

# **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.

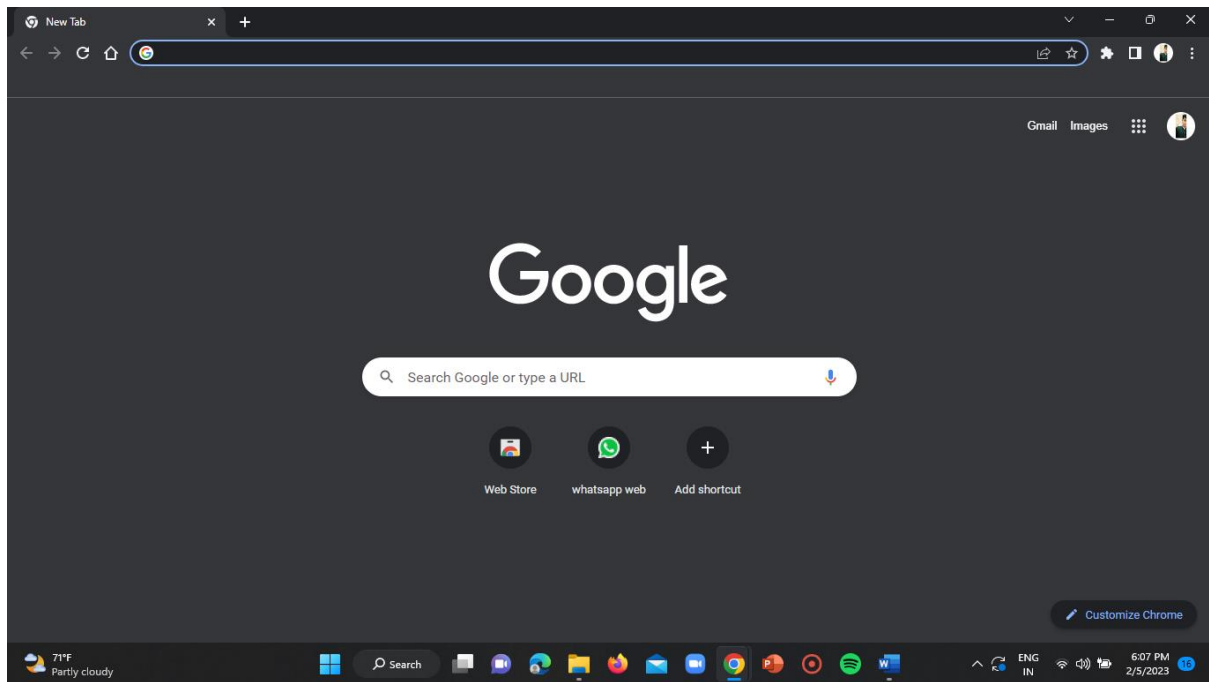
- 1) DOMAIN NAME OF THE IP ADDRESS.
- 2) REGISTRAR OF THE DOMAIN.
- 3) HOSTING ORGANISATION OF THE DOMAIN.
- 4) HOSTING WEB SERVER AND OS OF THE DOMAIN.
- 5) CO – HOSTED WEBSITES OF THE DOMAIN.

## **1)DOMAIN NAMES :-**

**TOOL USED :- “SHODAN.IO”**

### **Step-1:**

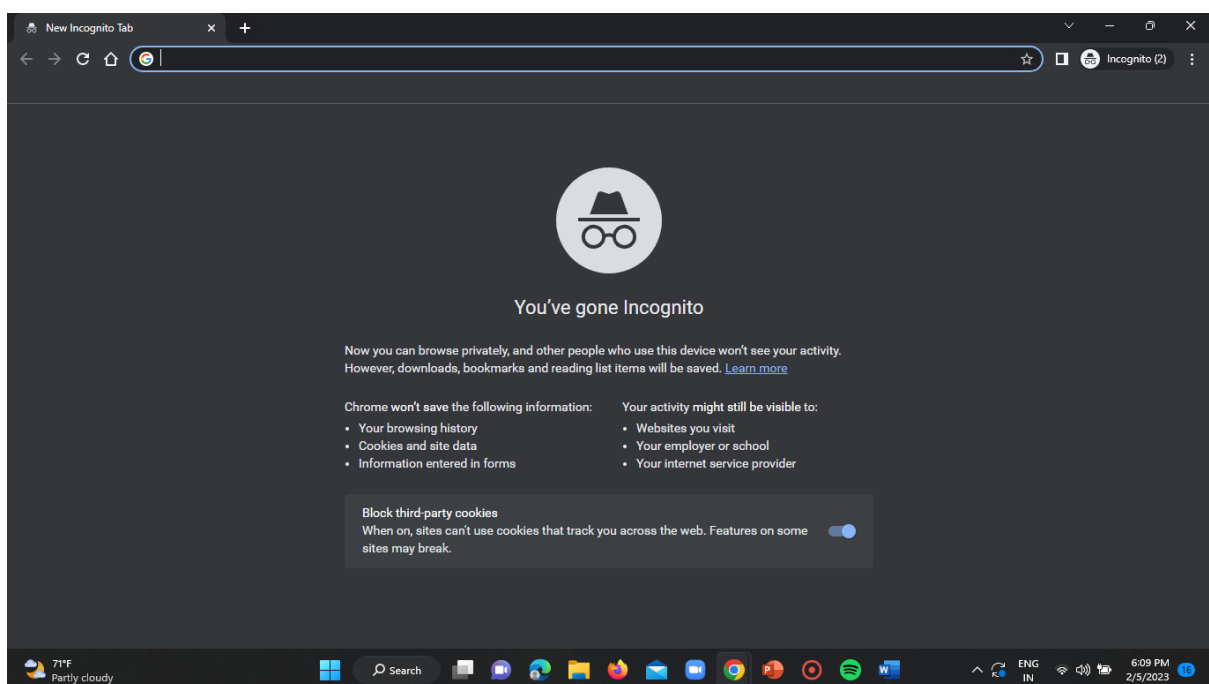
Open google chrome.



## Step-2:

Open an incognito window.

