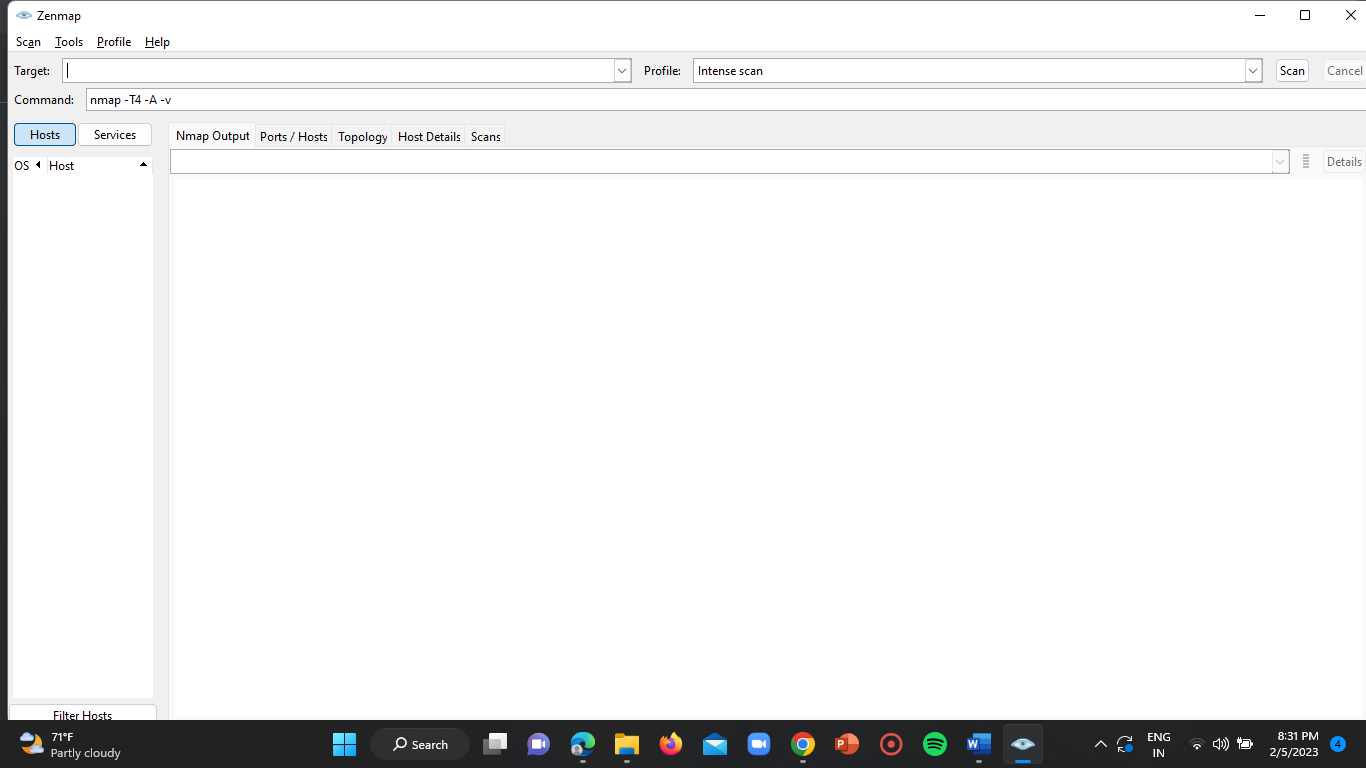
**Step-1:**

Click on start and search for “nmap” .



**Step-2:**

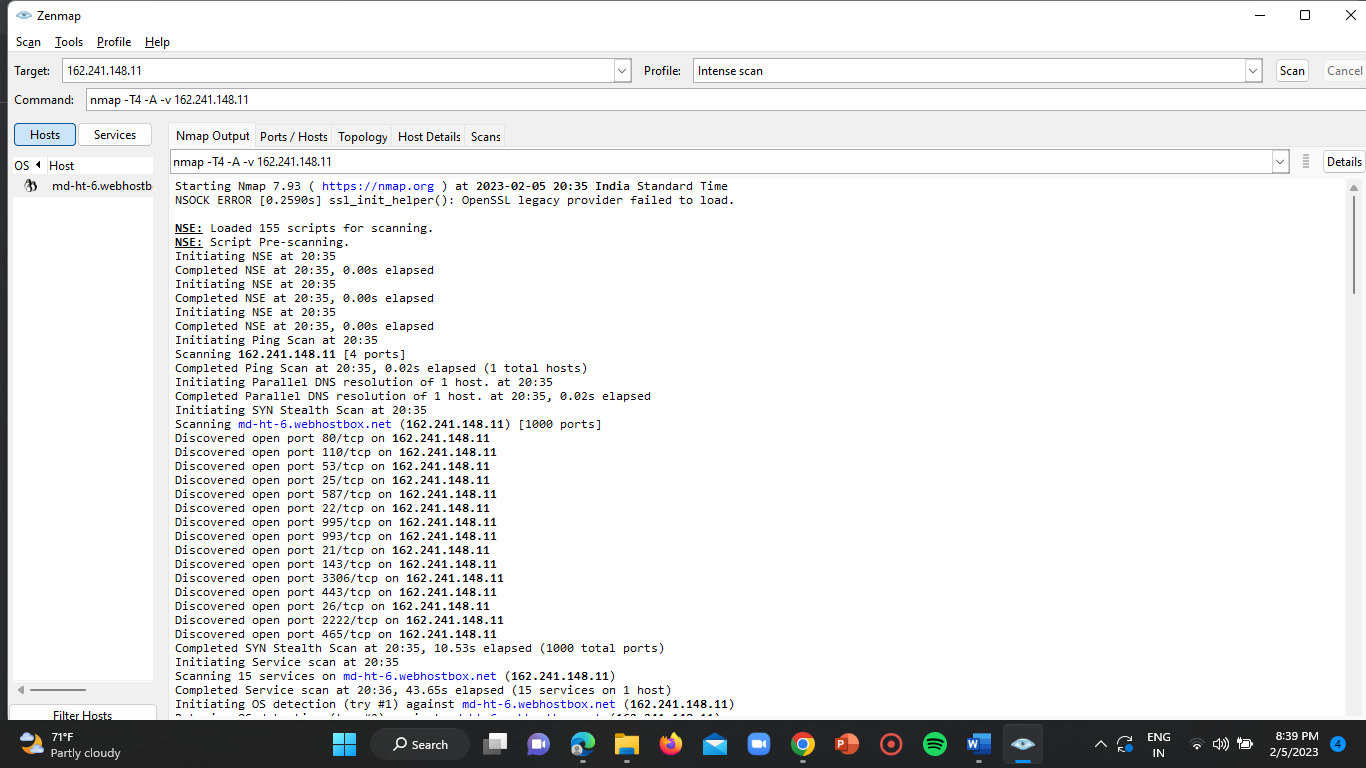
Open zenmap in administrator mode.



