Name : Kunal jawale

Module 2

Footprinting / Information gathering

Footprinting : *footprinting refers to the process of gathering information about a target system.network or organization to identify potential vulnerabilities*. **types**: *passive footprinting or active footprinting*

. passive - ***a passive is the stealthier method since it will not trigger a target IDS or otherwise alert the target of information being gathered.***

.active – ***active footprinting can trigger a targets instrusion detection system (IDS) and may be loged.***

---------- Google hacking ----------

. **here are some types of google search techniques to gathering some information.**

- **Filetype:pdf** - to collect any type of information in pdf form
- **Filetype:xls** - collect information in EXCEL form
- **Intitle.index**. – its helps you to find specific keyword or phrase appears in the title tag of the webpage.
- **Inurl:** - allowing for more precise searches and targeted results.
- **Exploit-DB** – this is used for provide a comprehencive database of known vulnerabilities & their corresponding exploits.
- **SHODAN** - To identify exposed devices , services and potential weaknesses on the internet.

. Here are some Google hacks for Information Gathering:

- **Netcraft.com –** this site is help to find all information about the domain or target like networks, hosting country, IPv4 address,IPv6 ,domain ,organization ,location etc.

Name : Kunal jawale

Netcraft is a UK-based cybersecurity and internet services company that provides services for identifying, disrupting, and takedown cyberattacks. It offers various solutions, including threat intelligence, cybercrime detection, and online brand protection.

Here's a more detailed breakdown:

- **Threat Intelligence:**

  Netcraft collects and analyzes data on malicious websites, phishing scams, and malware, providing actionable insights to help organizations protect their users and networks.

- **Cybercrime Disruption:**

  They offer services to detect, disrupt, and take down online attacks, including phishing attacks, fake websites, and malware campaigns.

- **Brand Protection:**

  Netcraft helps businesses monitor for and disrupt websites impersonating their brand, protecting their reputation and customer safety.

- **Internet Data & Research:**

  They track websites, IP addresses, and other internet infrastructure data, providing insights into trends and patterns.

- **Free Tools:**

  Netcraft offers a free browser extension and app that provide real-time protection against malicious websites.

- **Global Reach:**

  Netcraft's threat intelligence data is used to protect billions of people globally, through partnerships with various organizations like browsers, antivirus companies, and internet infrastructure providers.

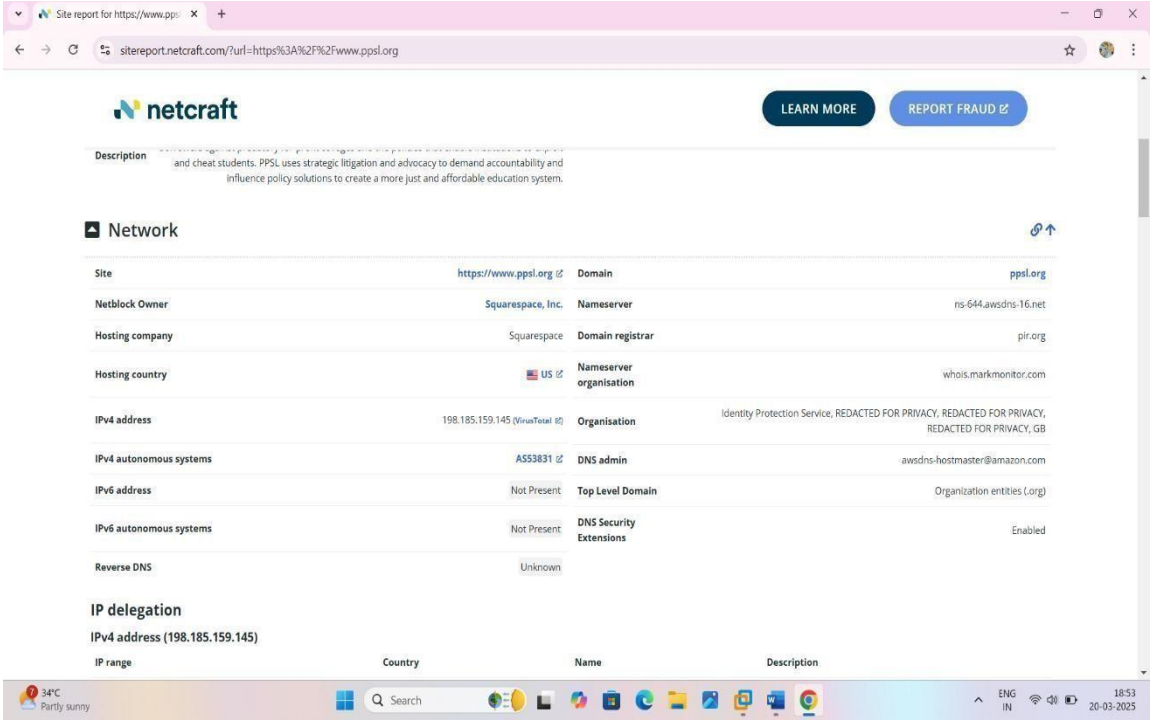
- **Transparency & Reporting:**

  Netcraft provides transparent reporting and analytics, allowing customers to track performance, monitor active takedown requests, and analyze trends.

- **Cybersecurity Solutions:**

  They offer a comprehensive platform for identifying and disrupting cyberattacks, including solutions for businesses, information security professionals, and other organizations. In essence, Netcraft is a cybersecurity firm that uses technology and data analysis to identify and disrupt online threats, protect brands, and provide actionable threat intelligence.

Name : Kunal jawale



- **DNSDumpster.com –** this website shows all information about the domain like email **subdomains,** host ,IP , ASN name ,open services and hosting networks location also.

DNSDumpster.com is a free, online tool that helps with DNS reconnaissance and research. It's essentially a domain research tool that can reveal information about a domain's structure, including subdomains, IP addresses, email servers, and more. This information is gathered by querying various publicly available DNS records and other data sources.

Here's a more detailed explanation:

- **DNS Reconnaissance:**

  DNSDumpster performs DNS reconnaissance, which is a process of collecting information about a domain's DNS records. This includes discovering hostnames, IP addresses, and other DNS record types.

- **Open Source Intelligence (OSINT):**

  It leverages open source intelligence (OSINT) resources to gather data, such as certificate transparency logs, web data repositories, and search engines.

- **Domain Profiling:**

  The tool profiles domain names and generates reports about related systems and publicly available information.

- **Information Gathering:**

Name : Kunal jawale

DNSDumpster collects various DNS and host data to help users understand a domain's digital footprint.

- **Attack Surface Identification:**

  It can help identify a domain's attack surface, which is the set of assets that can be targeted by an attacker.

- **Subdomain Discovery:**

  DNSDumpster can discover hidden subdomains that might not be immediately apparent.

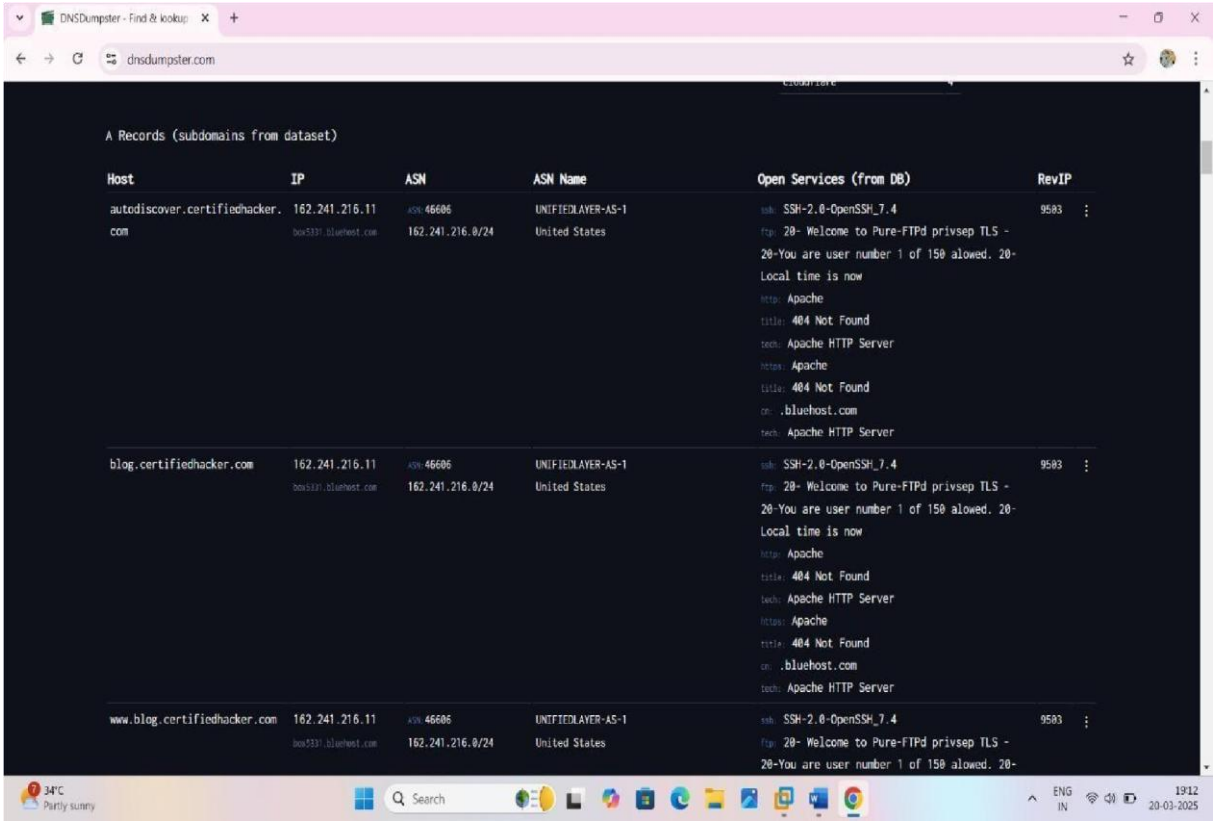
- **Web Host Discovery:**

  It also helps identify web hosts associated with a domain.

- **Free and Plus Options:**

  DNSDumpster offers both free and paid "Plus" options, with the "Plus" option providing access to more data and features.

- **Cybersecurity Use:**
  It's a valuable tool for cybersecurity professionals and anyone interested in network security and domain research.
  -



  - **Whois –** its show you all information about the domain or IP address ALL.

Name : Kunal jawale

A WHOIS website is a public directory where you can look up information about registered domain names, including the registrant's contact details, registration dates, and nameserver information. It essentially acts as a "phonebook" for the internet, allowing you to find out who owns a website and how to contact them.

Here's a more detailed explanation:

- **Public Database:**

  WHOIS is a public database maintained by the Internet Corporation for Assigned Names and Numbers (ICANN).

- **Domain Information:**

  It stores the information provided when a domain name is registered, including the registrant's name, address, email, phone number, and other technical details.