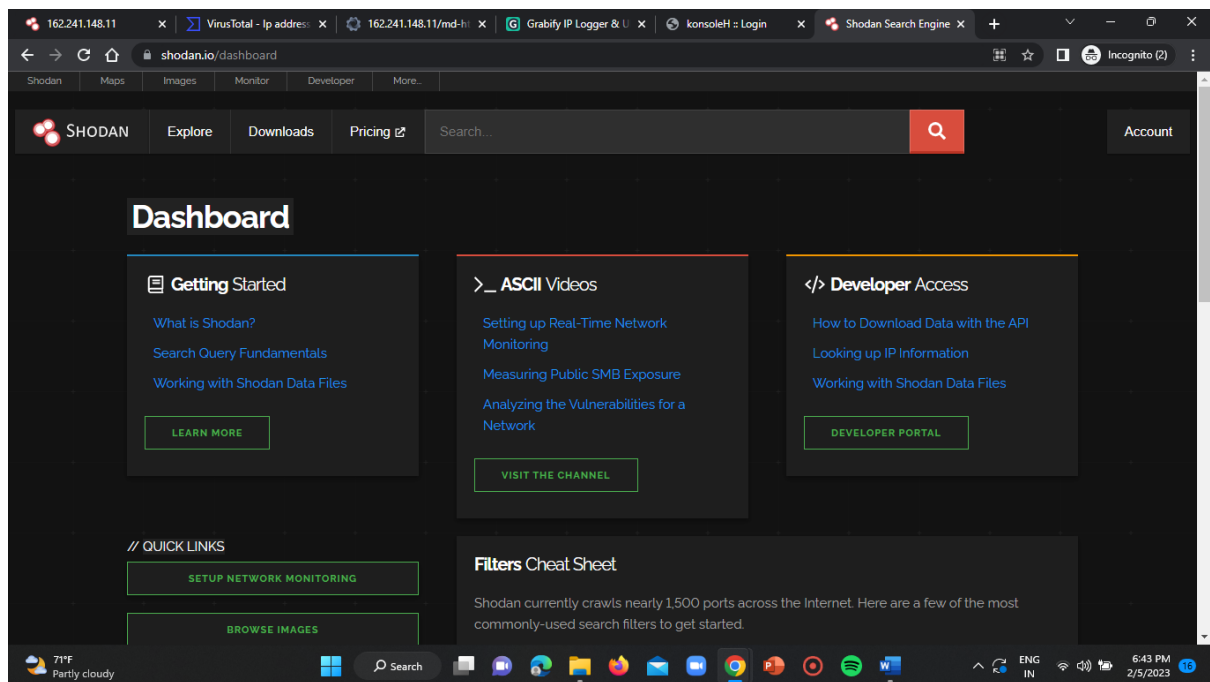
Use the shortcut = ctrl+shift+n



## 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/>

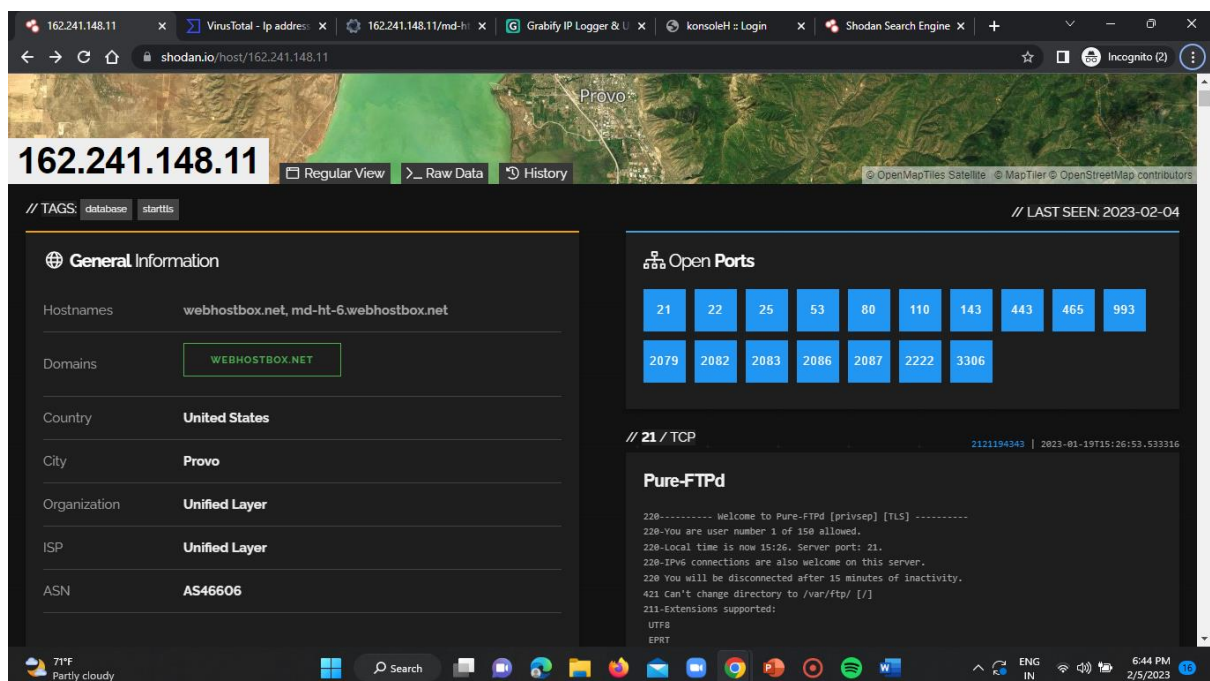


### Step-5:

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>

ST#IS#4899

The screenshot shows the Shodan search engine interface for the IP address 188.40.28.165. The top navigation bar includes links for Shodan, Maps, Images, Monitor, Developer, and More. The main header displays the IP address 188.40.28.165 and a search bar. Below the header, the 'General Information' section lists hostnames (your-server.de, www265.your-server.de), domains (YOUR-SERVER.DE), country (Germany), city (Gunzenhausen), organization (Hetzner Online GmbH), and ISP (Hetzner Online GmbH). The 'Open Ports' section shows a list of ports: 21, 22, 80, 110, 143, 443, 465, 587, 993, and 995. The '21 / TCP' section displays the banner: '228 FTP Server 1.0', '550 SSL/TLS required on the control channel', '550 SSL/TLS required on the control channel', and '211-Features: AUTH TLS, CCC, CLNT, EPRT'.

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

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

The screenshot shows the Shodan search engine interface for the IP address 165.22.245.174. The top navigation bar includes links for Shodan, Maps, Images, Monitor, Developer, and More. The main header displays the IP address 165.22.245.174 and a search bar. Below the header, the 'General Information' section lists hostnames (invisishieldlab.com.sg), domains (INVISISHIELDLAB.COM.SG), cloud provider (DigitalOcean), cloud region (sg-05), country (Singapore), and city (Singapore). The 'Open Ports' section shows a list of ports: 22, 80, and 443. The '22 / TCP' section displays the banner: 'OpenSSH 8.2p1 Ubuntu-4ubuntu0.3', 'SSH-2.0-OpenSSH\_8.2p1\_Ubuntu-4ubuntu0.3', 'Key type: ssh-rsa', and a long RSA key.

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

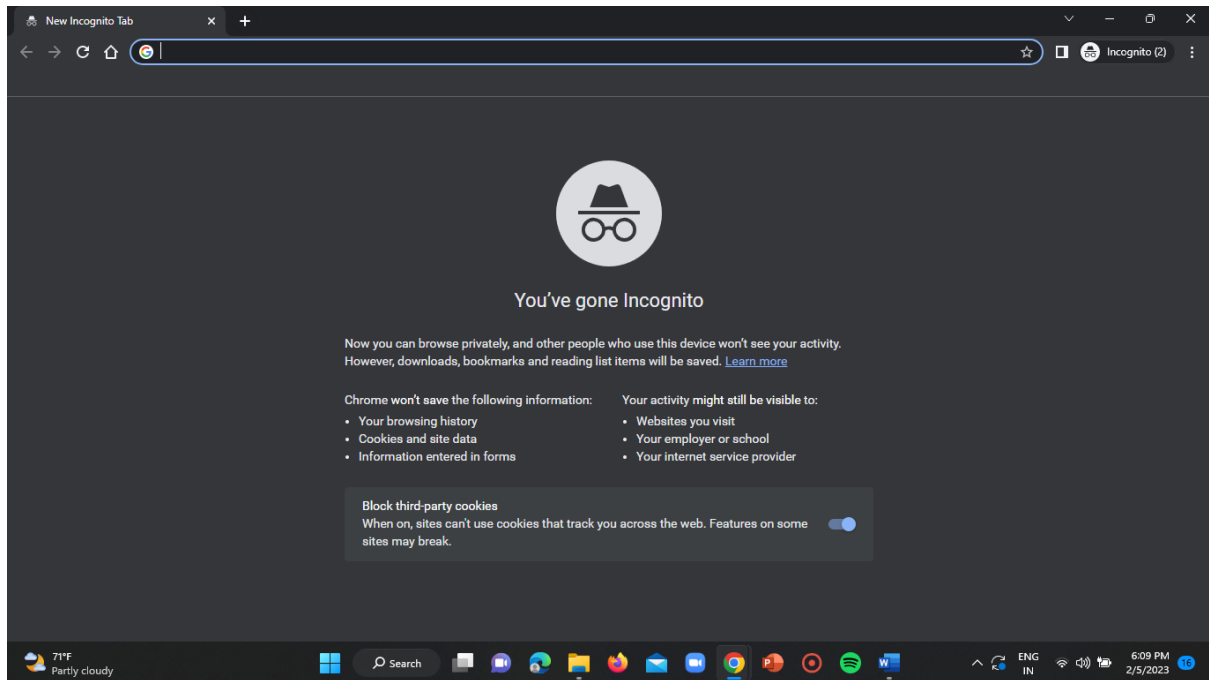
**TOOL USED:-** "WHOIS LOOKUP"

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

## Step-1:

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

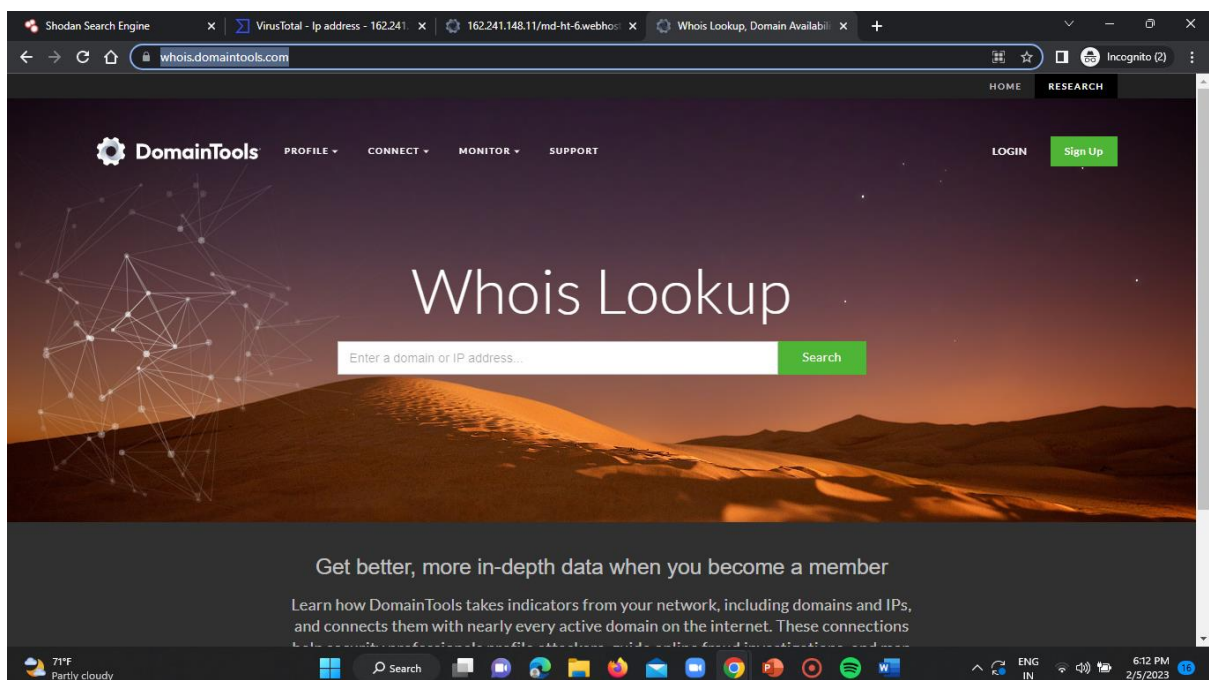
Shortcut = ctrl+shift+n



## Step-2:

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

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



ST#IS#4899

### 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.

The screenshot displays the DomainTools website interface. The browser's address bar shows the URL <https://whois.domaintools.com/webhostbox.net>. The page title is "Whois Record for WebHostBox.net". The domain profile information is as follows:

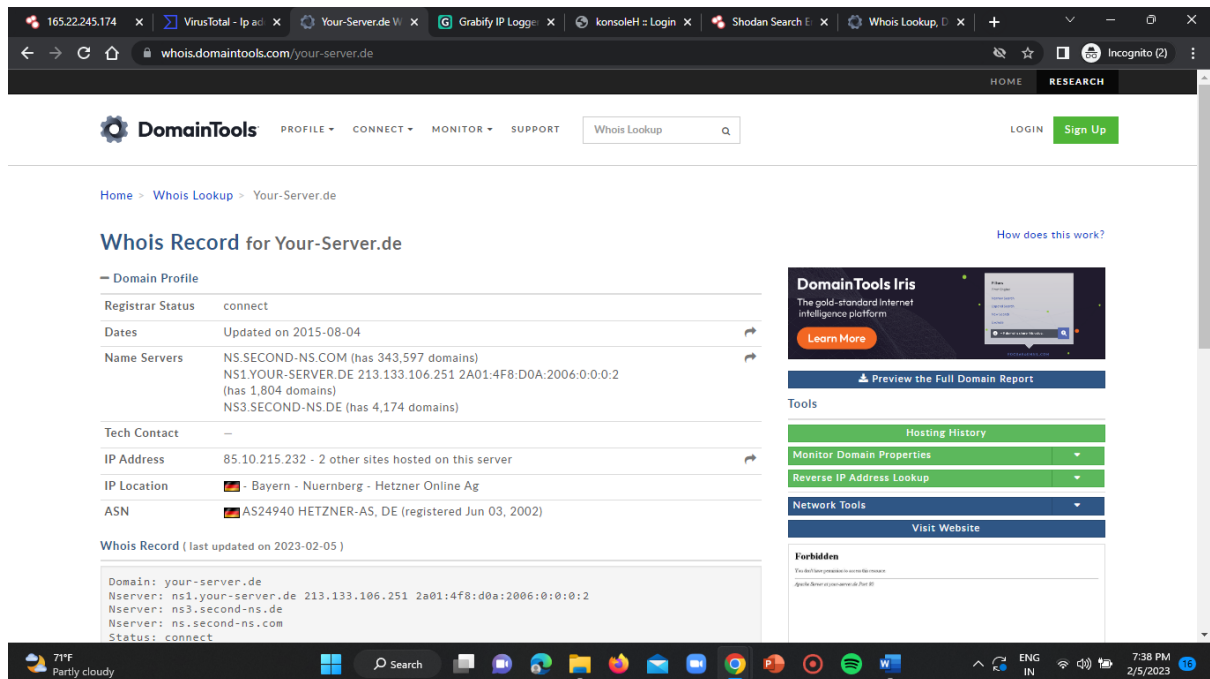
Domain Profile	
Registrant	Domain Administrator
Registrant Org	The Endurance International Group, Inc.
Registrant Country	us
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com IANA ID: 303 URL: <a href="http://www.publicdomainregistry.com">www.publicdomainregistry.com</a> Whois Server: <a href="http://whois.publicdomainregistry.com">whois.publicdomainregistry.com</a> abuse-contact: <a href="mailto:publicdomainregistry.com">publicdomainregistry.com</a> (p) 12013775952
Registrar Status	clientTransferProhibited
Dates	4,742 days old Created on 2010-02-11 Expires on 2027-02-11 Updated on 2022-03-17
Name Servers	ANDY.NS.CLOUDFLARE.COM (has 25,879,428 domains) DORA.NS.CLOUDFLARE.COM (has 25,879,428 domains)
Tech Contact	Domain Administrator

On the right side of the page, there is a "Tools" section with links for "Hosting History", "Monitor Domain Properties", and "Visit Website". Below this is a section for "Available TLDs" with tabs for "General TLDs" and "Country TLDs". The page also features a "DomainTools Iris" advertisement and a "Preview the Full Domain Report" button.



ST#IS#4899

## IP ADDRESS-2:- (188.40.28.165)



The screenshot shows the DomainTools website interface. The browser's address bar displays 'whois.domaintools.com/your-server.de'. The page title is 'Whois Record for your-server.de'. The 'Domain Profile' section contains the following information:

Domain Profile	
Registrar Status	connect
Dates	Updated on 2015-08-04
Name Servers	NS.SECOND-NS.COM (has 343,597 domains) NS1.YOUR-SERVER.DE 213.133.106.251 2A01:4F8:D0A:2006:0:0:0:2 (has 1,804 domains) NS3.SECOND-NS.DE (has 4,174 domains)
Tech Contact	—
IP Address	85.10.215.232 - 2 other sites hosted on this server
IP Location	Bayern - Nuernberg - Hetzner Online Ag
ASN	AS24940 HETZNER-AS, DE (registered Jun 03, 2002)

The 'Whois Record (last updated on 2023-02-05)' section shows the following raw whois data:

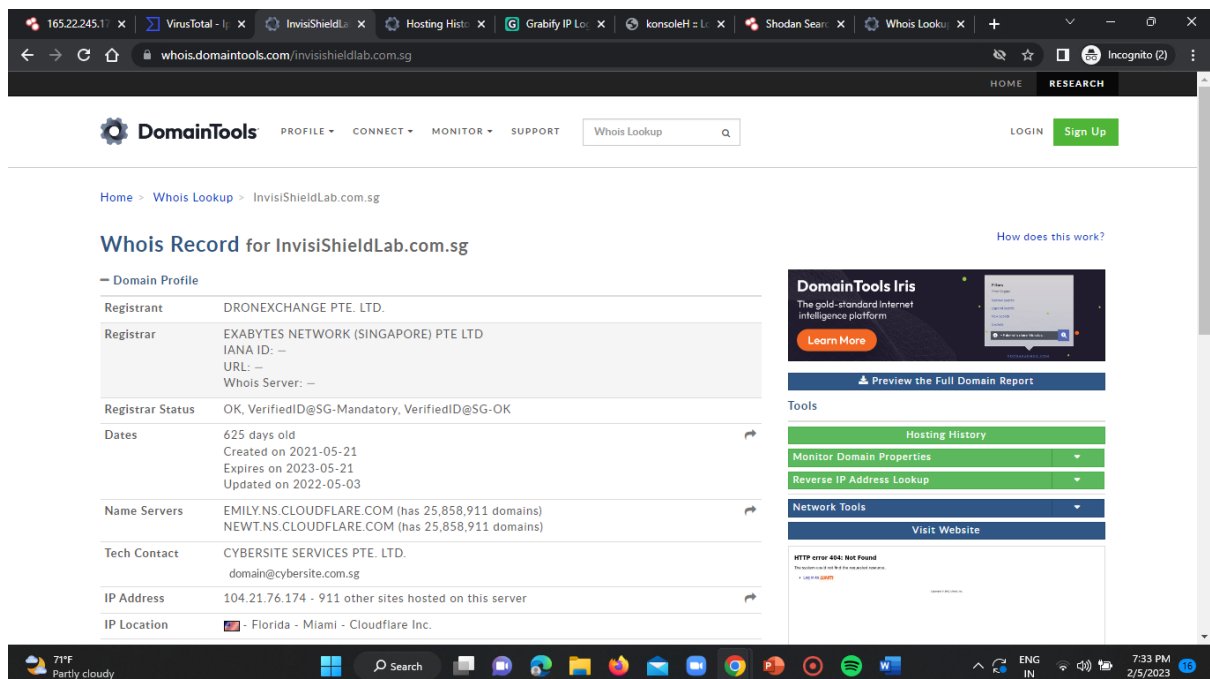
```
Domain: your-server.de
Nserver: ns1.your-server.de 213.133.106.251 2a01:4f8:d0a:2006:0:0:0:2
Nserver: ns3.second-ns.de
Nserver: ns.second-ns.com
Status: connect
```

On the right side, there is a 'DomainTools Iris' advertisement and a 'Tools' section with links to 'Hosting History', 'Monitor Domain Properties', 'Reverse IP Address Lookup', 'Network Tools', and 'Visit Website'. A 'Forbidden' message is also visible at the bottom right.

## IP ADDRESS-3:- (165.22.245.174)

Registrar = EXABYTES NETWORK (SINGAPORE) PTE LTD

Hosting organisation = DRONEXCHANGE PTE. LTD.



The screenshot shows the DomainTools website interface. The browser's address bar displays 'whois.domaintools.com/invisishieldlab.com.sg'. The page title is 'Whois Record for InvisiShieldLab.com.sg'. The 'Domain Profile' section contains the following information:

Domain Profile	
Registrant	DRONEXCHANGE PTE. LTD.
Registrar	EXABYTES NETWORK (SINGAPORE) PTE LTD IANA ID: — URL: — Whois Server: —
Registrar Status	OK, VerifiedID@SG-Mandatory, VerifiedID@SG-OK
Dates	625 days old Created on 2021-05-21 Expires on 2023-05-21 Updated on 2022-05-03
Name Servers	EMILY.NS.CLOUDFLARE.COM (has 25,858,911 domains) NEWT.NS.CLOUDFLARE.COM (has 25,858,911 domains)
Tech Contact	CYBERSITE SERVICES PTE. LTD. domain@cybersite.com.sg
IP Address	104.21.76.174 - 911 other sites hosted on this server
IP Location	Florida - Miami - Cloudflare Inc.