**Step-3:**

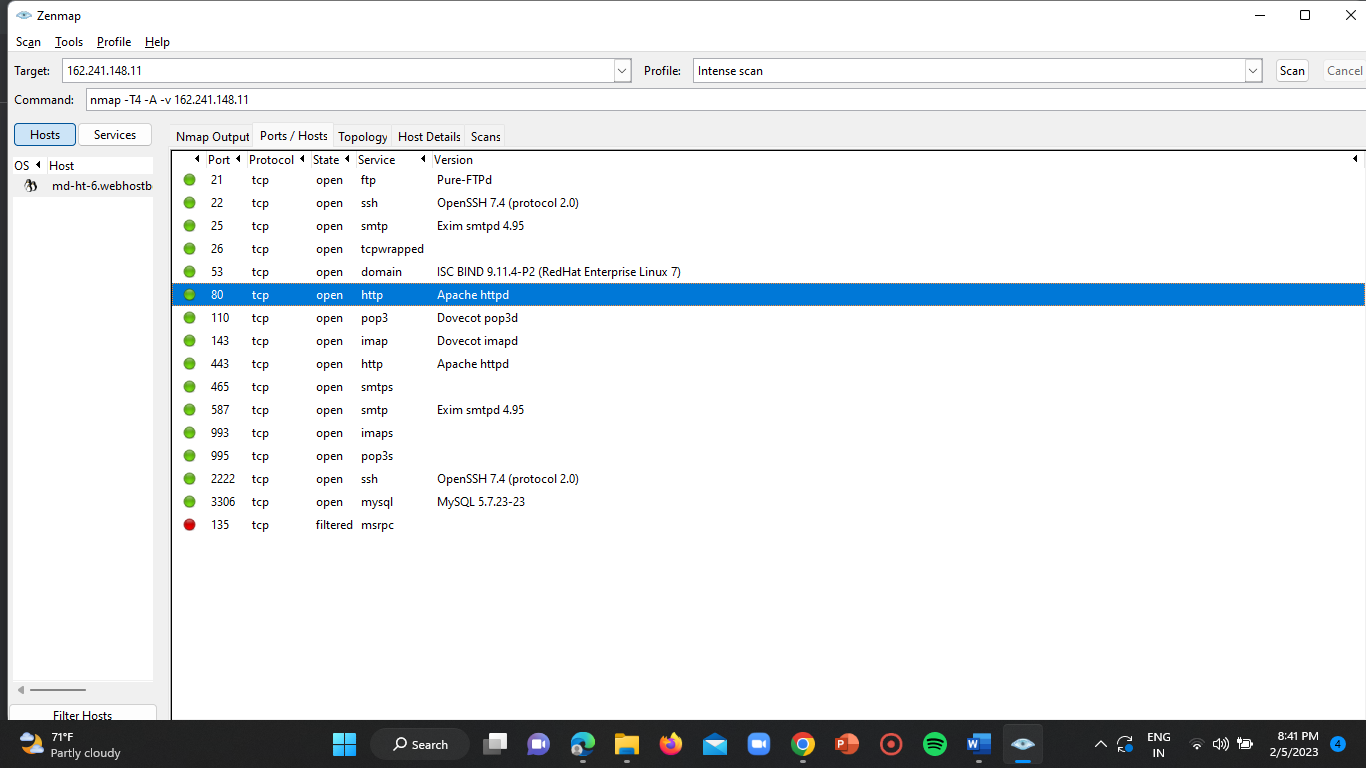
Enter the target IP address or domain name in the target input section of the nmap home page and select the option “intense scan” option in the profile section and then click on scan.

Wait until the scanning completes it may take sometime.



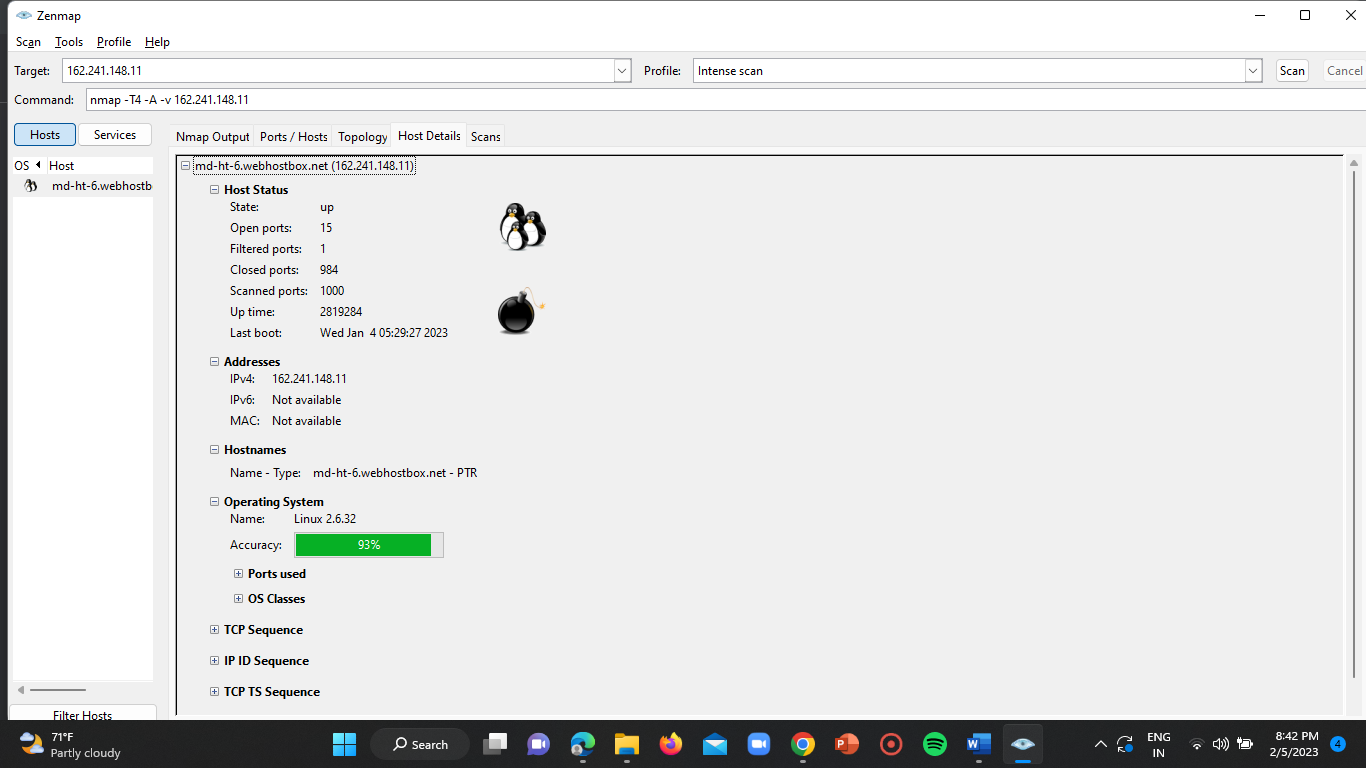
**Step-4:**

Visit hosts/ports section to find out the hosting web server.