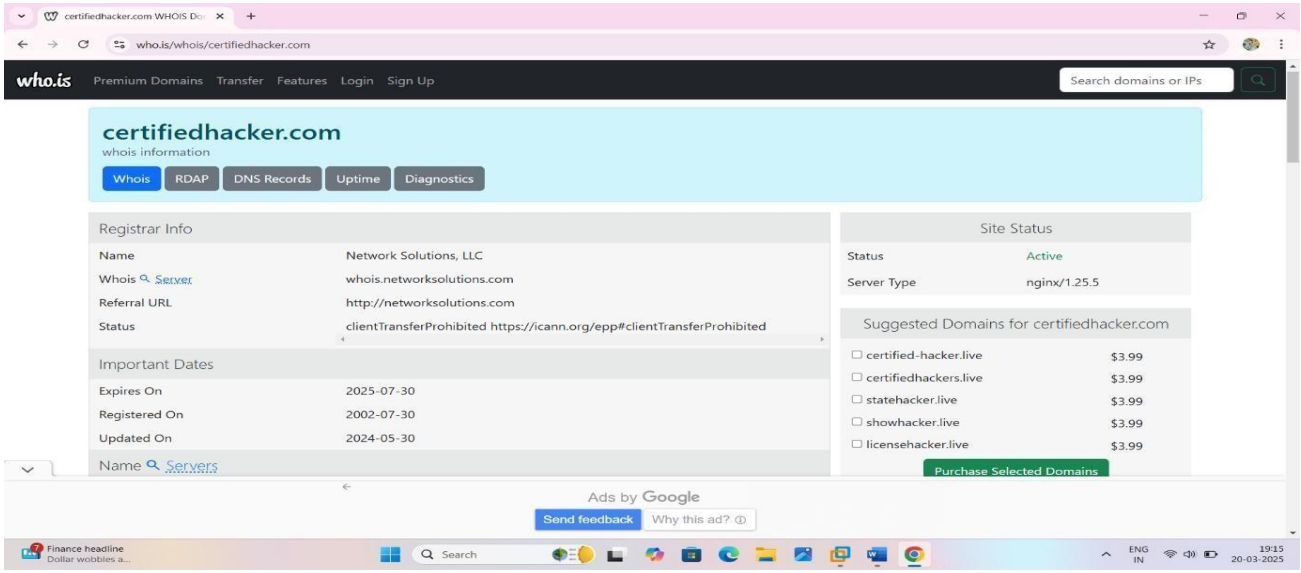
- **Lookup Functionality:**

  You can use a WHOIS lookup tool to search for a specific domain name and access its corresponding WHOIS information.

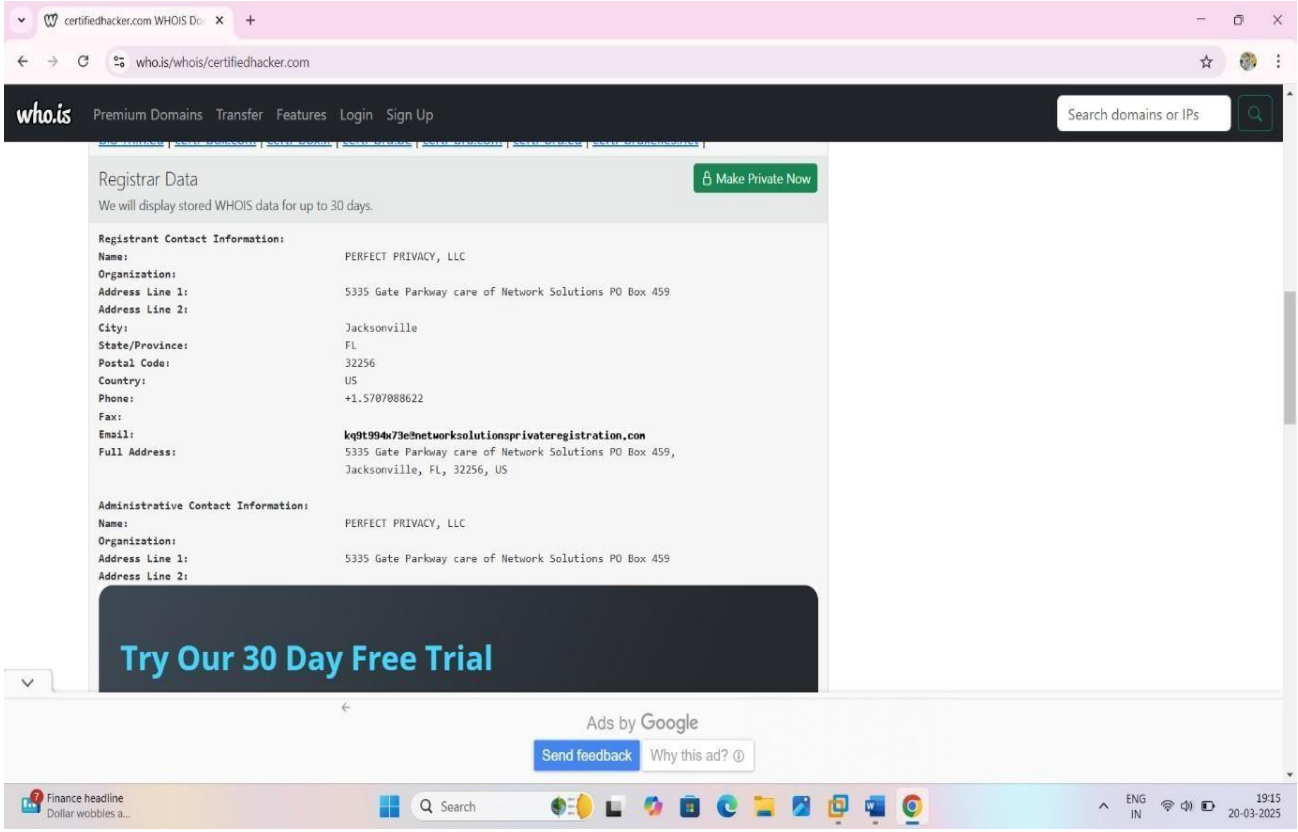
- **Various Uses:**

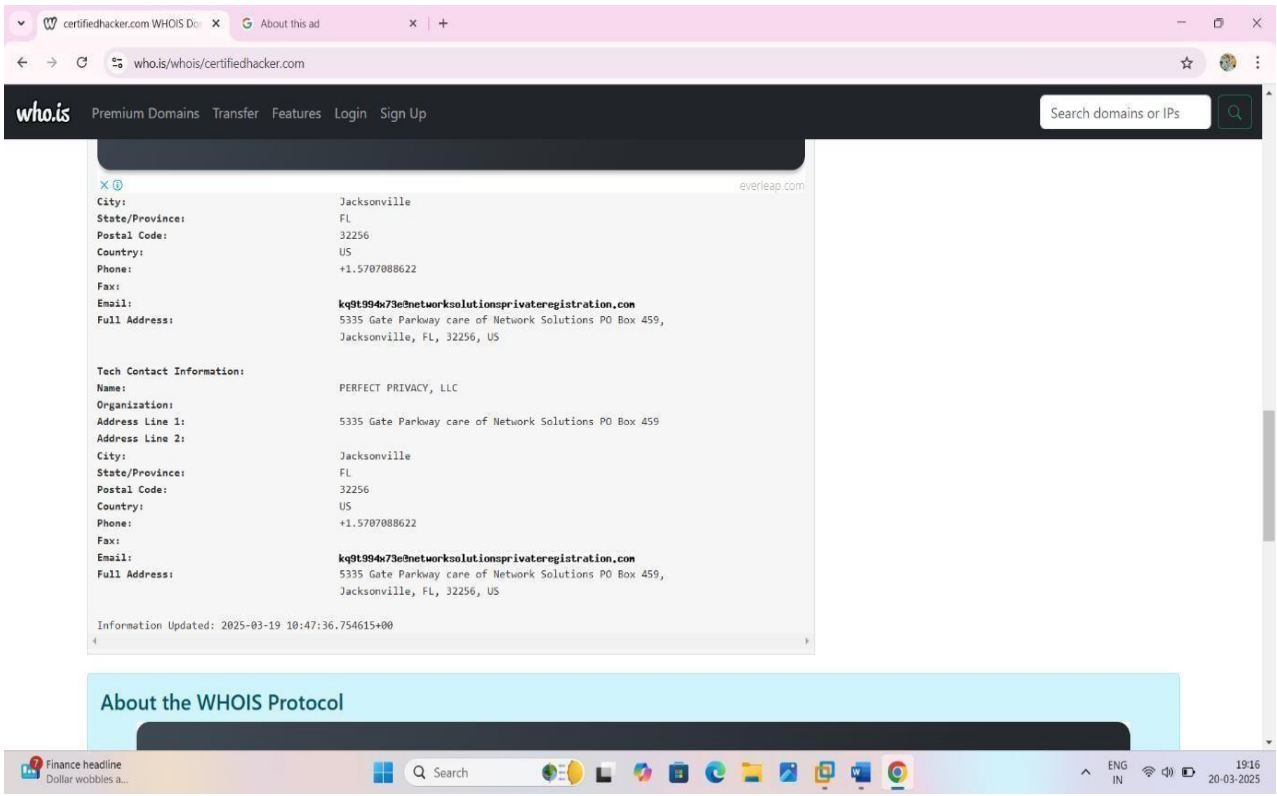
  WHOIS data is used for various purposes, including verifying domain ownership, contacting website owners, and investigating potential cyber threats.

- **Privacy Concerns:**
  While WHOIS provides valuable information, it's important to note that some registrants choose to use privacy protection services to mask their personal details from the public view.



Name : Kunal jawale





Name : Kunal jawale

- **OSINT framework –** OSINT framework has all types of searching tools and websites are available for all type of information gathering

An OSINT (Open Source Intelligence) framework is a structured methodology for gathering, analyzing, and utilizing information from publicly available sources. It helps security professionals and other researchers identify and understand potential threats by leveraging tools and techniques to collect, process, and interpret data from various online sources. Key aspects of an OSINT framework:

- **Data Collection:**

  OSINT frameworks guide the process of gathering information from various public sources, such as social media, news articles, government databases, and more.

- **Organization and Categorization:**

  The framework helps organize collected data by type, source, and context, making it easier to analyze and draw conclusions.

- **Analysis and Interpretation:**

  OSINT frameworks provide methods for analyzing the collected data, identifying patterns, and making inferences about potential threats or adversaries.

- **Ethical Considerations:**

  A good OSINT framework also includes guidelines on ethical considerations, such as privacy, data protection, and legal compliance. Examples of OSINT frameworks and tools:

- **OSINT Framework:**

  A comprehensive directory of OSINT resources, organized by category and type.