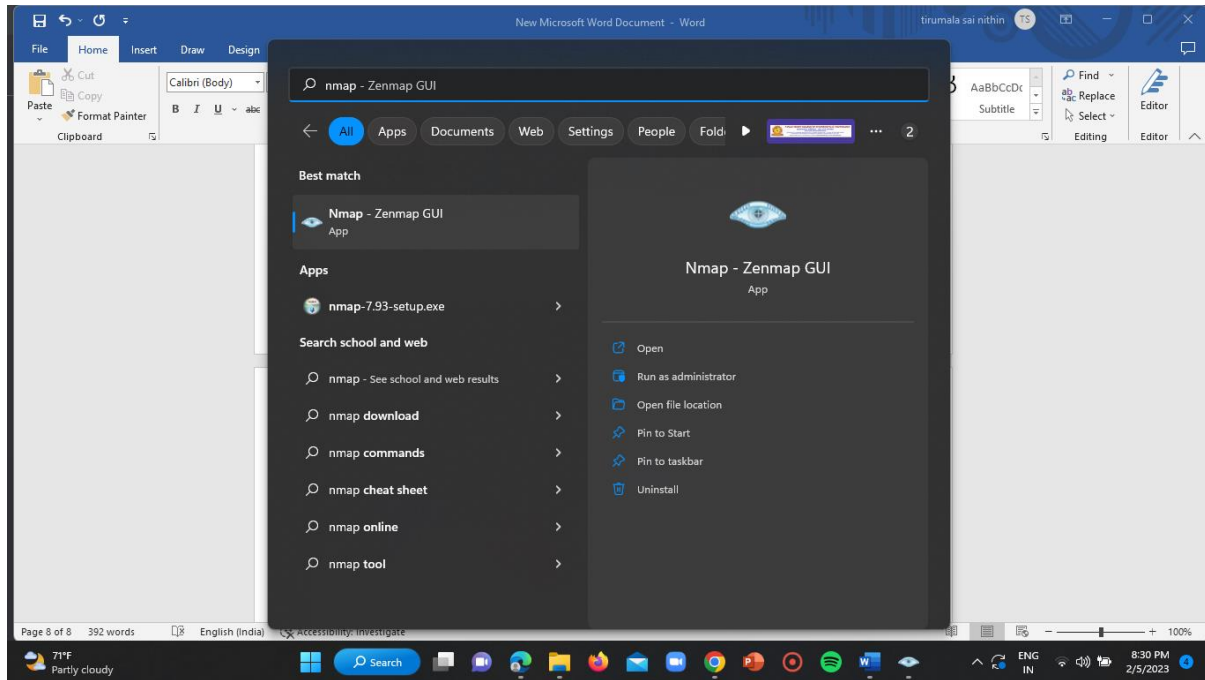
The 'Tools' section on the right includes links to 'Hosting History', 'Monitor Domain Properties', 'Reverse IP Address Lookup', 'Network Tools', and 'Visit Website'. An 'HTTP error 404: Not Found' message is displayed at the bottom right.

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

**TOOL USED:- “ NMAP-ZENMAP GUI ”**

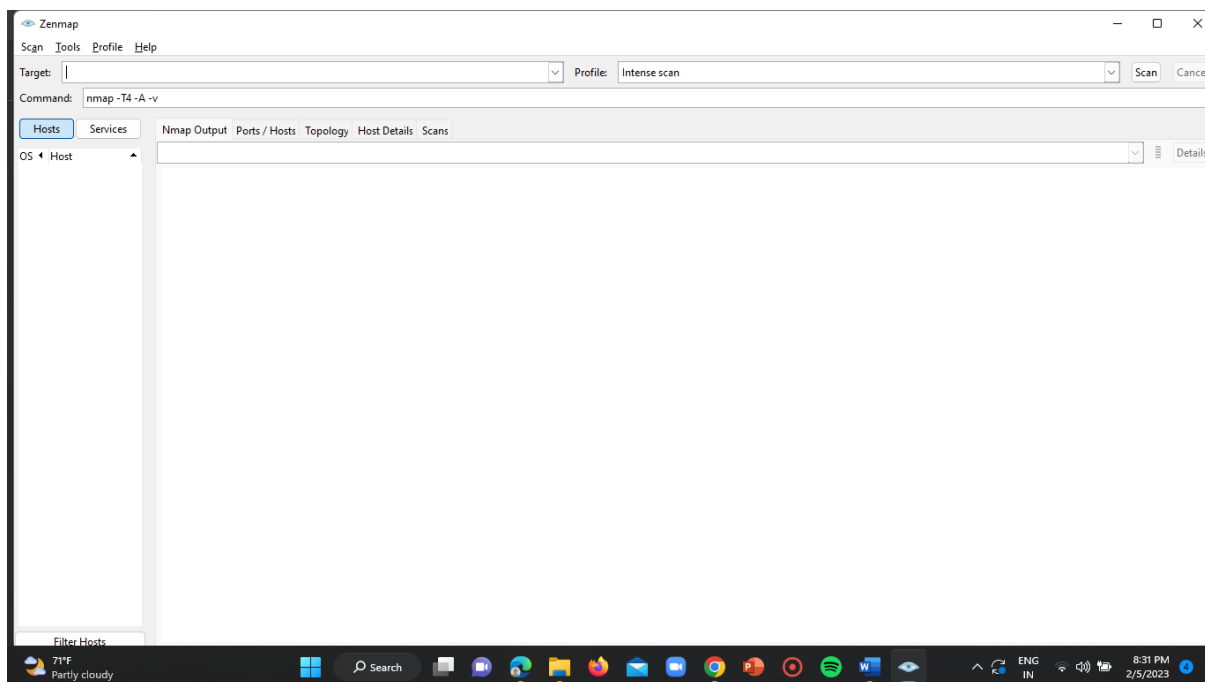
#### **Step-1:**

Click on start and search for “nmap” .



#### **Step-2:**

Open zenmap in administrator mode.