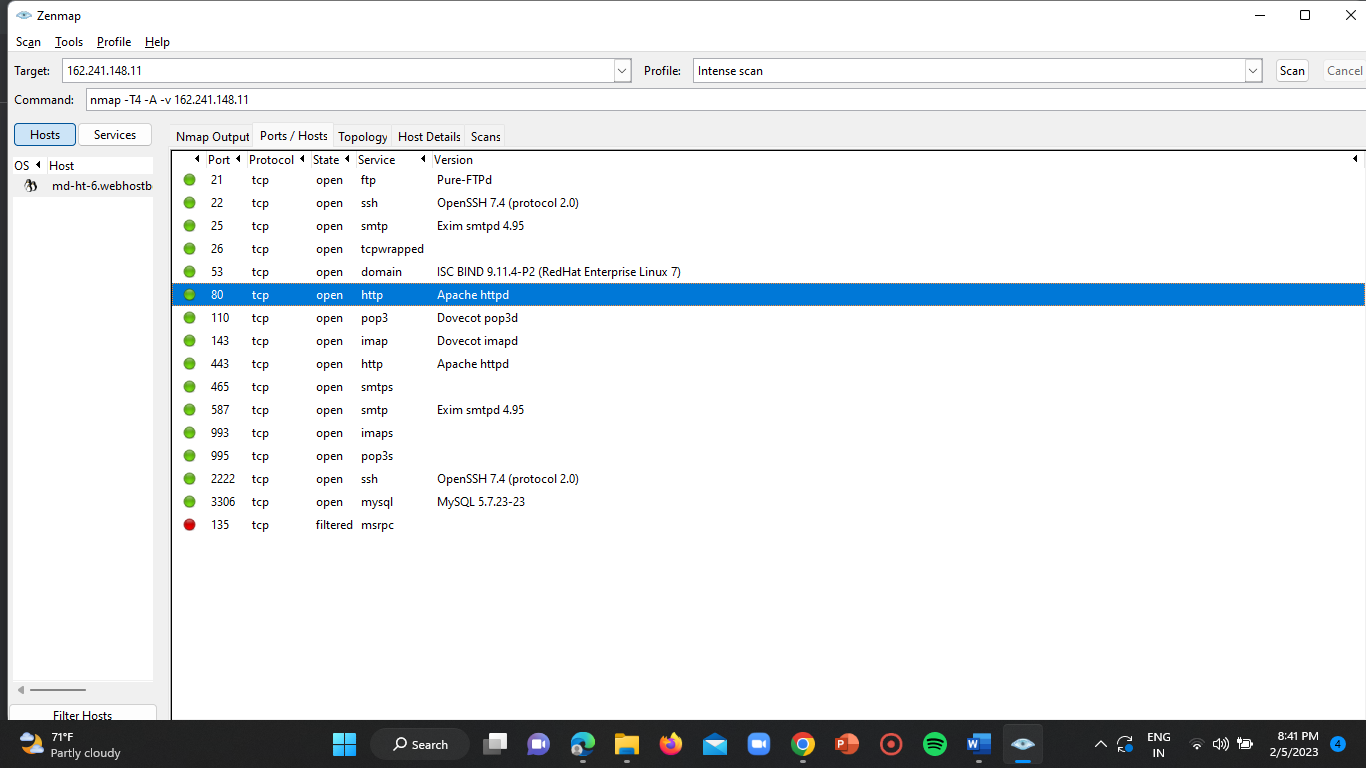
**Step-5:**

Visit the host details to get the OS details of the target IP.