- Recorded Future's Threat Intelligence platform:

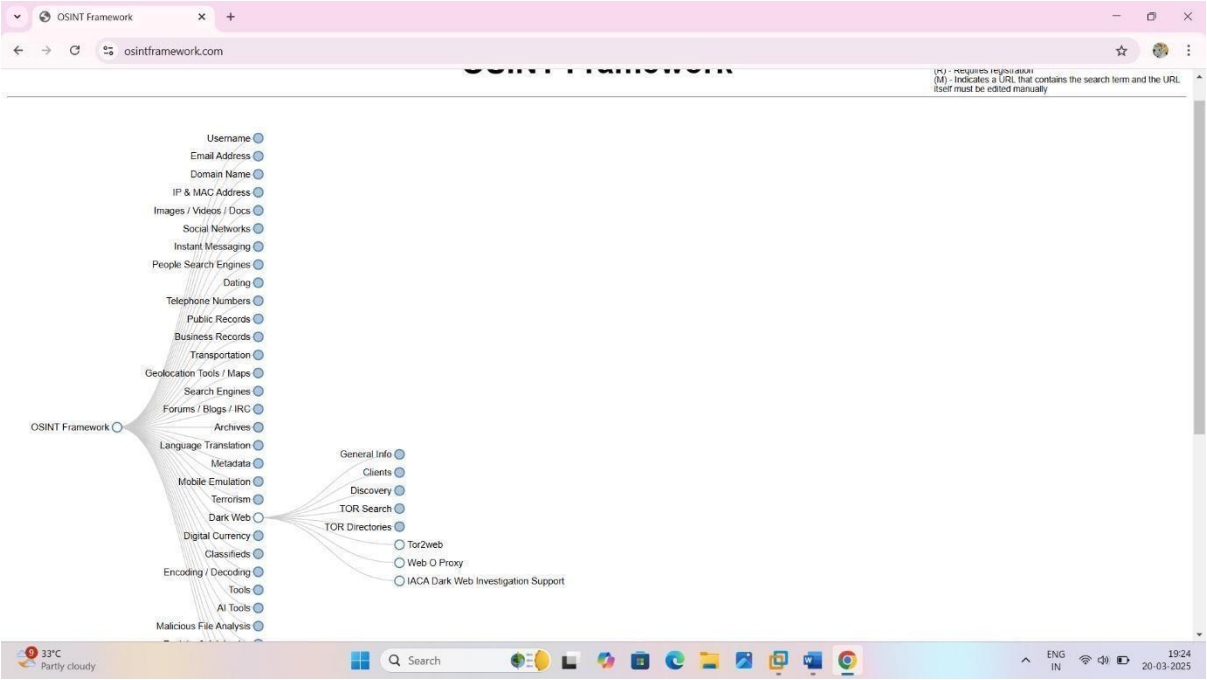
  Provides tools for collecting and analyzing data from various open-source sources.

- **CrowdStrike's OSINT methodology:**

  Integrates data, processes, methods, and tools to help security teams identify and understand threats.

Name : Kunal jawale

OSINT frameworks are valuable tools for both defensive and offensive security strategies, enabling professionals to gather intelligence, identify vulnerabilities, and respond to threats more effectively.



- **emkei.cz –** <u>this tool is very useful to sent fake mail using any mail id.</u> Here is the page :

"Emkei.cz" is the domain name of a website that's been flagged in a report about email spoofing, suggesting it may have been involved in sending fraudulent emails. While not much other information about the specific website is readily available, the report indicates it was used to send emails that appeared to originate from other sources, according to HackerOne. This type of email spoofing can be used for malicious purposes like phishing or spreading malware. Elaboration:

- **Email Spoofing:**

  Spoofing involves forging the sender's email address in a message, making it appear as if the email originated from a different source than it actually did.

- **Emkei.cz in the Report:**

  The report details a case where an email spoofing attack was traced to the domain "emkei.cz".

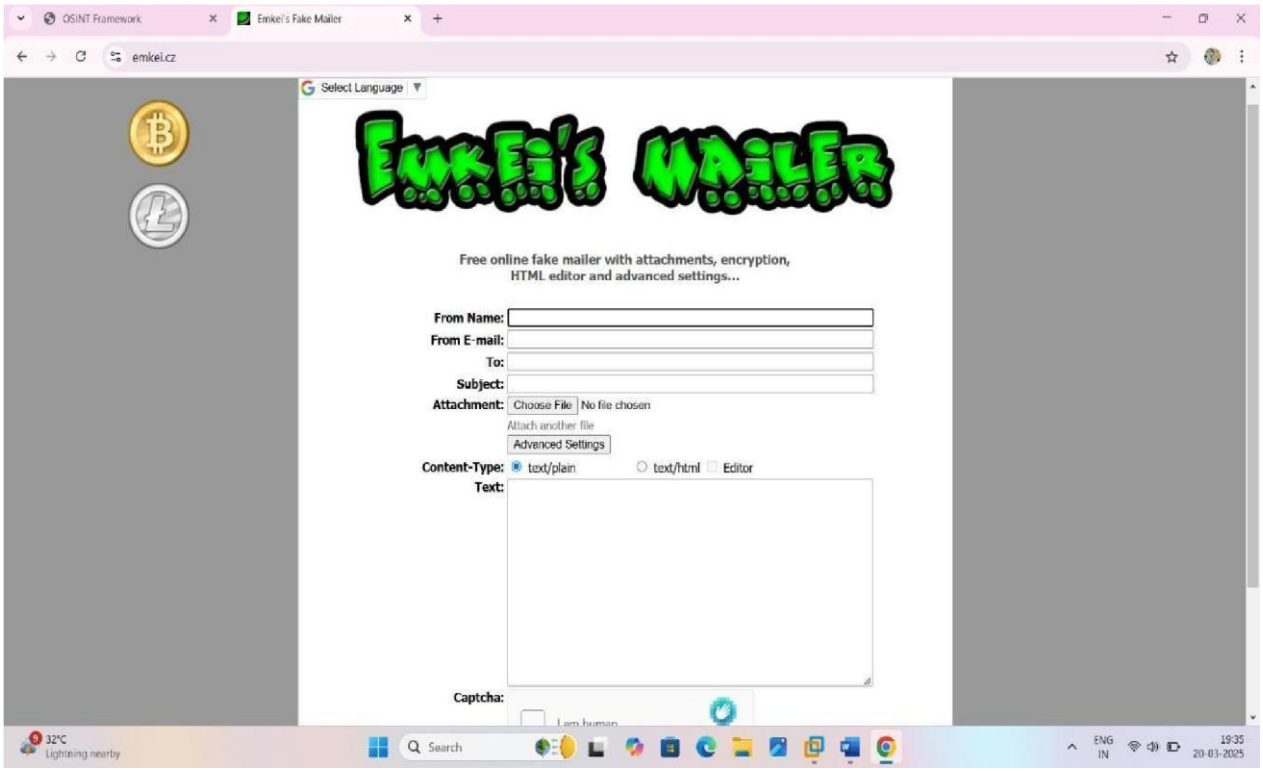
- **Malicious Intent:**

Name : Kunal jawale

This type of email spoofing can be used for various malicious purposes, including:

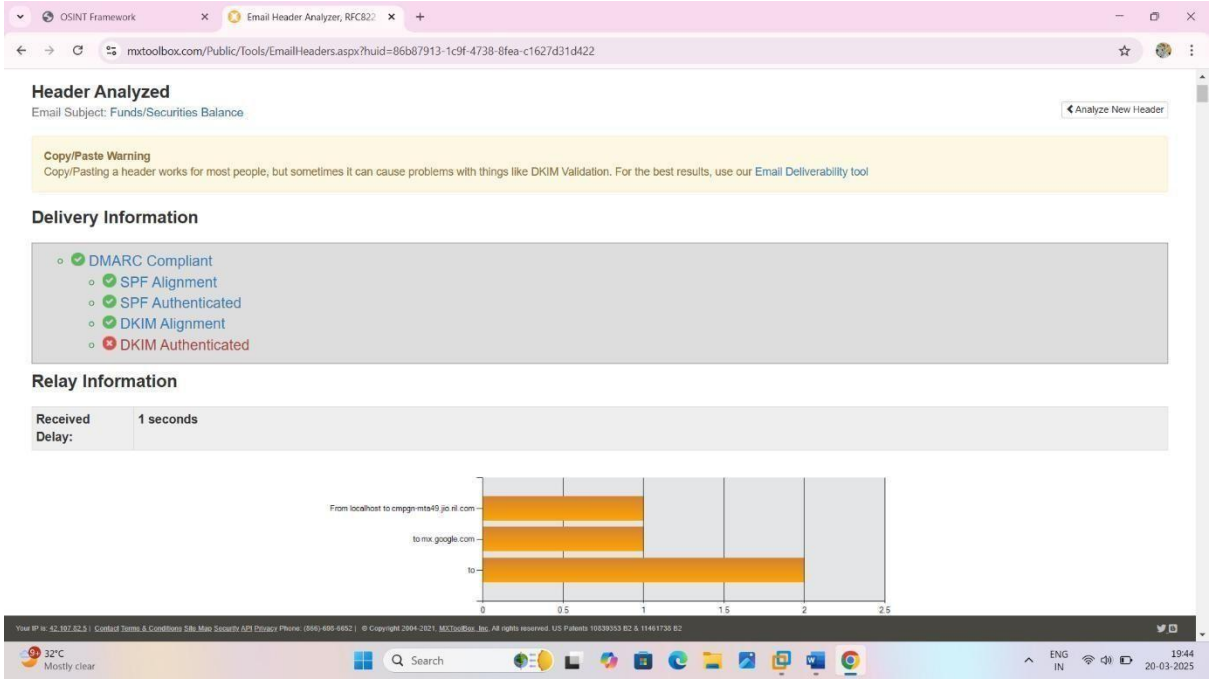
- **Phishing:** Deceiving users into providing sensitive information like usernames, passwords, or financial details.
- **Malware Distribution:** Sending infected email attachments or links that, when clicked, install malware on the recipient's device.
- **Identifying Spoofed Emails:**

  While the sender address can be forged, the IP address of the sending computer is usually revealed in the email header, which can help in identifying the source of the spoofed message.
- **"Received:" Lines:**
  The "Received:" lines in an email header provide information about the servers and IP addresses through which the email passed during transmission, helping to trace its origin.

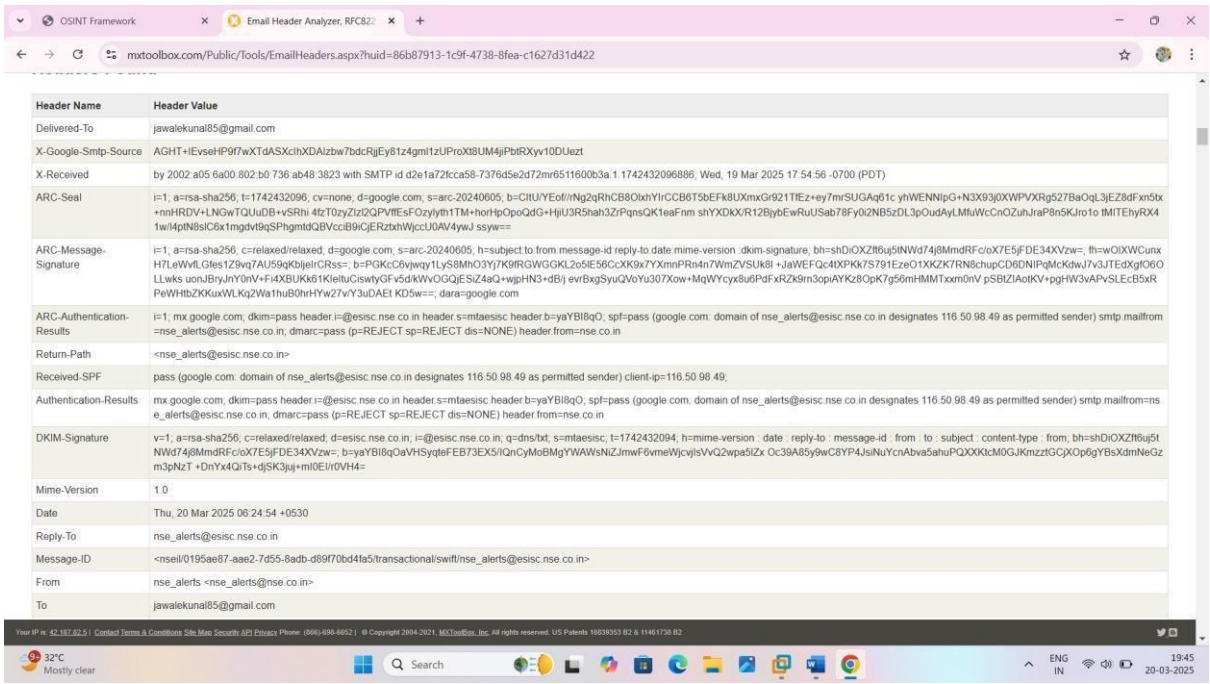


- **MxToolbox.com –** this website is usually used for check mail is fake or not using header Analyzer . just go to Gmail tap the three icon and choose the (show original option) and then copy the clipboard and paste it . then see mail is fake or real and all the information about the mail like this :

Name : Kunal jawale



See the mail I received is the original one..