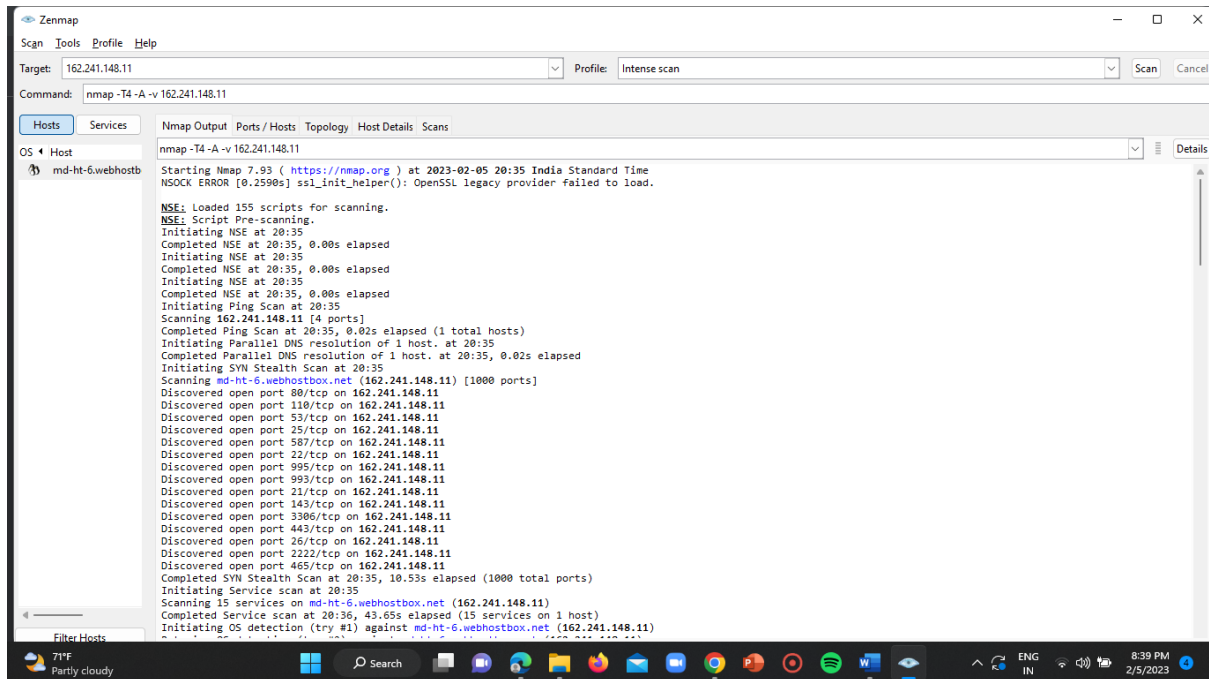




### Step-3:

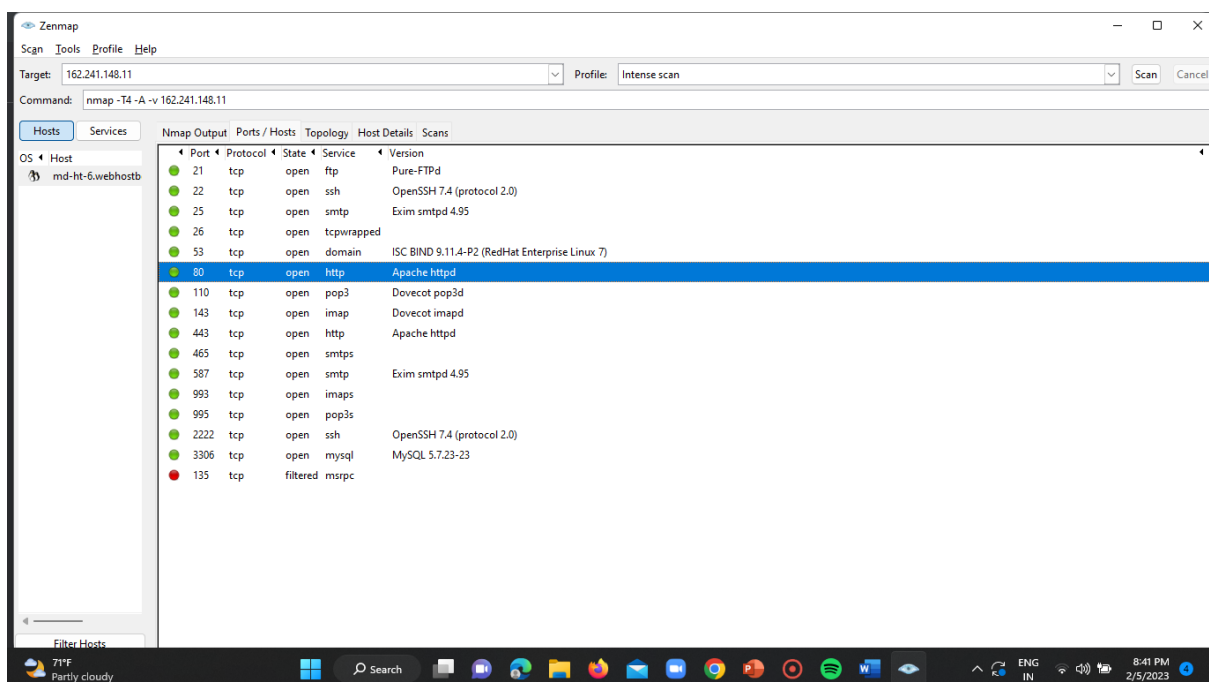
Enter the target IP address or domain name in the target input section of the nmap home page and select the option “intense scan” option in the profile section and then click on scan.

Wait until the scanning completes it may take sometime.



### Step-4:

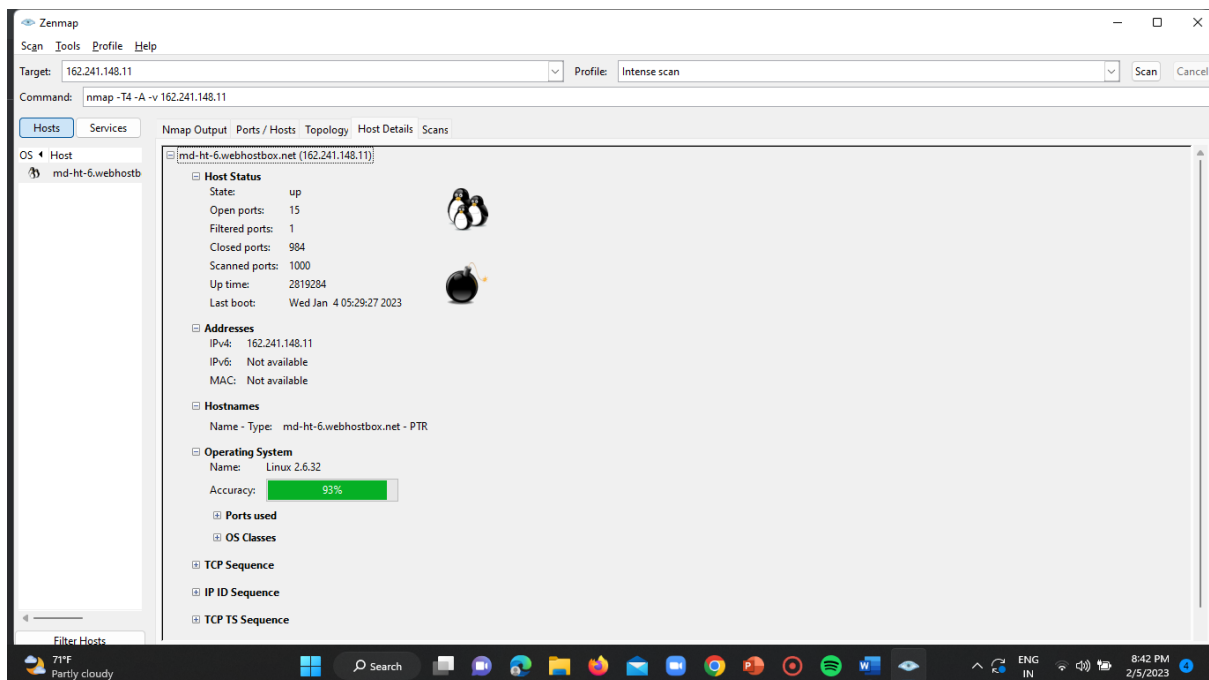
Visit hosts/ports section to find out the hosting web server.



ST#IS#4899

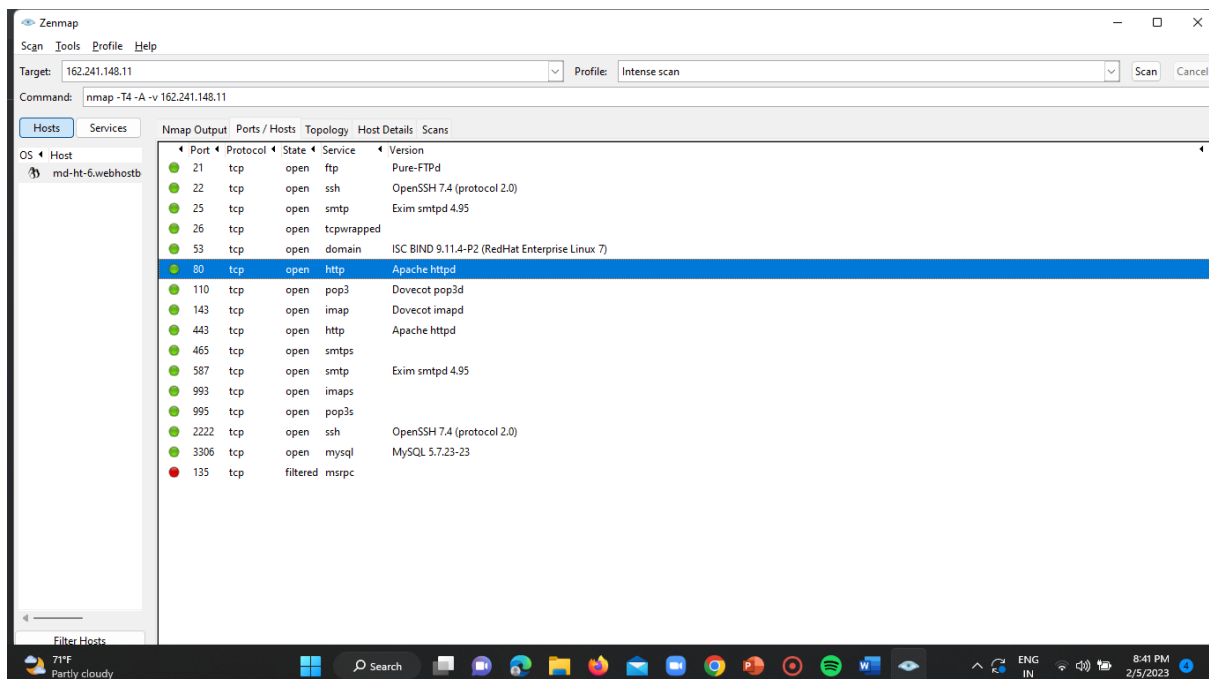
## Step-5:

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



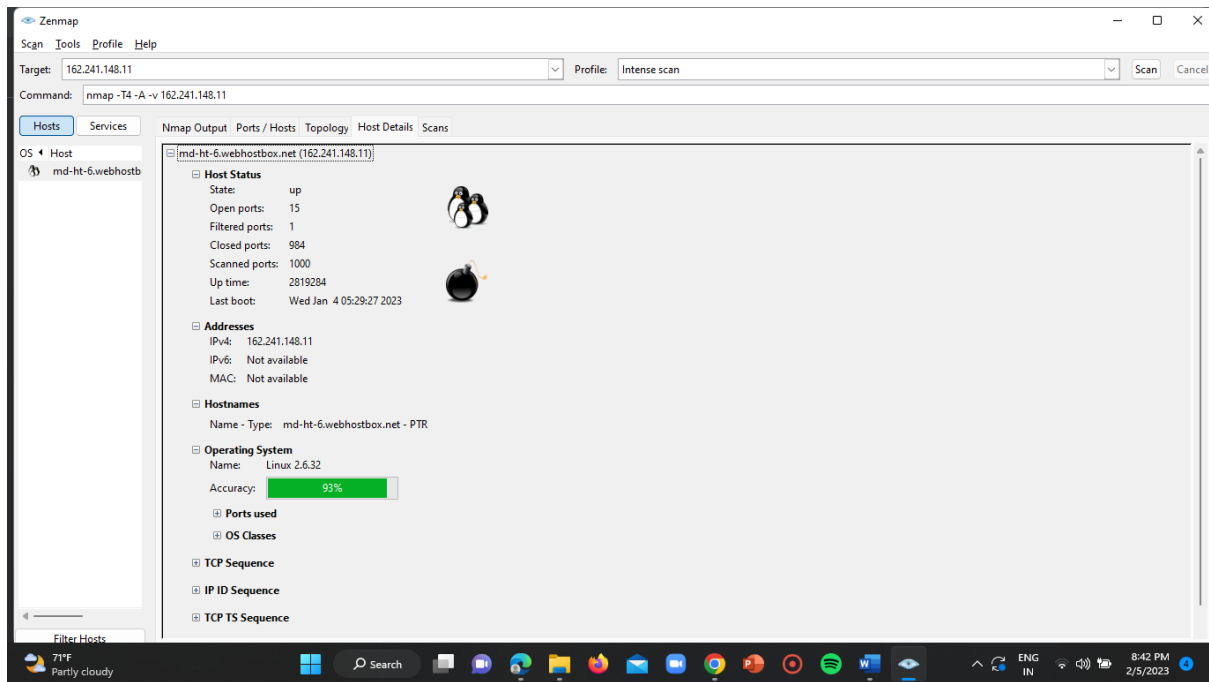
**IP ADDRESS-1:-** (162.241.148.11)