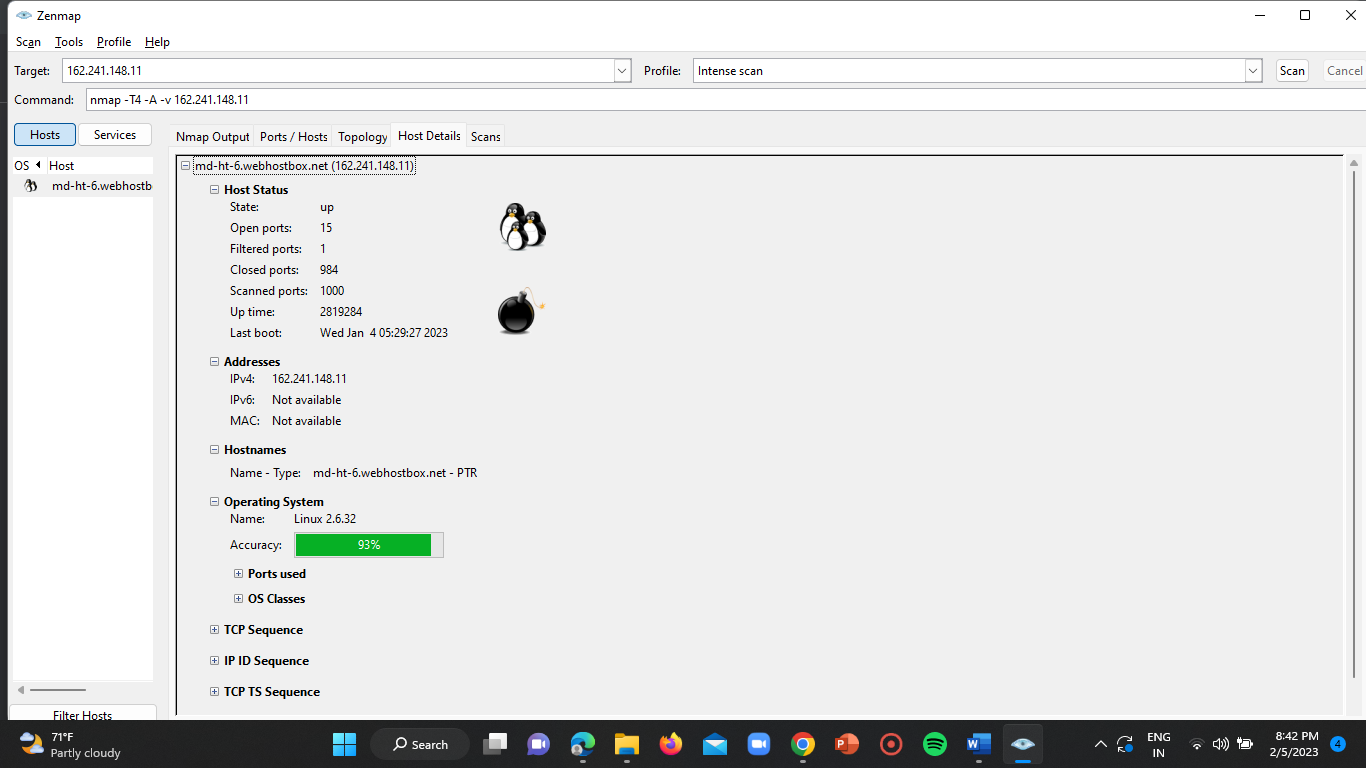


**IP ADDRESS-1:-** (162.241.148.11)

**Hosting web server =** Apache httpd

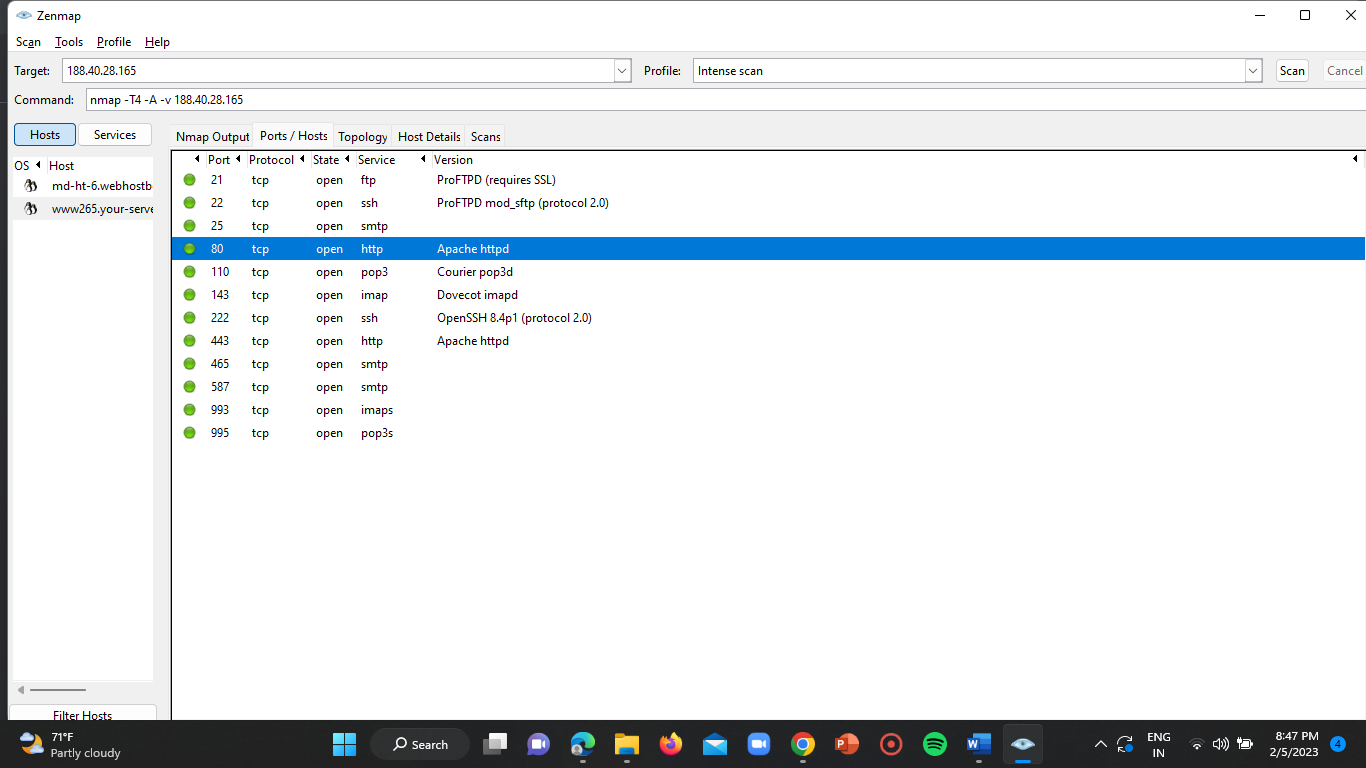


**Operating System =** Linux 2.6.32

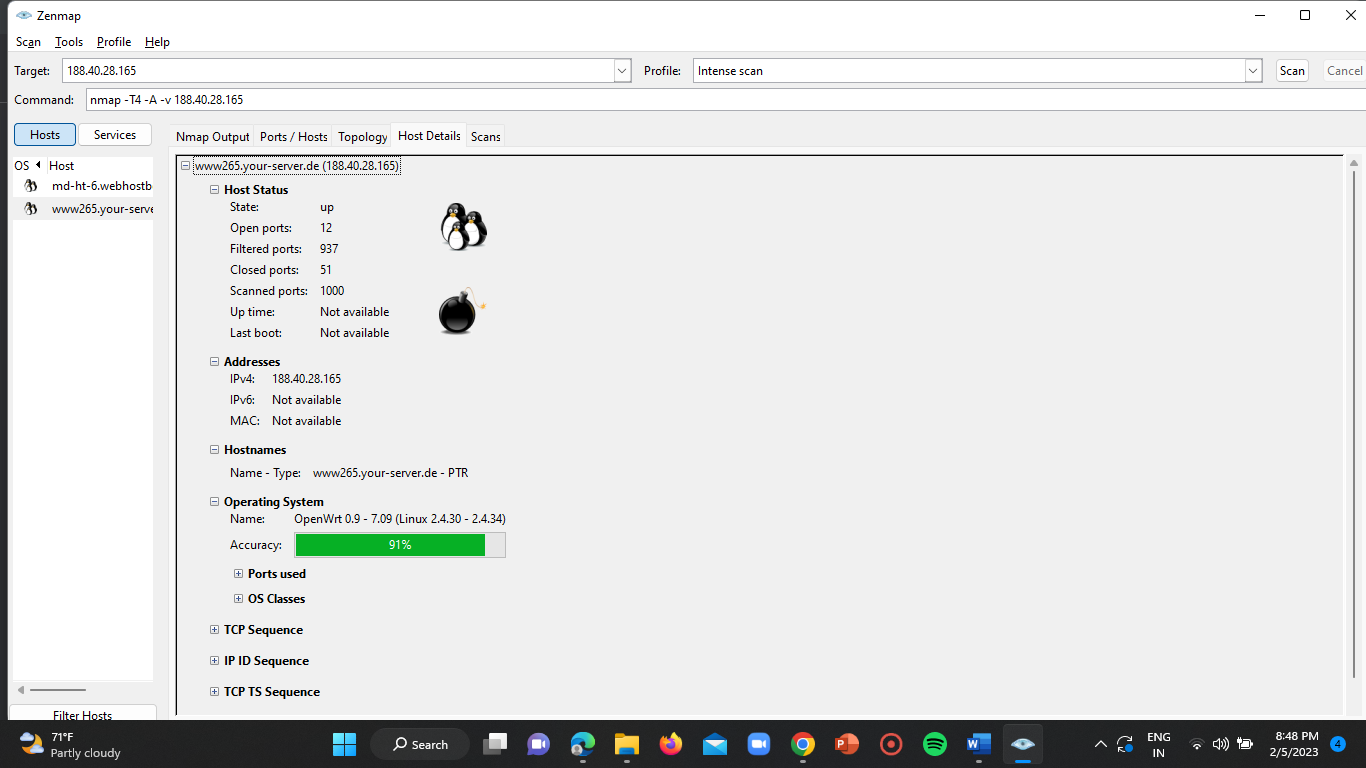