This is the header information about the mail.

KLOTH.NET – KLOTH.NET is a website that provides a variety of tools and information related to internet communications, especially focusing on radio and network technologies. It offers services like DNS lookup, WHOIS, and tools for testing and understanding internet protocols. The site also includes information

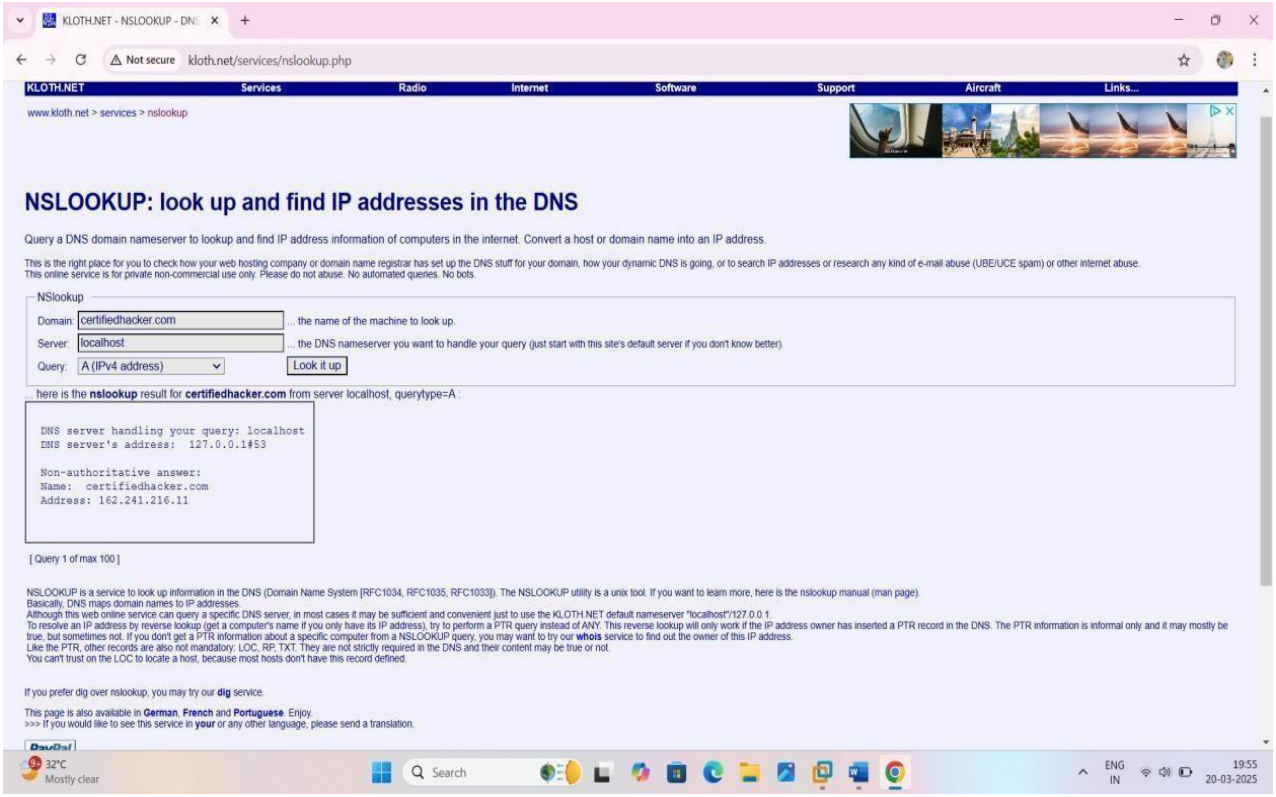
Name : Kunal jawale

about radio communications, including aeronautical and maritime radio, and offers tools for DNS analysis and troubleshooting.
Here's a more detailed breakdown of what you can find on KLOTH.NET:

Internet Tools and Services:

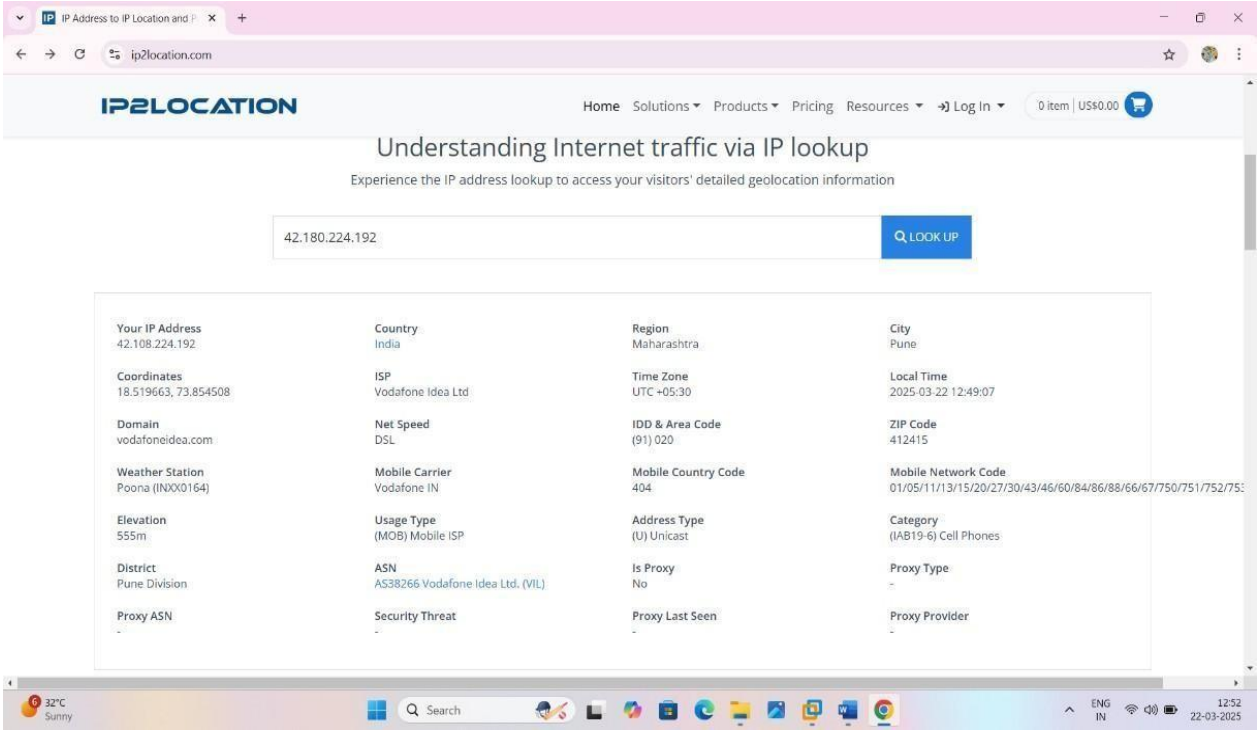
- **DNS Lookup (dig, nslookup):** Provides tools to query domain name servers and find the IP addresses of websites.
- **WHOIS:** Allows you to look up domain registration information.
- **IP Locate:** Provides tools to translate IP addresses, reverse lookups (PTR records), and location information based on IP addresses.
- **Ping, Traceroute:** Tools for testing network connectivity and tracing the path of packets.
- **Server Information:** Tools to retrieve HTTP headers and other server information.
- **DNSBL Check:** A tool to check if an IP address is listed on various DNS blacklist servers.

- this website is lookup and find IP addresses in the DNS using domain name :



- **IP2LOCATION -** This website show you the location of the target IP address, only you just type target IP address and press Enter :

Name : Kunal jawale



IPVOID.COM – IPVoid is an online tool that helps users analyze the reputation and security of IP addresses and domains. It offers various tools and services to gather information, including checking for malicious activity, identifying proxies and Tor addresses, and retrieving geolocation data. Here's a more detailed explanation:

- **IP Reputation Analysis:**

  IPVoid uses data from various blacklists and reputation services to assess the reputation of an IP address. This can help identify IPs associated with spam, malware, or other malicious activities.

- **Domain Reputation Analysis:**

  Beyond IP addresses, IPVoid can also analyze domain reputations. This can be useful for identifying potentially phishing or malicious websites.

- **Geolocation and ISP Information:**

  IPVoid can provide information about the geographic location and Internet Service Provider (ISP) associated with an IP address.