**Hosting web server =** Apache httpd



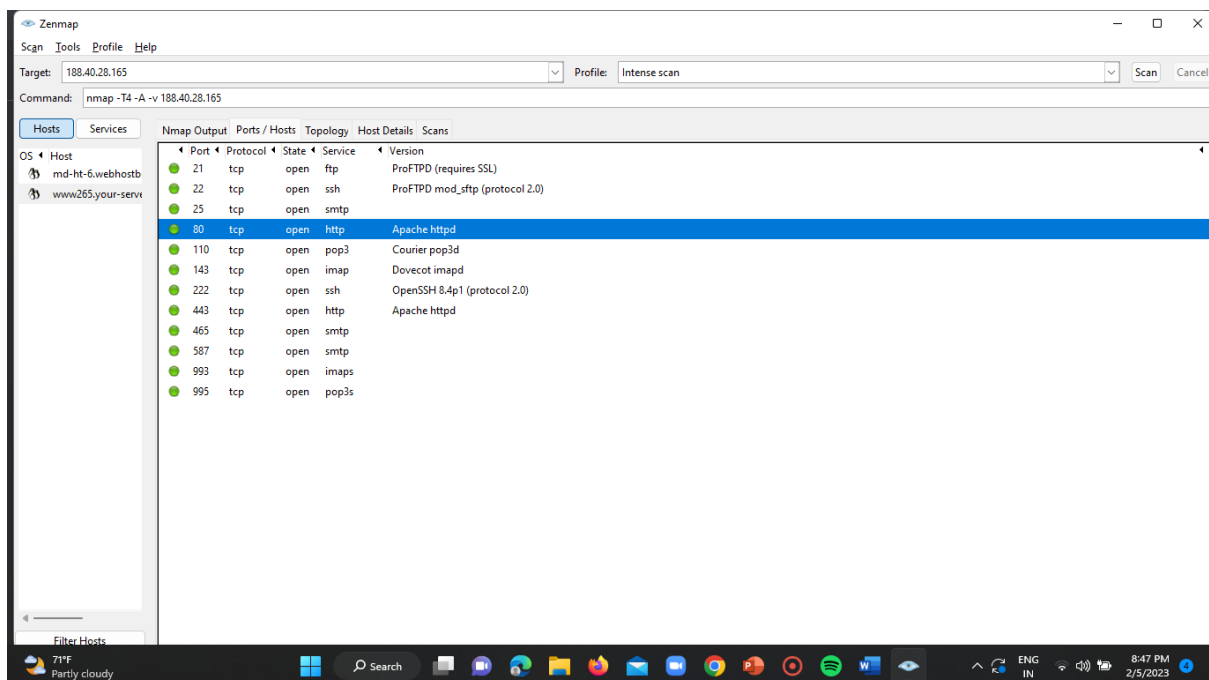
**Operating System =** Linux 2.6.32

ST#IS#4899



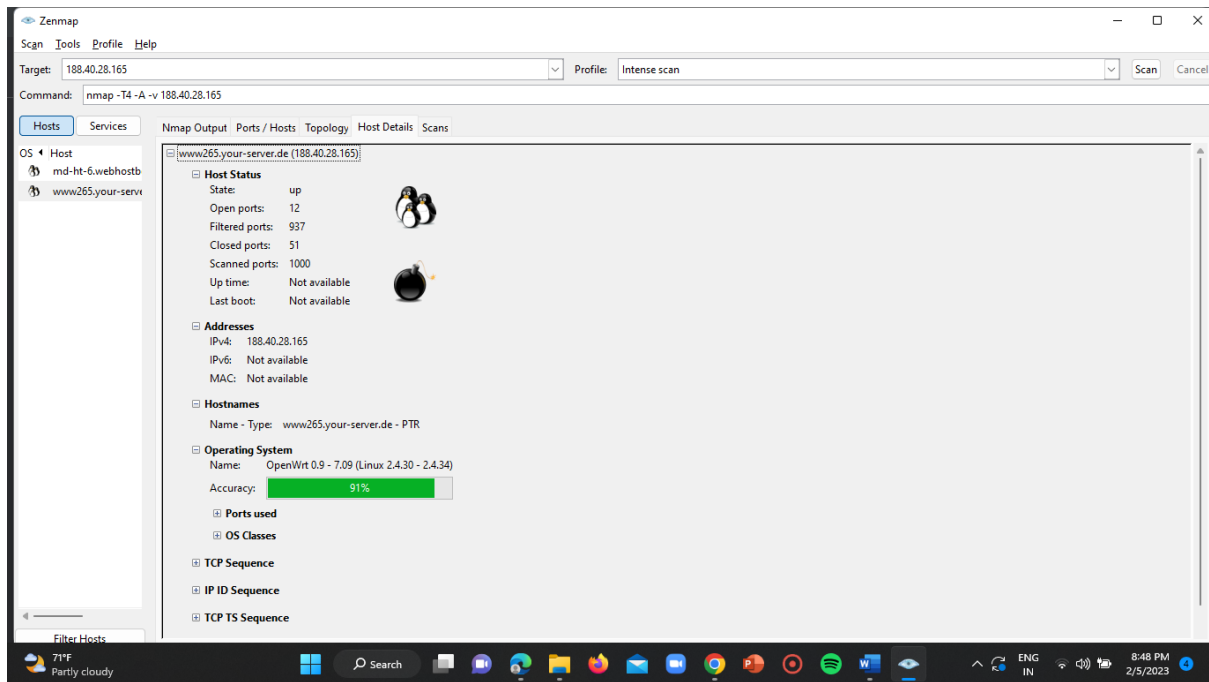
**IP ADDRESS-2:- (188.40.28.165)**

**Hosting web server = Apache httpd**



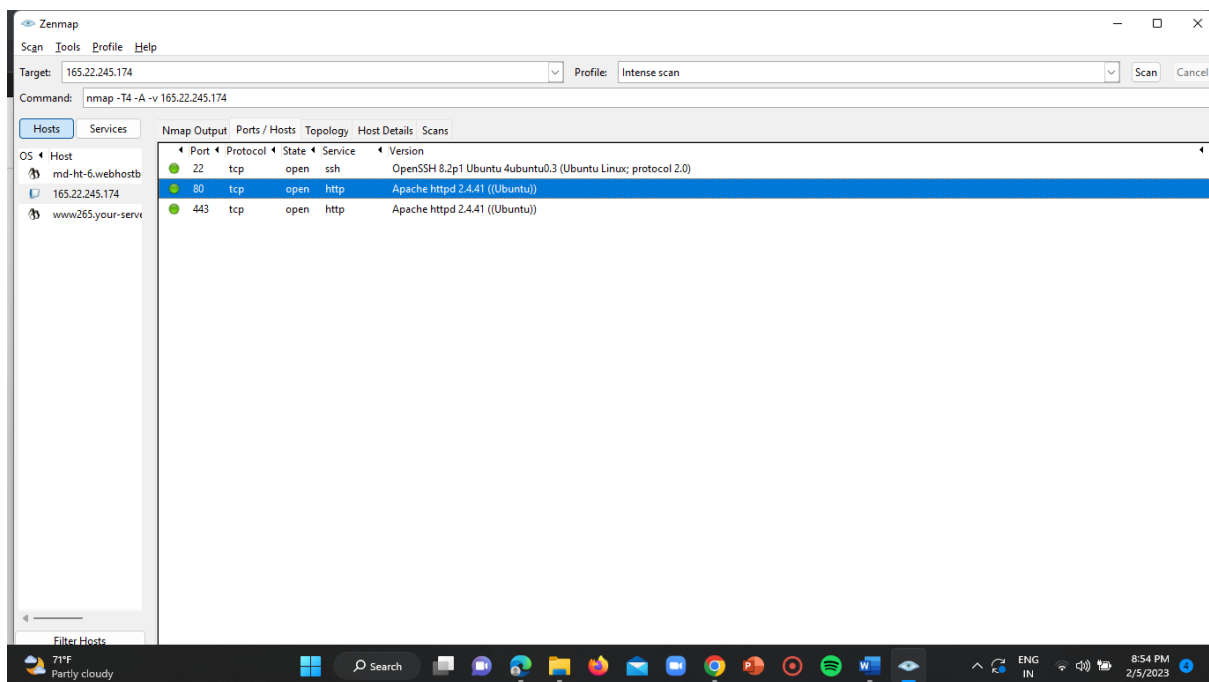
**Operating System = Linux (2.4.30 – 2.4.34)**