**IP ADDRESS-2:-** (188.40.28.165)

**Hosting web server =** Apache httpd

****

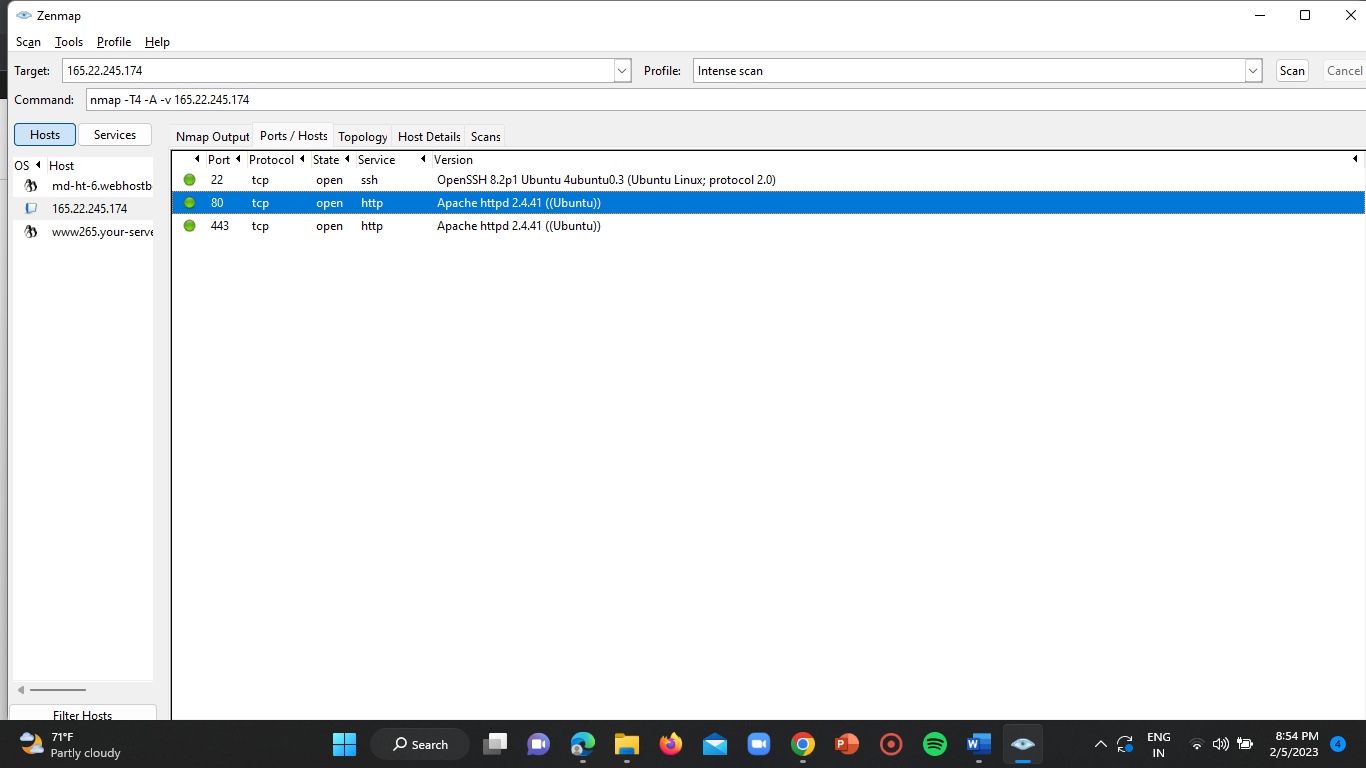
**Operating System =** Linux (2.4.30 – 2.4.34)



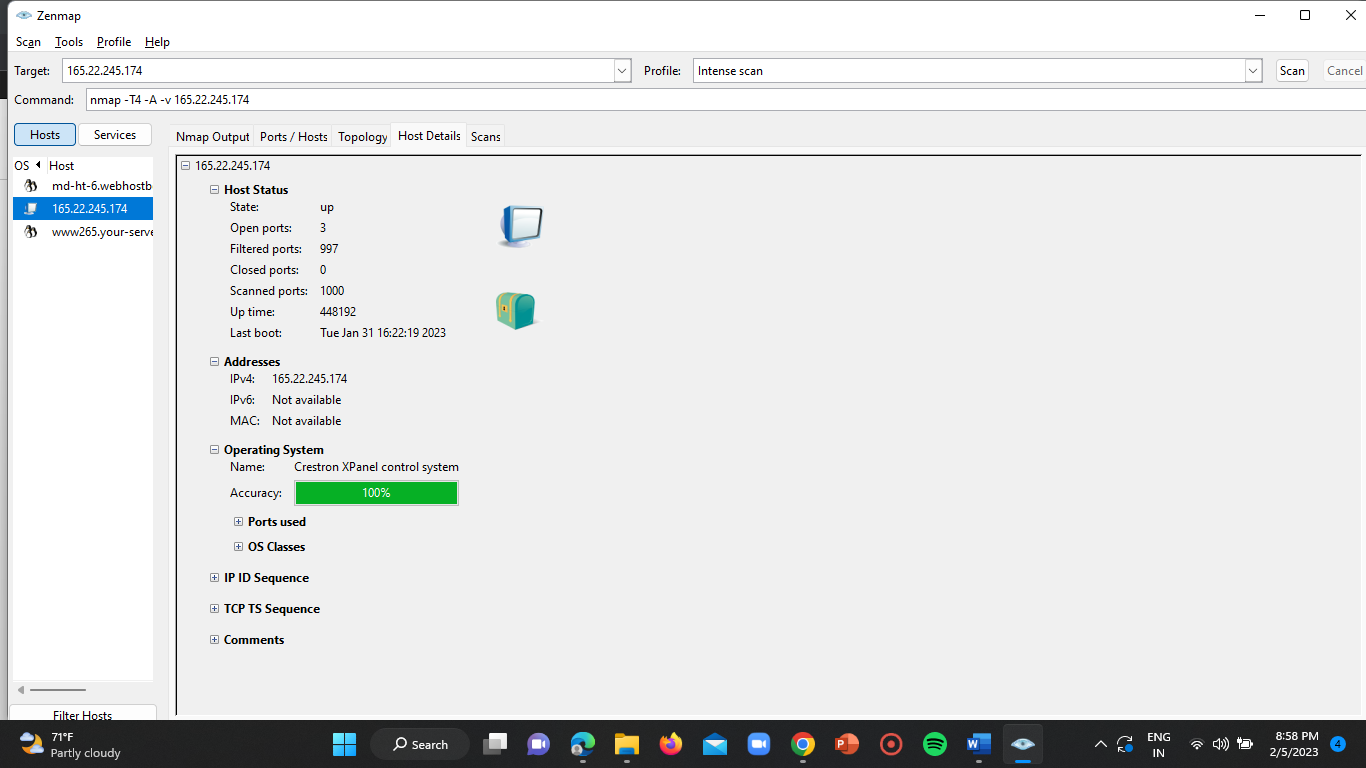
**IP ADDRESS-3:- (**165.22.245.174**)**

**Hosting web server =**

Apache httpd 2.4.41((Ubuntu))