- **Proxy and Tor Detection:**

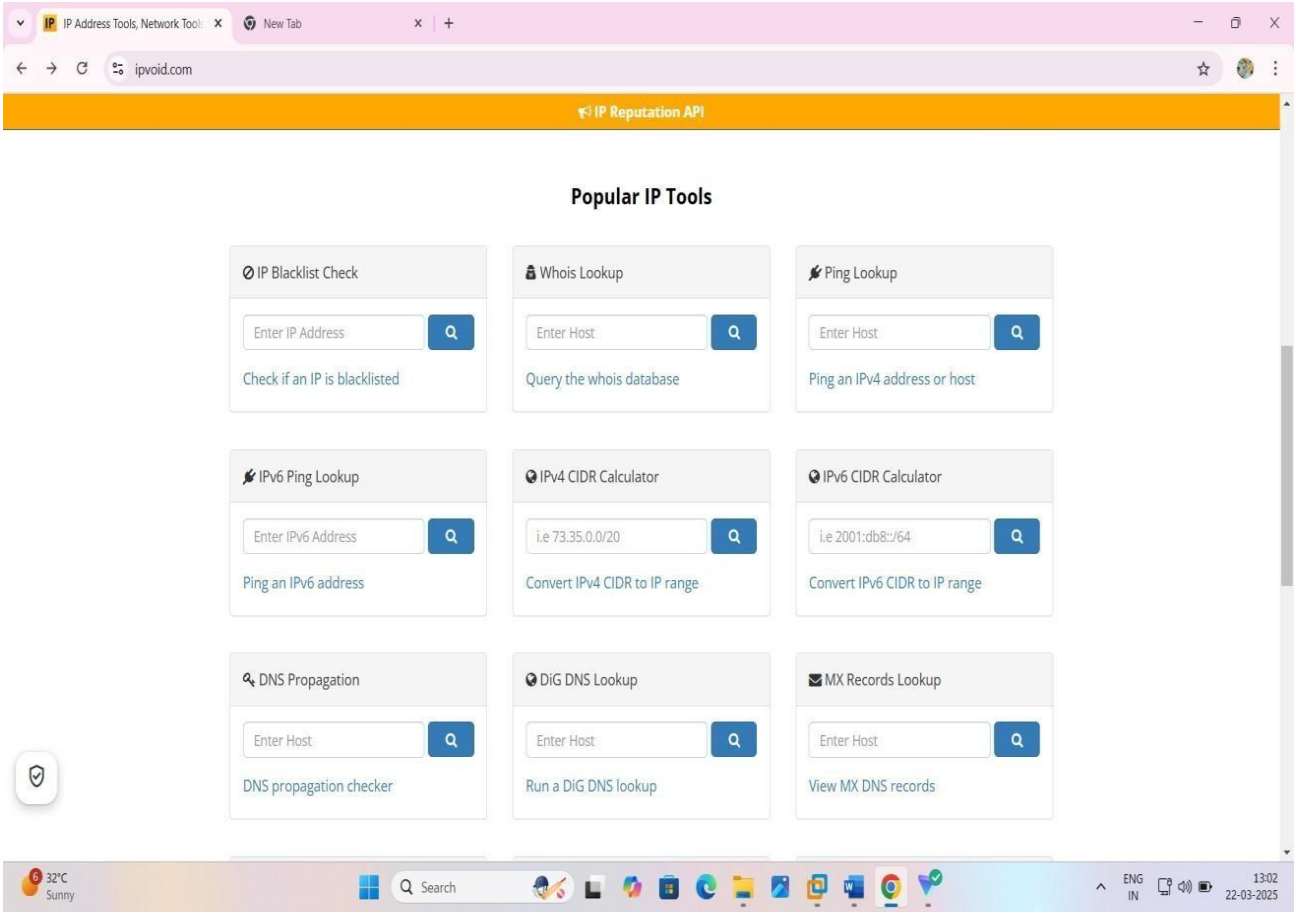
  The tool can also detect if an IP address is associated with a proxy or Tor network, which are often used for anonymous browsing and can be associated with malicious activities.

- **Threat Intelligence APIs:**

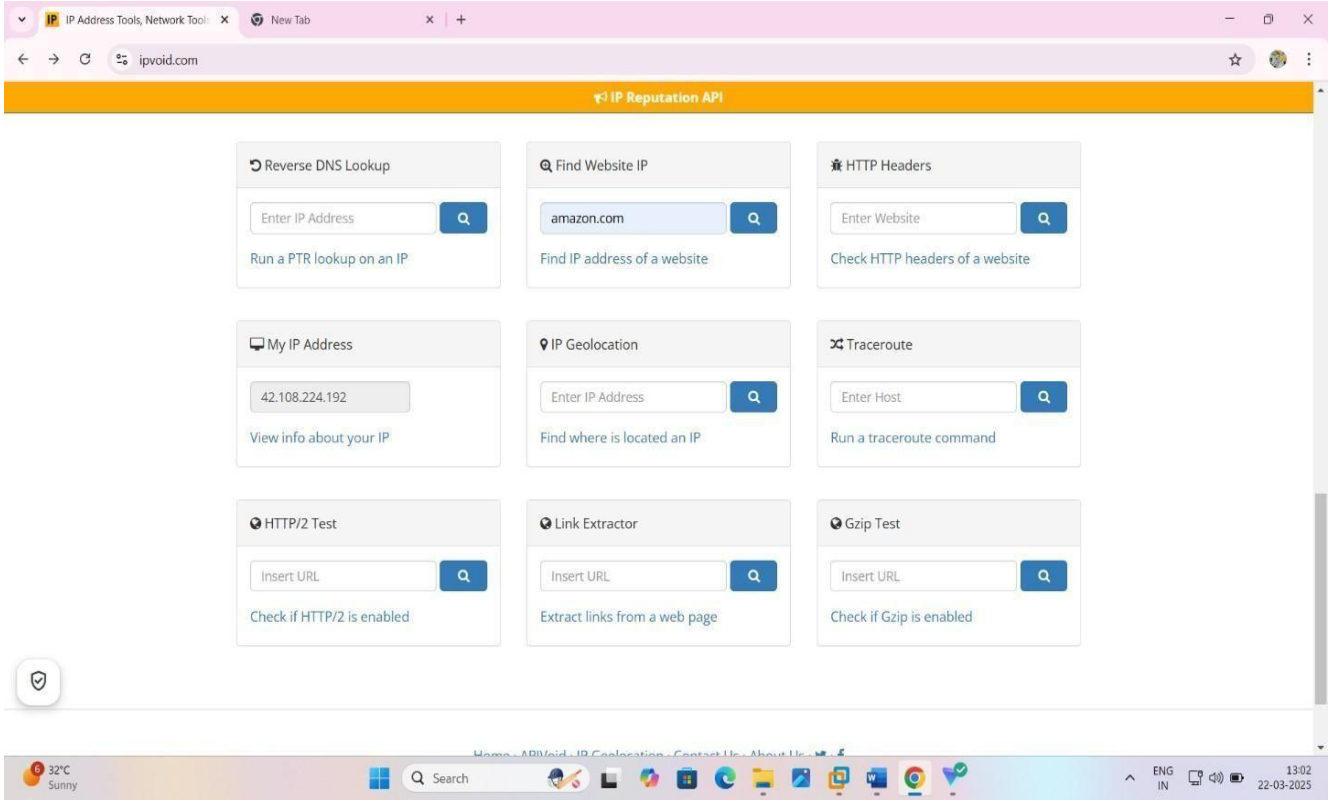
Name : Kunal jawale

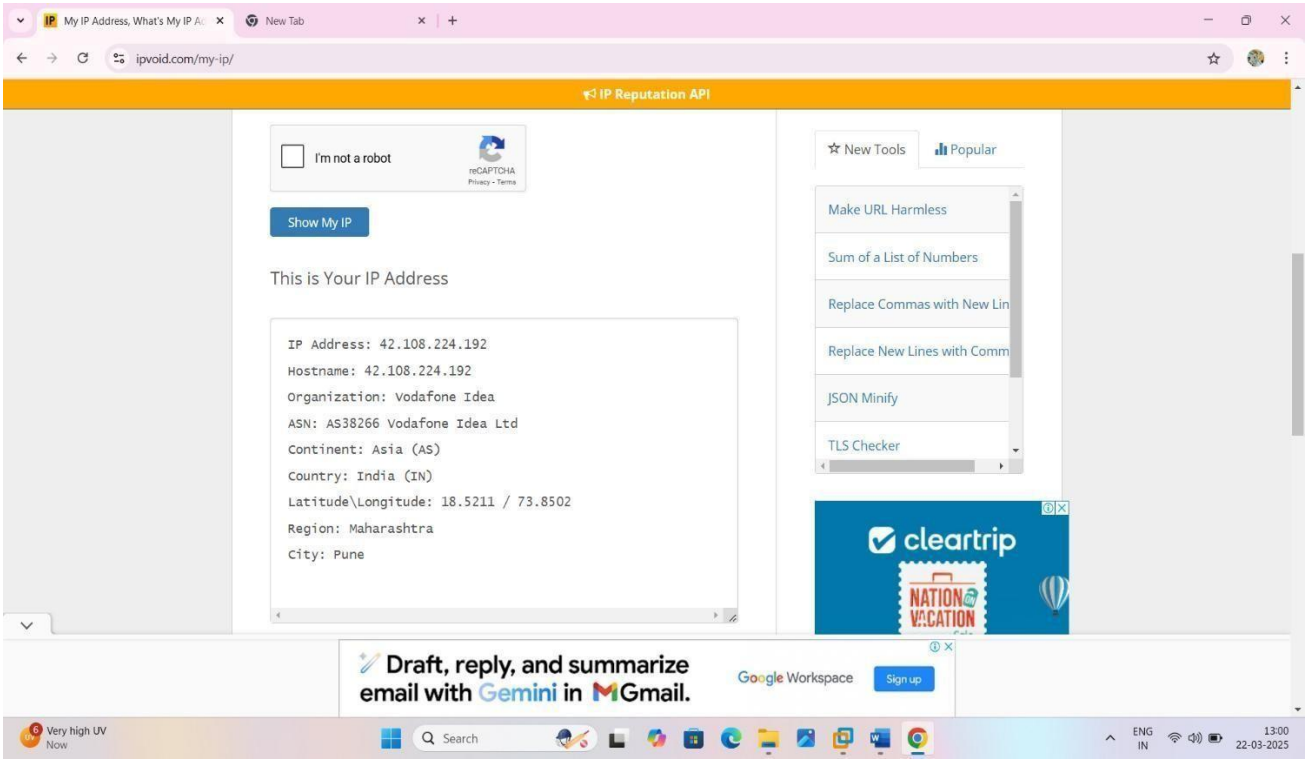
IPVoid offers APIs that allow developers to integrate their threat intelligence capabilities into their systems. These APIs can be used to automatically detect malicious IP addresses and other threats.

This website provide all IP address tools and its very useful to find any information about the IP address, they have best popular IP tools :