ST#IS#4899



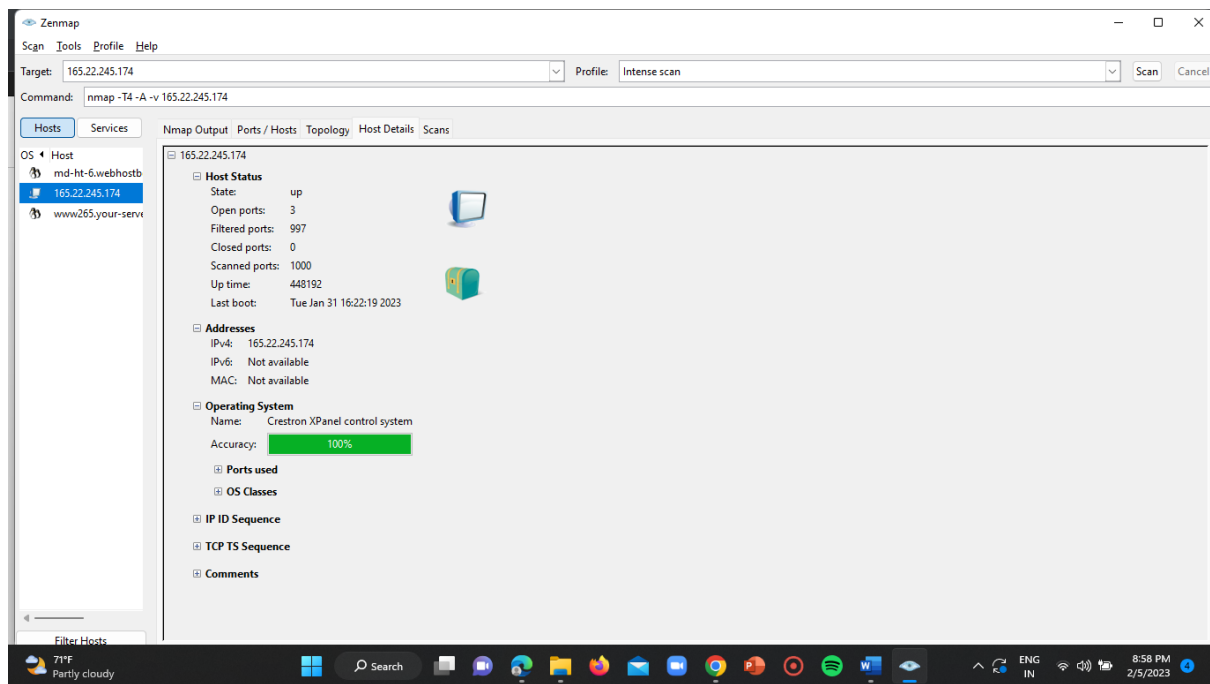
**IP ADDRESS-3:- (165.22.245.174)**

**Hosting web server = Apache httpd 2.4.41((Ubuntu))**



**Operating System = Creston XPanel control system**

ST#IS#4899



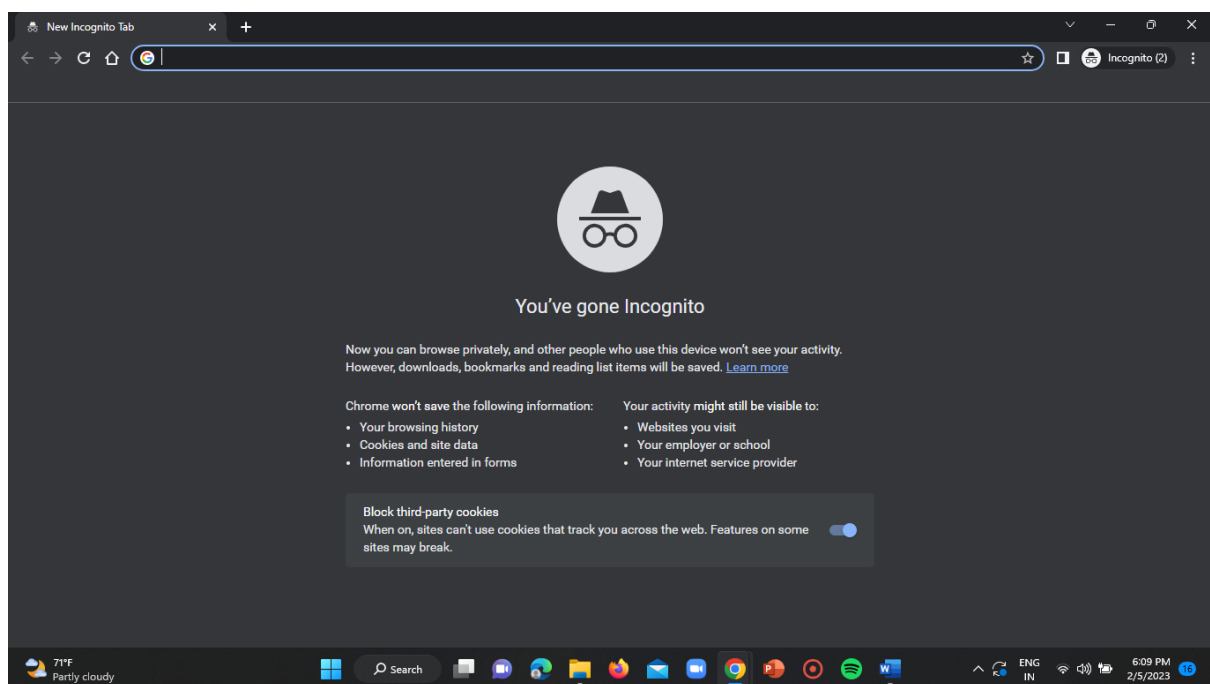
#### 4)CO-HOSTED WEBSITES:-

TOOL USED: “ VIRUSTOTAL ”

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

##### Step-1:

Open incognito tab in the google chrome.

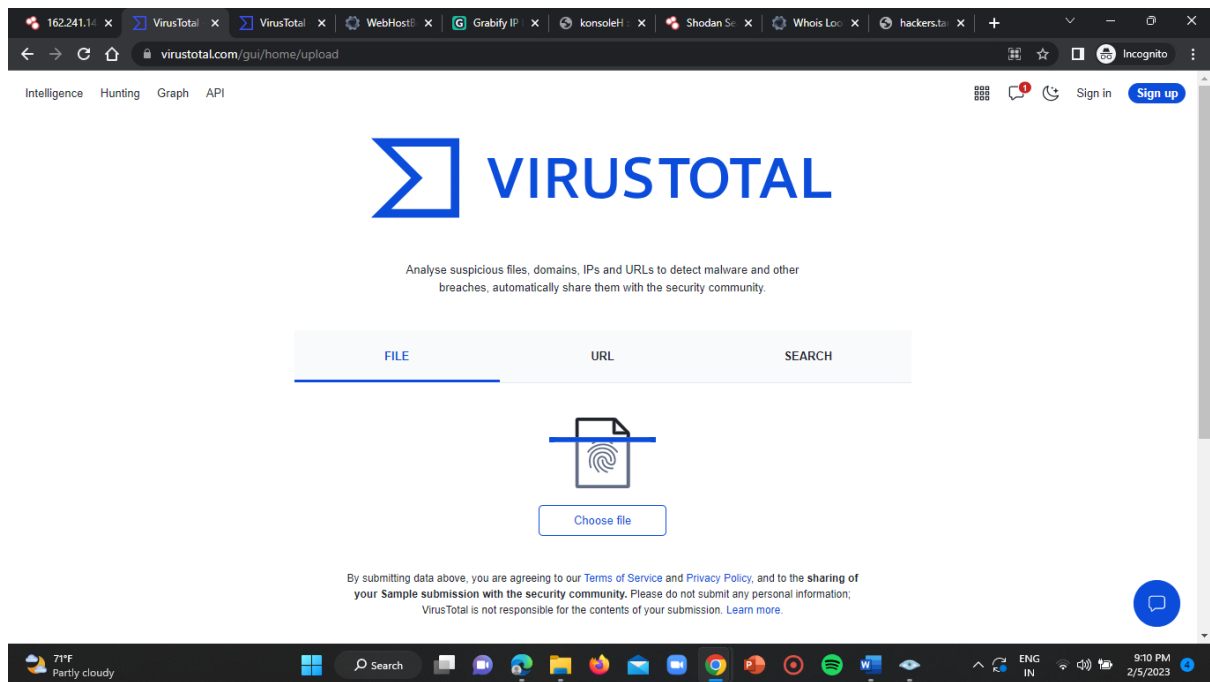


ST#IS#4899

## 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>

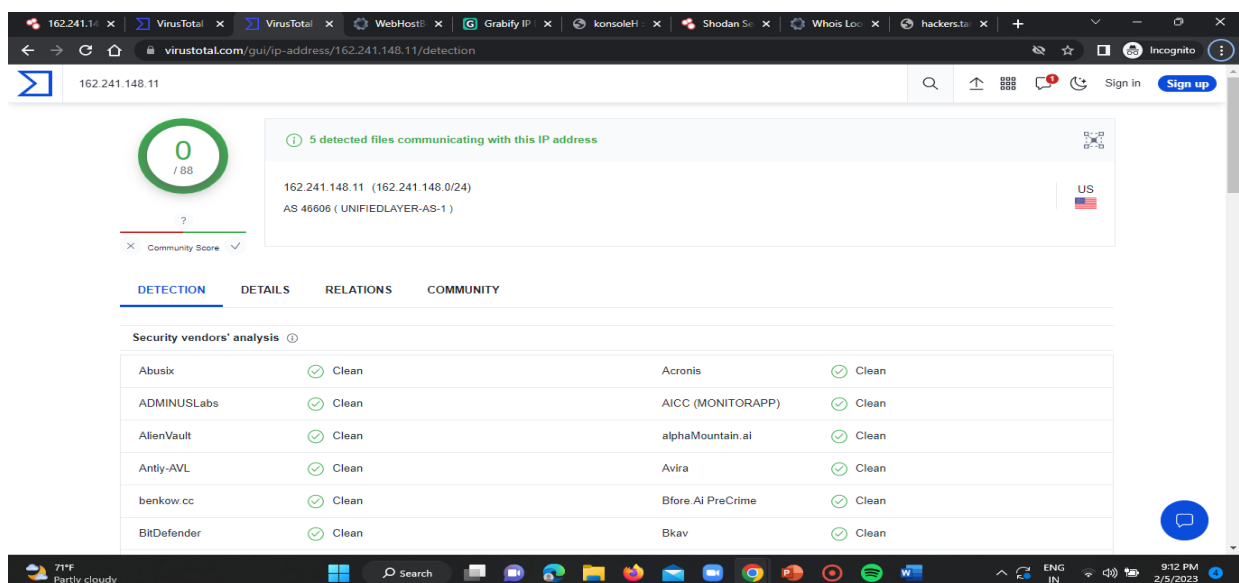


## Step-3:

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

Then click on enter.