**Operating System =** Creston XPanel control system



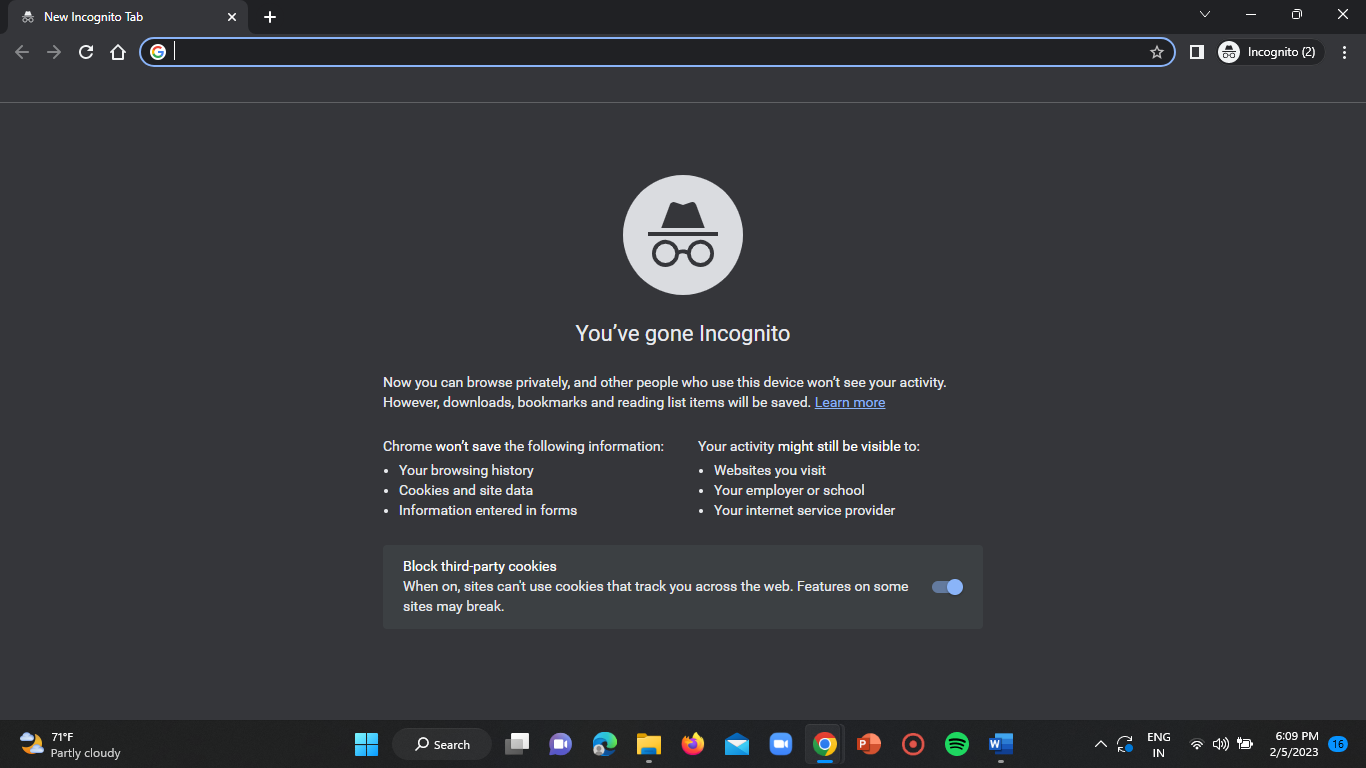
**4)CO-HOSTED WEBSITES:-**

**TOOL USED: “** VIRUSTOTAL **”**

**LINK:** <https://www.virustotal.com/gui/home/upload>

**Step-1:**

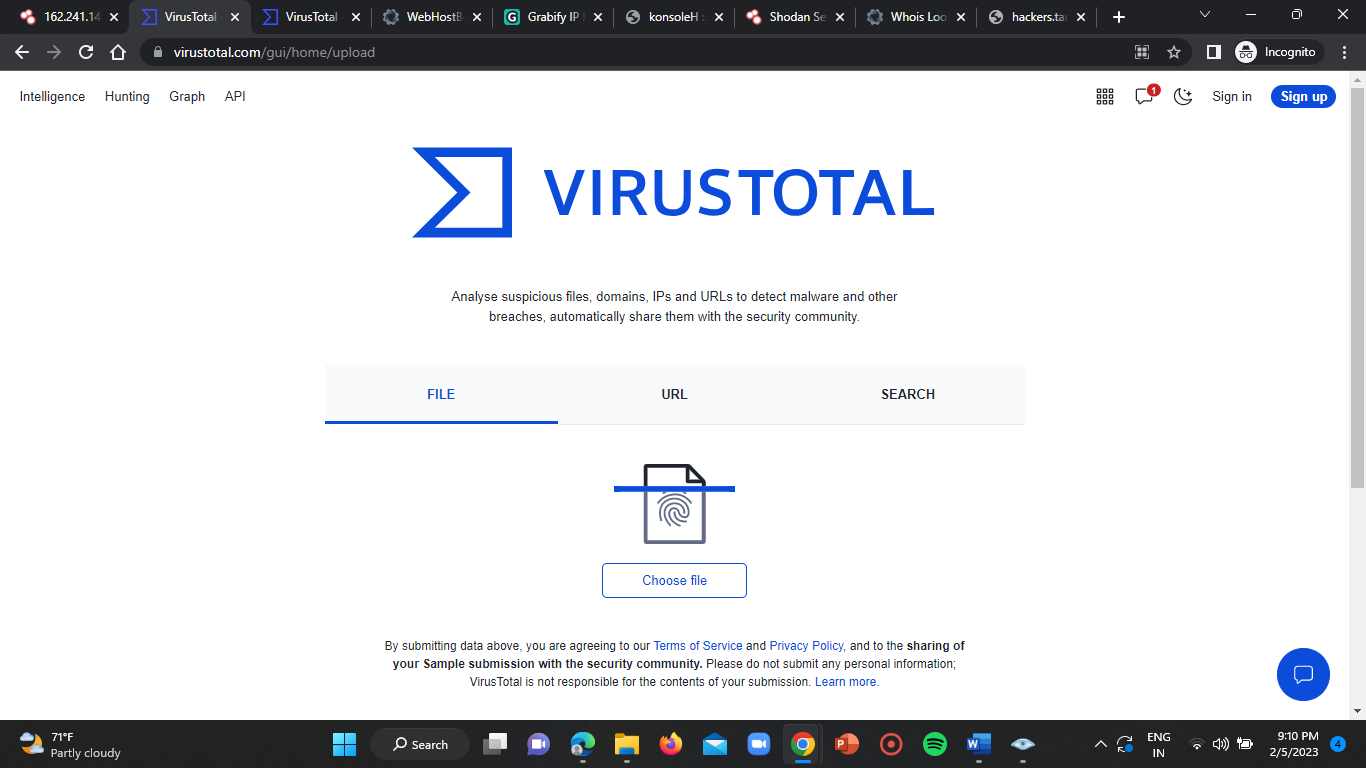
Open incognito tab in the google chrome.