Name : Kunal jawale



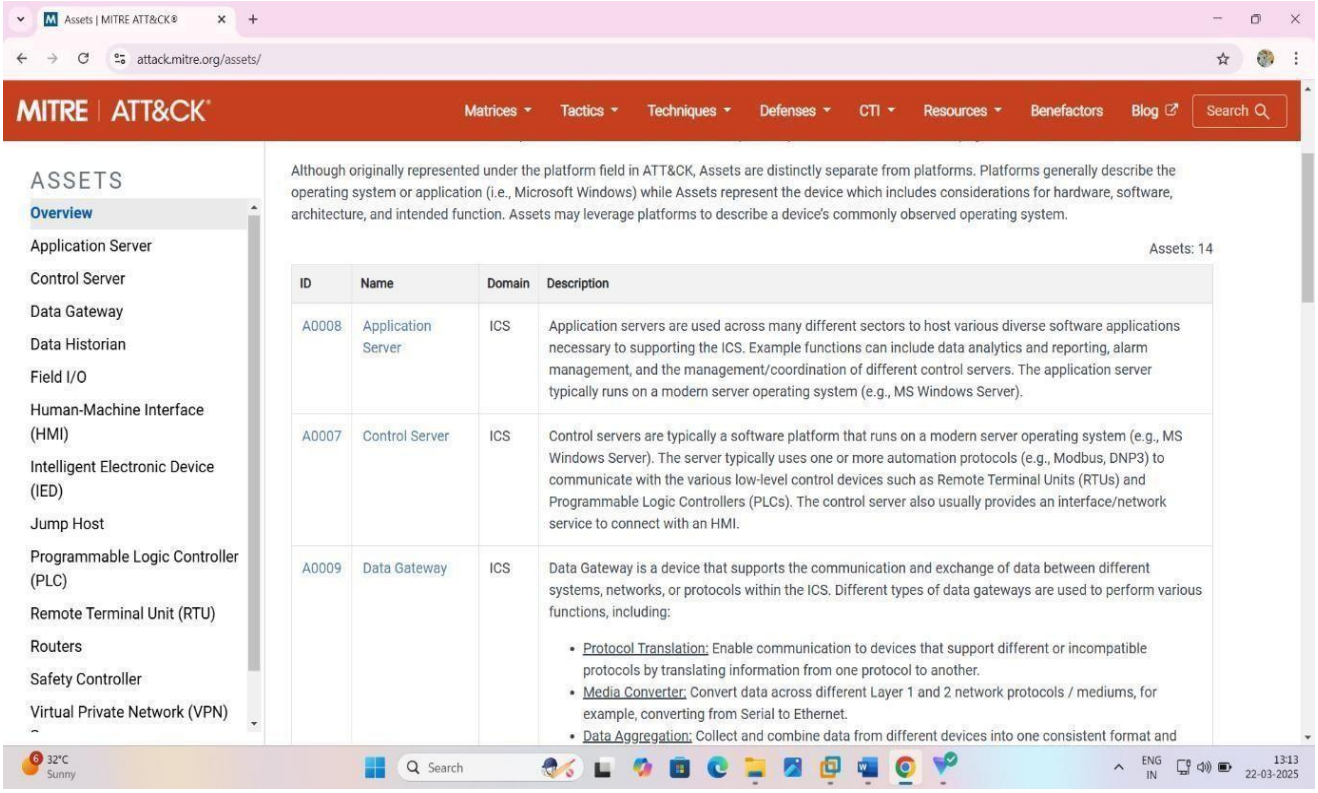


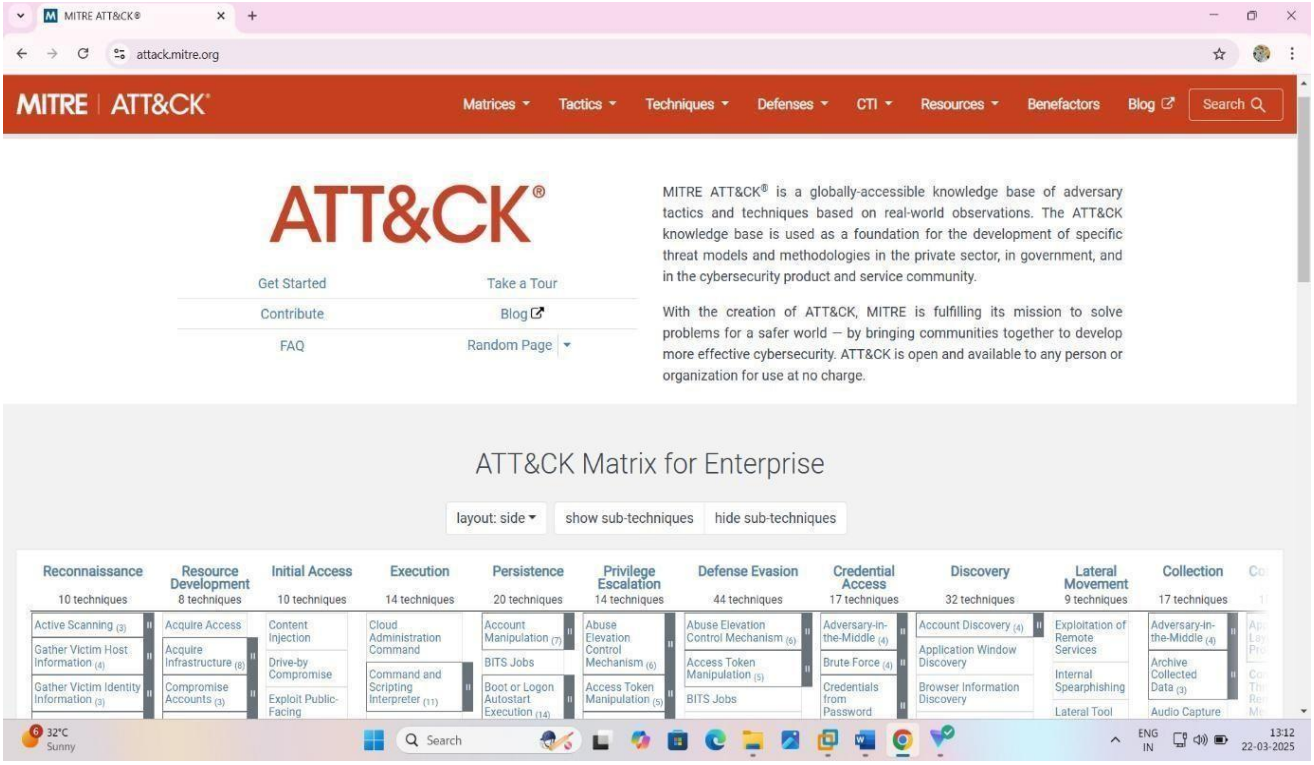
- **Attack.mitre.org –** this framework we use for to understand and defend against cyber attacks by providing a structure knowledge base of adversary tactics ,techniques and procedures (TTPs) ,enabling

Name : Kunal jawale

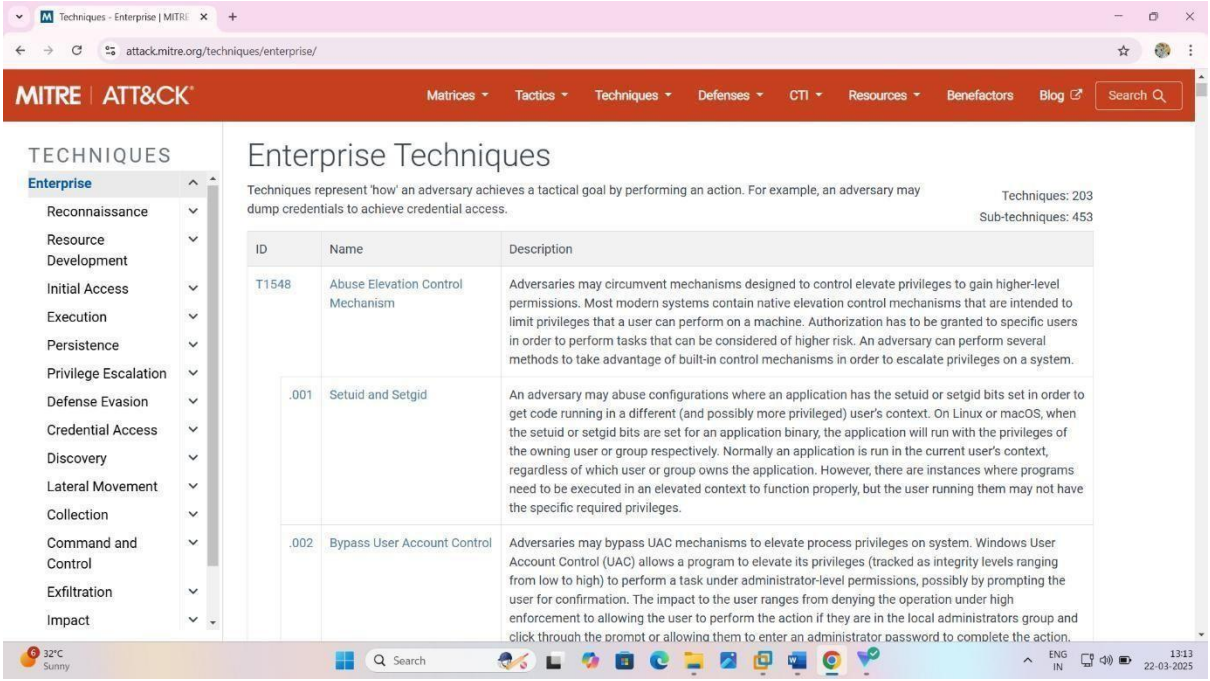
organizations to improve their security posture and incident response capabilities. :