The results get displayed as below.



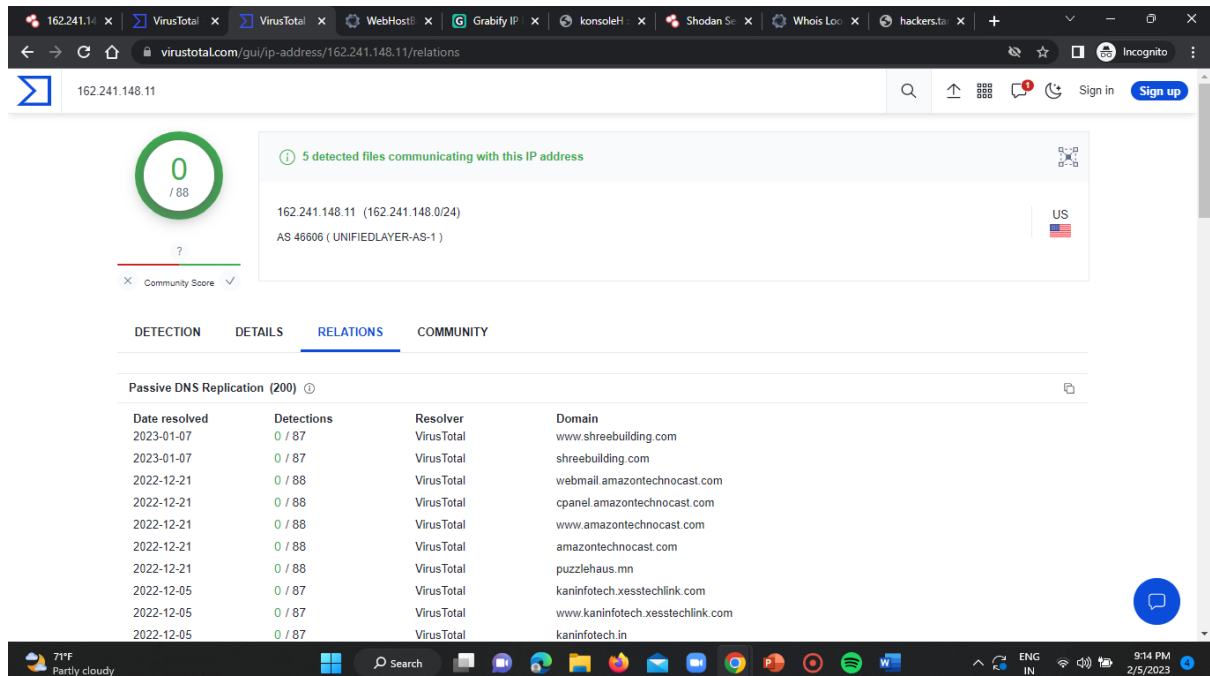


ST#IS#4899

## Step-5:

Click on “RELATIONS” section of the result page.

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



The screenshot shows the VirusTotal web interface for the IP address 162.241.148.11. The page is titled "162.241.148.11" and shows a "Community Score" of 0/88. A notification states "5 detected files communicating with this IP address". The "RELATIONS" tab is selected, displaying a table of "Passive DNS Replication (200)". The table lists the date resolved, detection status, resolver, and domain for various websites.

Date resolved	Detections	Resolver	Domain
2023-01-07	0 / 87	VirusTotal	www.shreebuilding.com
2023-01-07	0 / 87	VirusTotal	shreebuilding.com
2022-12-21	0 / 88	VirusTotal	webmail.amazontechnocast.com
2022-12-21	0 / 88	VirusTotal	cpanel.amazontechnocast.com
2022-12-21	0 / 88	VirusTotal	www.amazontechnocast.com
2022-12-21	0 / 88	VirusTotal	amazontechnocast.com
2022-12-21	0 / 88	VirusTotal	puzzlehaus.mn
2022-12-05	0 / 87	VirusTotal	kaninfotech.xesstechlink.com
2022-12-05	0 / 87	VirusTotal	www.kaninfotech.xesstechlink.com
2022-12-05	0 / 87	VirusTotal	kaninfotech.in

### 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

ST#IS#4899

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

The screenshot shows the VirusTotal website interface. At the top, there's a navigation bar with various tools like VirusTotal, WebHost, Graby IP, konsole, Shodan, Whois, and hackers. The main content area displays the IP address 162.241.148.11. A green circle with '0' indicates the number of detected files communicating with this IP address. Below this, a table shows the IP address and its location (US). The 'RELATIONS' tab is selected, showing a table of passive DNS replication data. The table has columns for Date resolved, Detections, Resolver, and Domain. The data shows various domains like www.shreebuilding.com, shreebuilding.com, webmail.amazontechnocast.com, cpanel.amazontechnocast.com, www.amazontechnocast.com, amazontechnocast.com, puzzlehaus.mn, kaninfotech.xesstechlink.com, and www.kaninfotech.xesstechlink.com. The bottom of the screen shows a Windows taskbar with various icons and the system clock.

Date resolved	Detections	Resolver	Domain
2023-01-07	0 / 87	VirusTotal	www.shreebuilding.com
2023-01-07	0 / 87	VirusTotal	shreebuilding.com
2022-12-21	0 / 88	VirusTotal	webmail.amazontechnocast.com
2022-12-21	0 / 88	VirusTotal	cpanel.amazontechnocast.com
2022-12-21	0 / 88	VirusTotal	www.amazontechnocast.com
2022-12-21	0 / 88	VirusTotal	amazontechnocast.com
2022-12-21	0 / 88	VirusTotal	puzzlehaus.mn
2022-12-05	0 / 87	VirusTotal	kaninfotech.xesstechlink.com
2022-12-05	0 / 87	VirusTotal	www.kaninfotech.xesstechlink.com
2022-12-05	0 / 87	VirusTotal	kaninfotech.in

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

**Co-hosted websites =**

tdh3d.com

tdh-3d.com

www.zweifreunde.tv

zweifreunde.tv

traumscape.com

ST#IS#4899

familiewolf.info

tolboothjazz.com

sachentag.de

hans-pausch.com

hanspausch.de

The screenshot shows the VirusTotal web interface in an Incognito browser window. The address bar displays the URL: `virustotal.com/gui/ip-address/188.40.28.165/relations`. The page header shows the IP address `188.40.28.165` with a green circle icon indicating a score of `0 / 87`. Below this, a green banner states: `4 detected files communicating with this IP address`. The IP details section shows `188.40.28.165 (188.40.0.0/16)` and `AS 24940 (Hetzner Online GmbH)` with a German flag icon. The main content area is divided into tabs: `DETECTION`, `DETAILS`, `RELATIONS` (selected), and `COMMUNITY`. Under the `RELATIONS` tab, there is a section titled `Passive DNS Replication (200)` with a table of data.

Date resolved	Detections	Resolver	Domain
2023-01-27	0 / 87	VirusTotal	tdh3d.com
2023-01-27	0 / 87	VirusTotal	tdh-3d.com
2023-01-12	0 / 88	VirusTotal	www.zweifreunde.tv
2023-01-12	0 / 88	VirusTotal	zweifreunde.tv
2022-12-15	0 / 88	VirusTotal	traumscape.com
2022-12-14	0 / 87	VirusTotal	familiewolf.info
2022-11-24	0 / 88	Georgia Institute of Technology	tolboothjazz.com
2022-11-19	0 / 87	VirusTotal	sachentag.de
2022-11-19	0 / 88	VirusTotal	hans-pausch.com
2022-11-18	0 / 88	VirusTotal	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

The screenshot shows the VirusTotal interface for the IP address 165.22.245.174. The security score is 0/87, indicating it is not flagged as malicious. The interface includes tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. The RELATIONS tab is active, showing a table of Passive DNS Replication and Historical Whois Lookups.

Date resolved	Detections	Resolver	Domain
2022-02-10	0 / 88	VirusTotal	invisishieldlab.com.sg
2021-07-13	0 / 88	VirusTotal	www.samruay.com
2021-07-13	0 / 88	VirusTotal	samruay.com
2021-07-13	0 / 87	VirusTotal	165-22-245-174.plesk.page
2021-07-13	0 / 88	VirusTotal	romantic-clark.165-22-245-174.plesk.page

Last Updated	Organization	Email
2021-11-10		

## **TASK OUTCOME:-**

This task is regarding about the footprinting technique used in both the hacking and the ethical hacking zones. Footprinting is the very 1<sup>st</sup> 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, CO-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