**Step-2:**

Enter the URL of the “virustotal” tool in the search box of the homepage and click on enter.

Link= <https://www.virustotal.com/gui/home/upload>

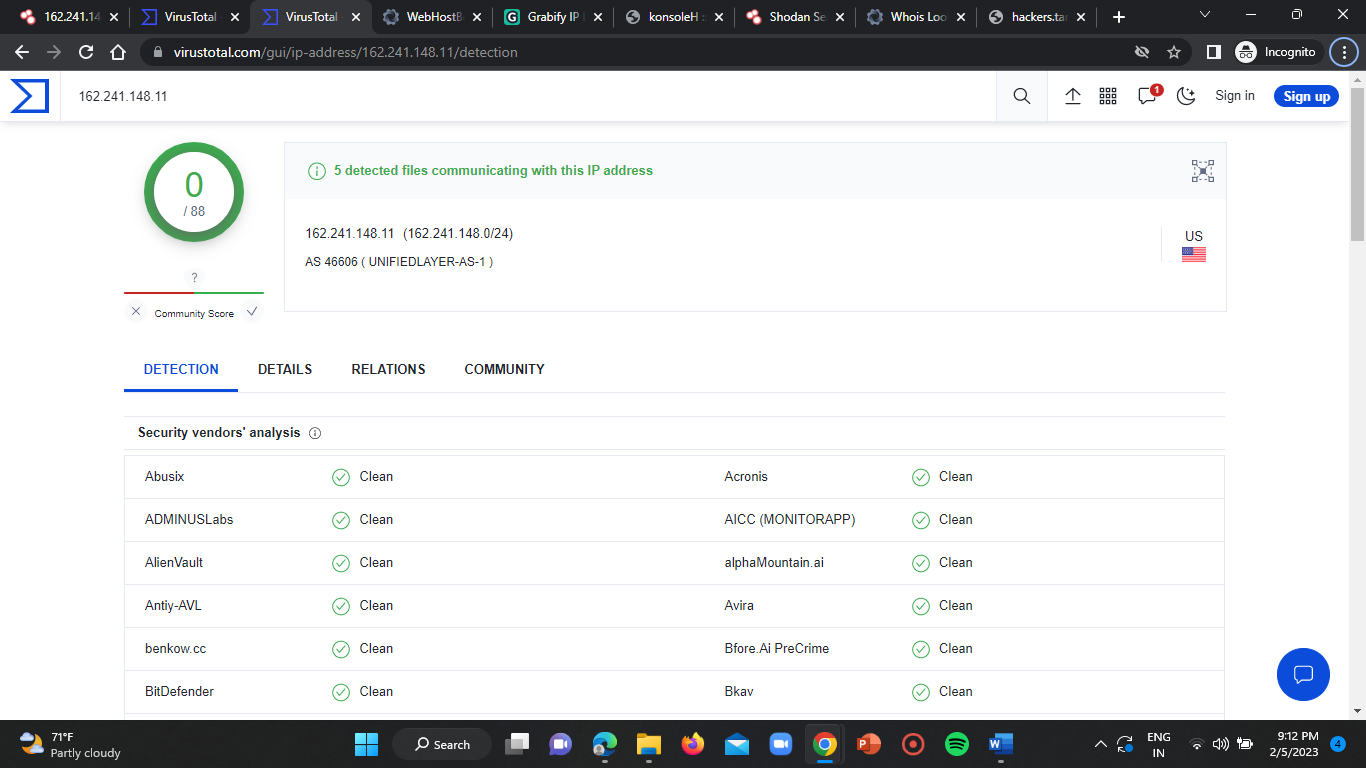


**Step-3:**

Enter the target IP address in the search section of the virustotal homepage.

Then click on enter.

The results get displayed as below.



**Step-5:**

Click on “RELATIONS” section of the result page.

Here the co-hosted websites of that particular domain gets listed.