-

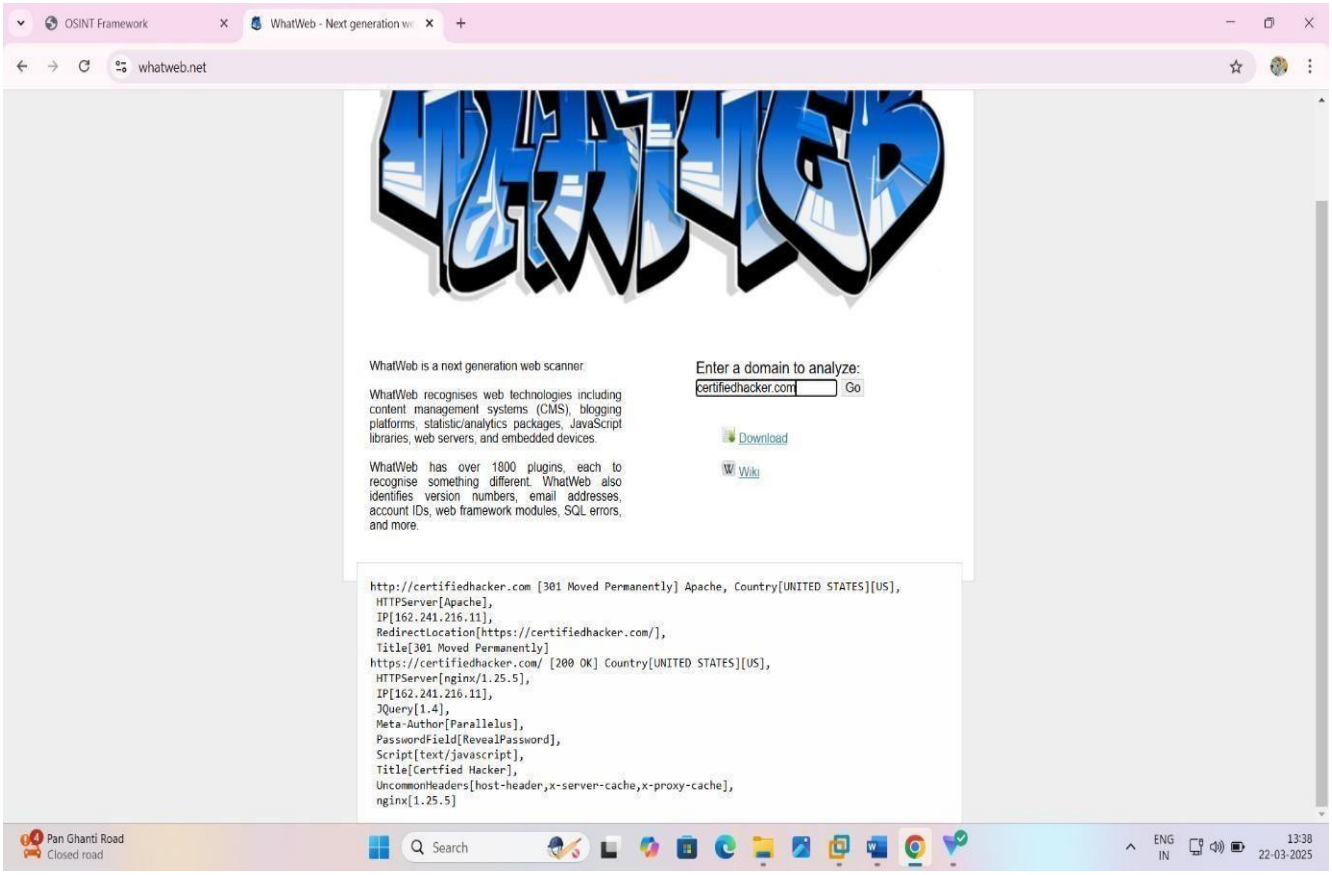




Name : Kunal jawale



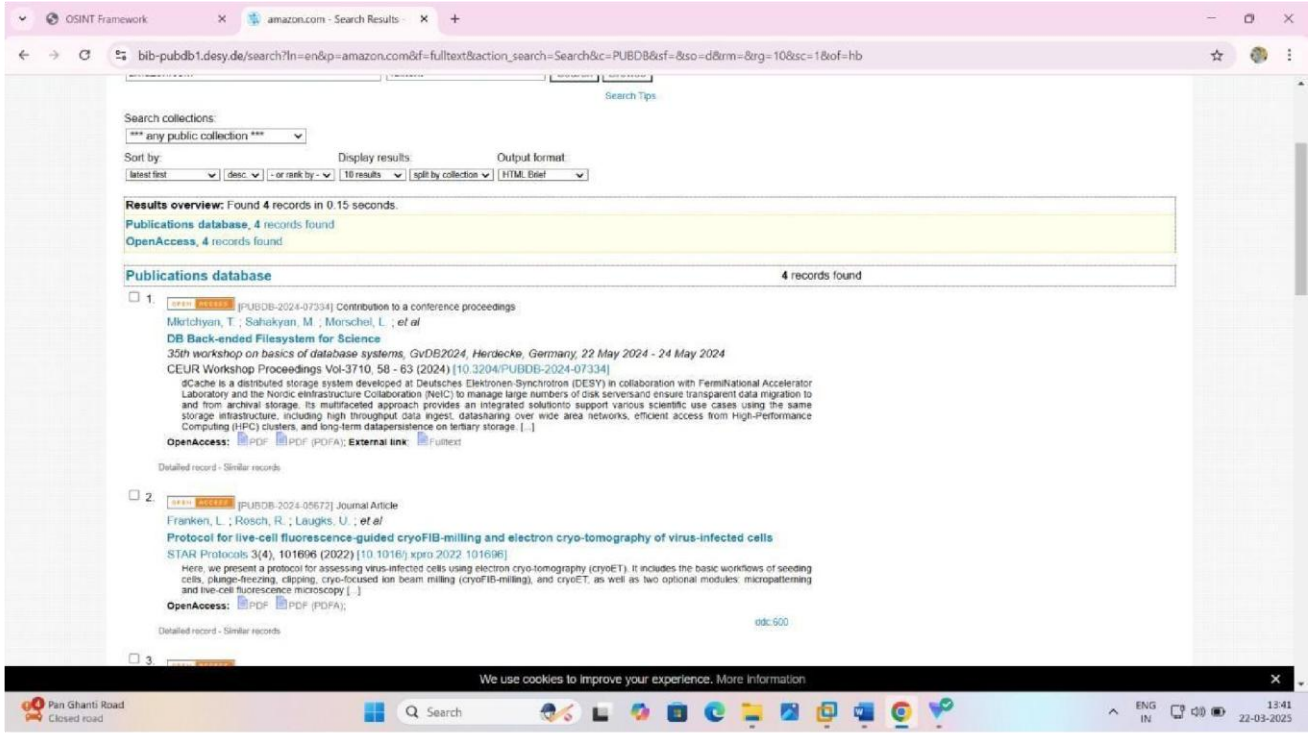
- **Whatweb.net –** this is used for identify the technologies powering a website including CMS ,web servers ,Java script libraries which aids in security
  vulnerability scanning and understanding websites architecture.



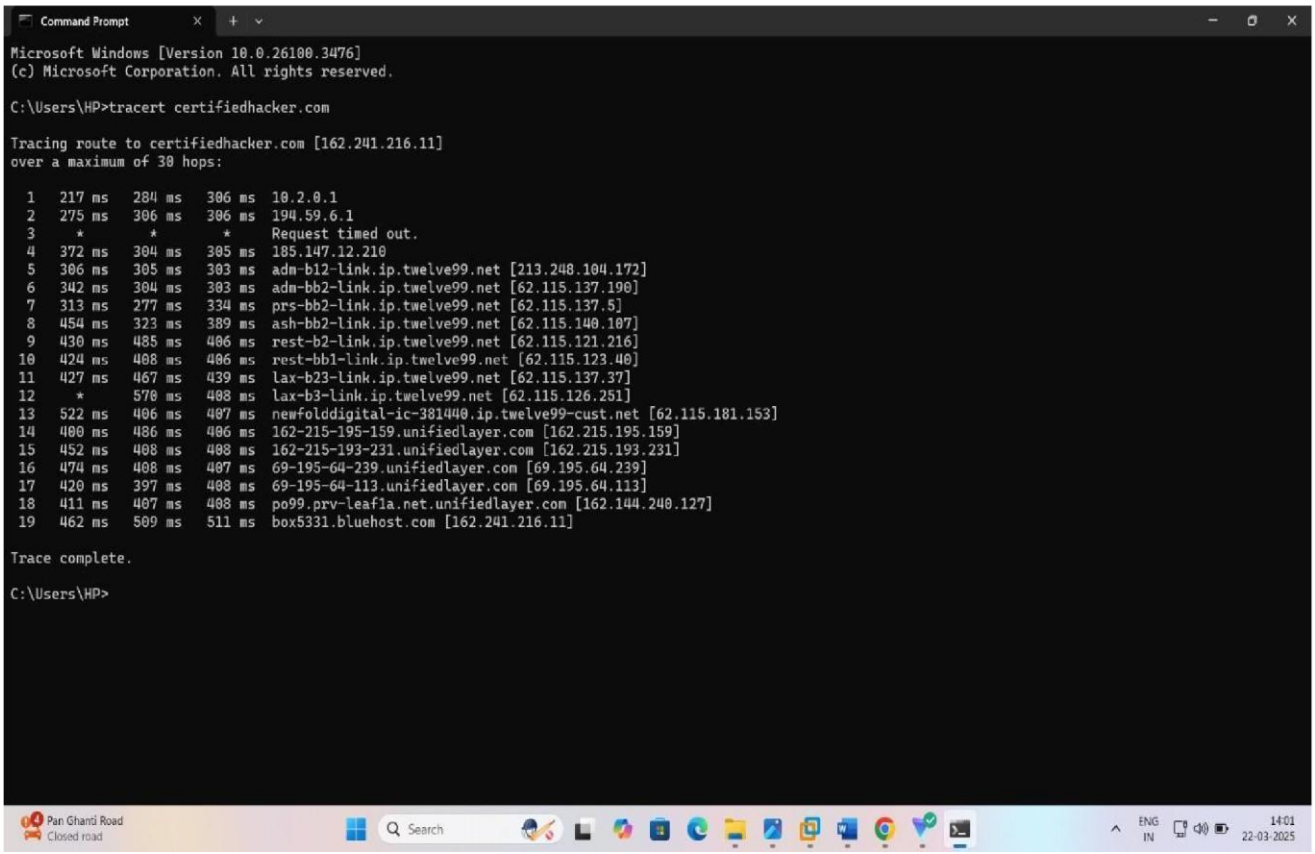
Name : Kunal jawale

- **PUBDB –** PUBDB is DESY publication database, is use for storing and preventing all DESY publications, including versions and providing access to them, often with open full texts .

Name : Kunal jawale



. **CMD command :** tracert - ~~to check how many hops are between destination~~ **:**



```
Command Prompt
Microsoft Windows [Version 10.0.26100.3476]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>tracert certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

  1   217 ms   284 ms   306 ms  10.2.0.1
  2   275 ms   306 ms   306 ms  194.59.6.1
  3     *        *        *     Request timed out.
  4   372 ms   304 ms   305 ms  185.147.12.210
  5   306 ms   305 ms   303 ms  adm-b12-link.ip.twelve99.net [213.248.104.172]
  6   342 ms   304 ms   303 ms  adm-bb2-link.ip.twelve99.net [62.115.137.190]
  7   313 ms   277 ms   334 ms  prs-bb2-link.ip.twelve99.net [62.115.137.5]
  8   454 ms   323 ms   389 ms  ash-bb2-link.ip.twelve99.net [62.115.140.107]
  9   430 ms   485 ms   406 ms  rest-b2-link.ip.twelve99.net [62.115.121.216]
 10   424 ms   408 ms   406 ms  rest-bb1-link.ip.twelve99.net [62.115.123.40]
 11   427 ms   467 ms   439 ms  lax-b23-link.ip.twelve99.net [62.115.137.37]
 12     *      570 ms   408 ms  lax-b3-link.ip.twelve99.net [62.115.126.251]
 13   522 ms   406 ms   407 ms  newfolddigital-ic-381440.ip.twelve99-cust.net [62.115.181.153]
 14   400 ms   486 ms   406 ms  162-215-195-159.unifiedlayer.com [162.215.195.159]
 15   452 ms   408 ms   408 ms  162-215-193-231.unifiedlayer.com [162.215.193.231]
 16   474 ms   408 ms   407 ms  69-195-64-239.unifiedlayer.com [69.195.64.239]
 17   420 ms   397 ms   408 ms  69-195-64-113.unifiedlayer.com [69.195.64.113]
 18   411 ms   407 ms   408 ms  po99.prv-leaf1a.net.unifiedlayer.com [162.144.240.127]
 19   462 ms   509 ms   511 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\HP>
```

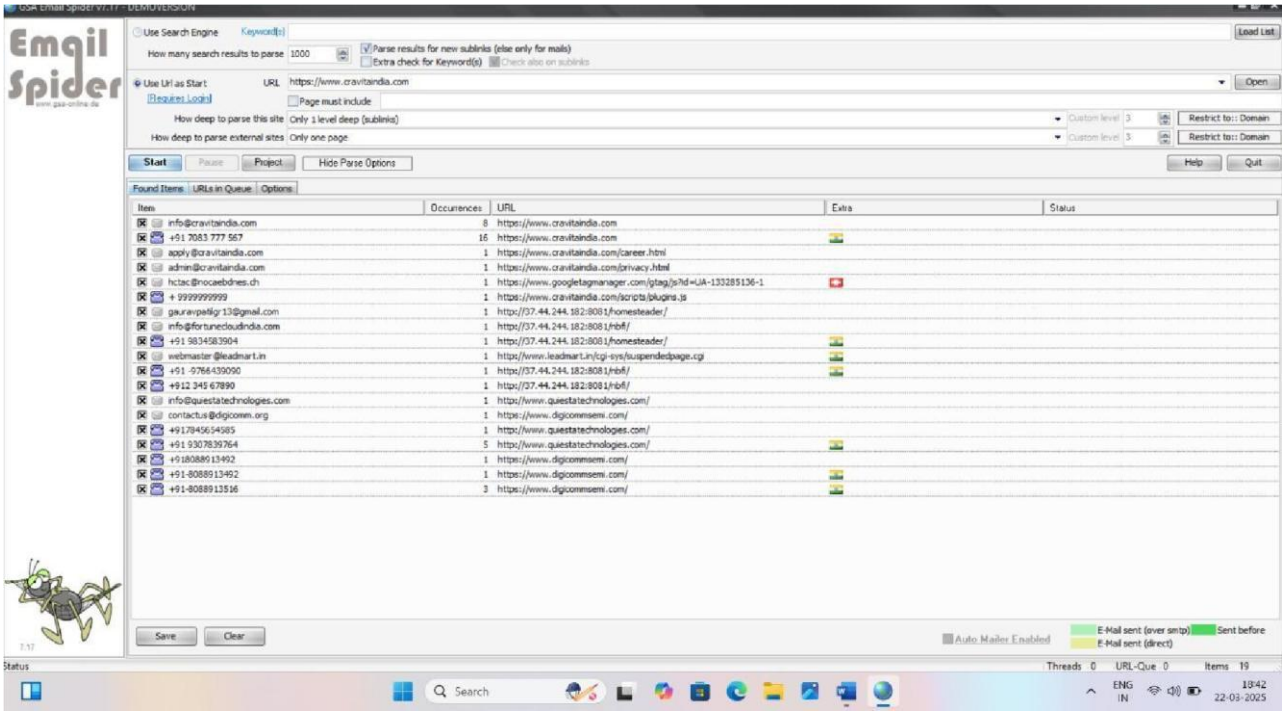
. there are 2 applications that is very useful when you do information gathering : 1 GSA email spider