**IP ADDRESS-1:** (162.241.148.11)

**Co-hosted websites =**

www.shreebuilding.com

shreebuilding.com

webmail.amazontechnocast.com

cpanel.amazontechnocast.com

www.amazontechnocast.com

amazontechnocast.com

puzzlehaus.mn

kaninfotech.xesstechlink.com

www.kaninfotech.xesstechlink.com

kaninfotech.in

arizaonlineservis.mayor.com.tr

www.arizaonlineservis.mayor.com.tr

arizaonlineservis.com.tr

onlinearizakayitservisi.mayor.com.tr

www.onlinearizakayitservisi.mayor.com.tr

onlinearizakayitservisi.com.tr

autodiscover.harposplace.com

mail.harposplace.com

webmail.harposplace.com

harposplace.com

****

**IP ADDRESS-2:** (188.40.28.165)

**Co-hosted websites =**

tdh3d.com

tdh-3d.com

www.zweifreunde.tv

zweifreunde.tv

traumscape.com

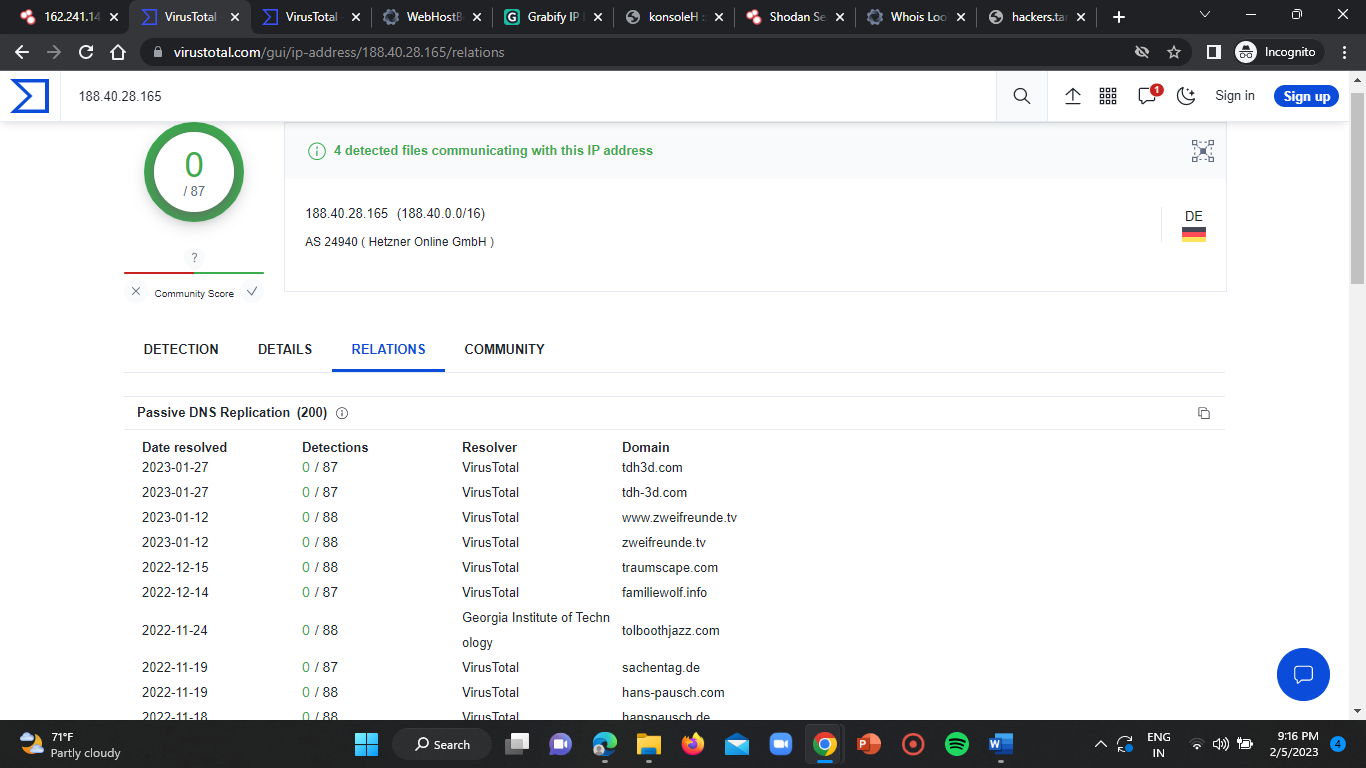
familiewolf.info

tolboothjazz.com

sachentag.de

hans-pausch.com

hanspausch.de



**IP ADDRESS-3: (**165.22.245.174**)**

**C0-hosted websites =**

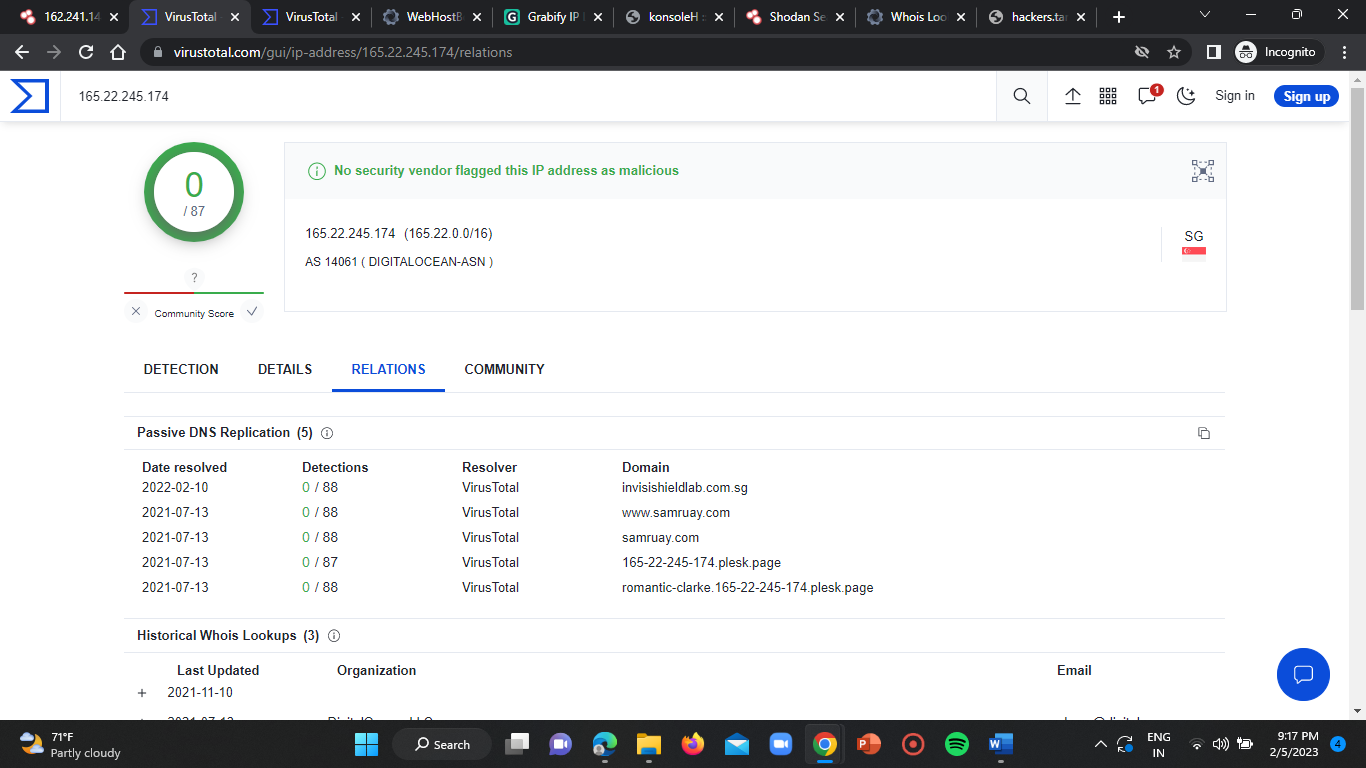
invisishieldlab.com.sg

www.samruay.com

samruay.com

165-22-245-174.plesk.page

romantic-clarke.165-22-245-174.plesk.page



**TASK OUTCOME:-**

This task is regarding about the footprinting technique used in both the hacking and the ethical hacking zones. Footprinting is the very 1st phase of the ethical hacking where we can get the data required to have an unauthorised access over the target domain. In this task we’ve collected the details of the given target IP addresses such as “DOMAIN NAME, REGISTRAR AND HOSTING ORGANISATION, HOSTING WEB SERVER AND OS, C0-HOSTED WEBSITES”. By this task we learnt the footprinting technique in different ways using different tools. Also we got to know about the importance of this footprinting phase in the ethical hacking and how a pen tester need to gather the data and identify the vulnerability using this footprinting technique which is a very basic and primary technique in the pen testing process.

Tools we’ve used:

1. Shodon.io
2. Whoislookup
3. Zenmap
4. VirusTotal