Name : Kunal jawale

2 Angry IP scanner

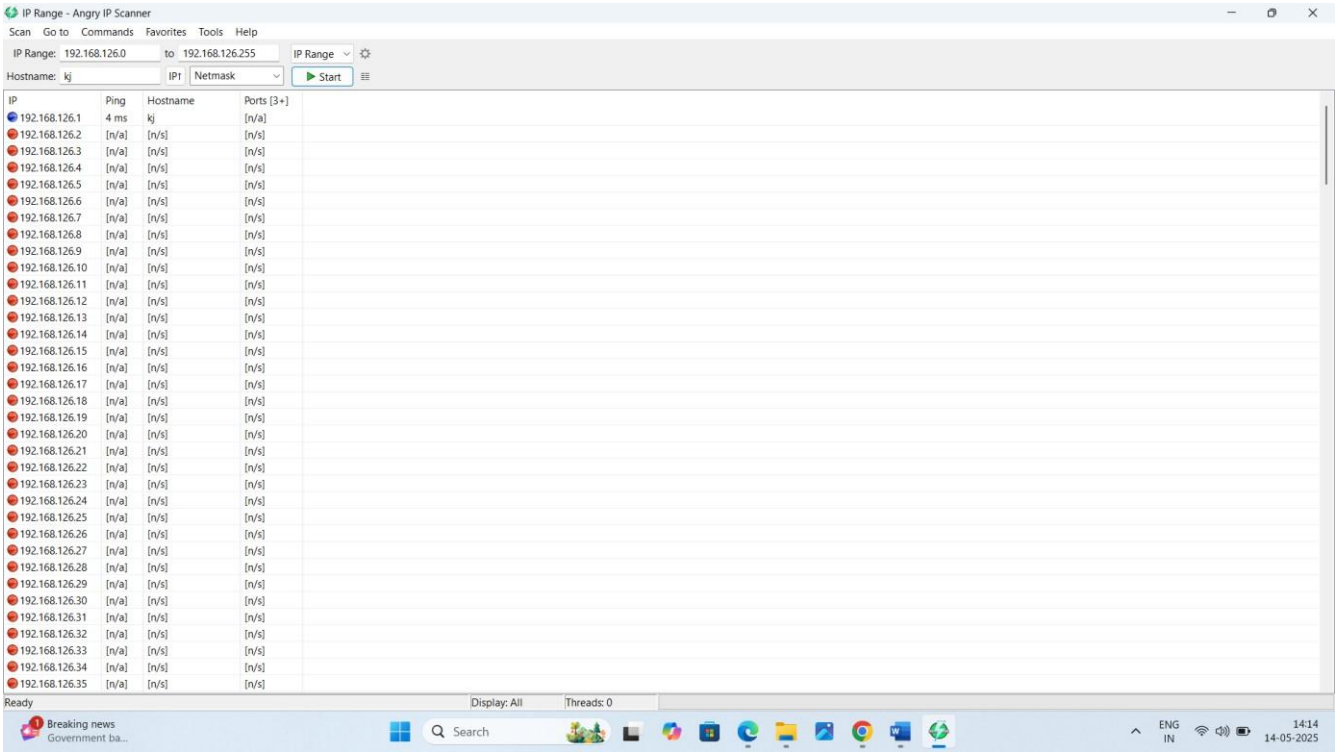
1 **GSA email spider :-** The GSA Email Spider is collecting E-Mails as well as phone and fax numbers from websites. It can locate websites by keywords using search engines or when you import or add URLs to parse.

The GSA Email spider is used to collect and extract email addresses , phone numbers and fax numbers from websites by searching for them using keywords or by importing URLs. :



2 **Angry IP Scanner :-** This tool is used for its speed , ease of use and ability to quickly scan IP addresses and ports to identify active devices ,gather network information and network management.

Name : Kunal jawale



Green colour indicates that the target IP address is up and it has open ports.

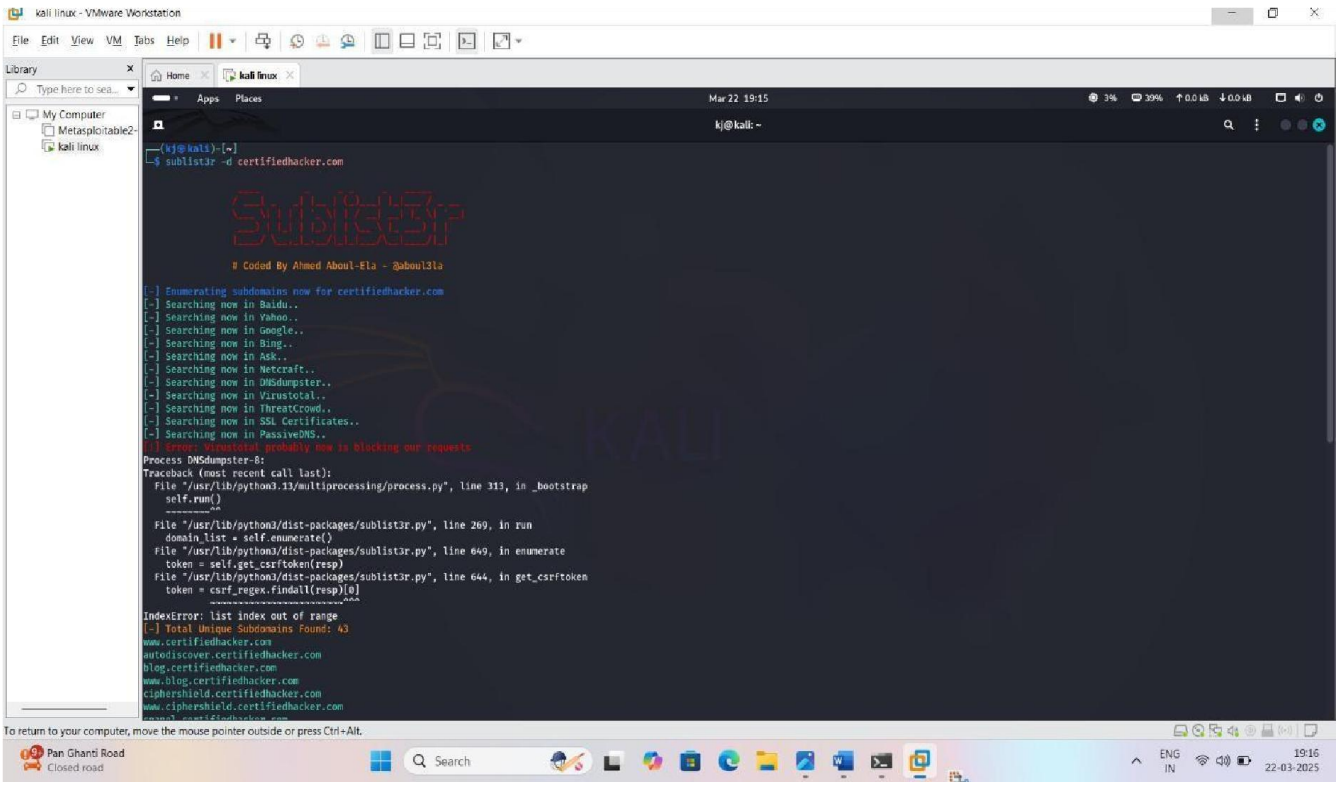
. now we are using some kali Linux tools for information gathering .

- **Sublist3r –** this tool is used for manual and automated subdomain enumeration , this is very Useful to find subdomains for a given domain: **Command is :**

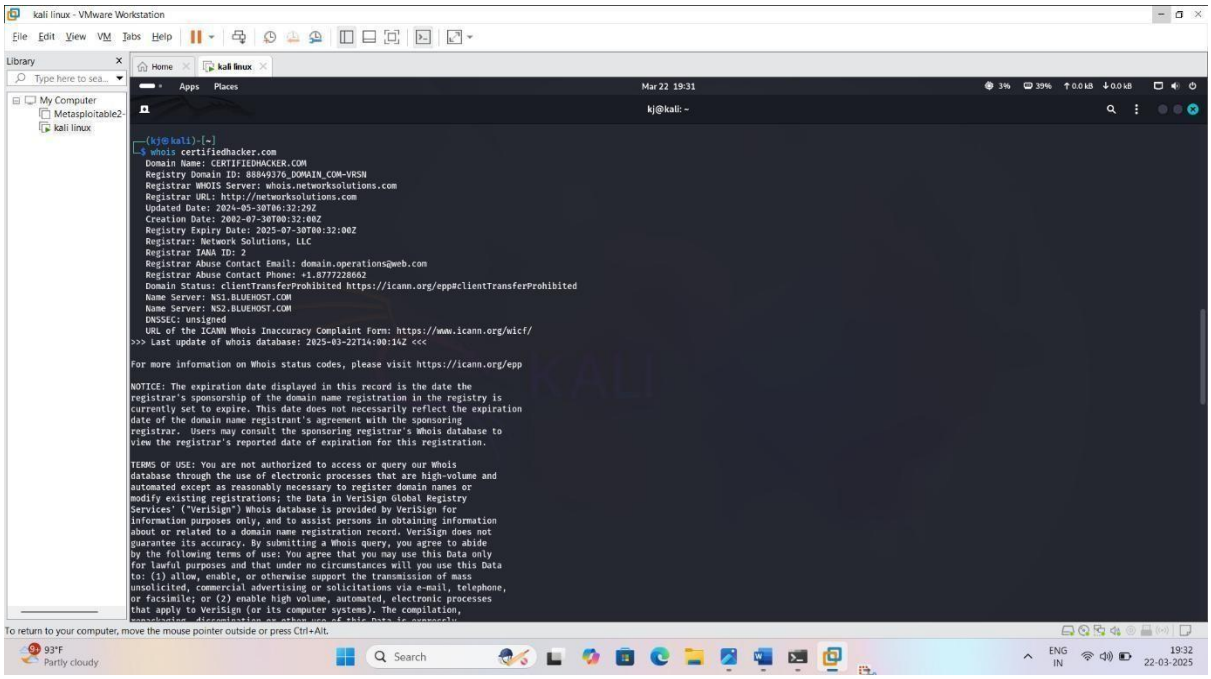
  Sublist3r -d (domain name)

  -d is used for domain

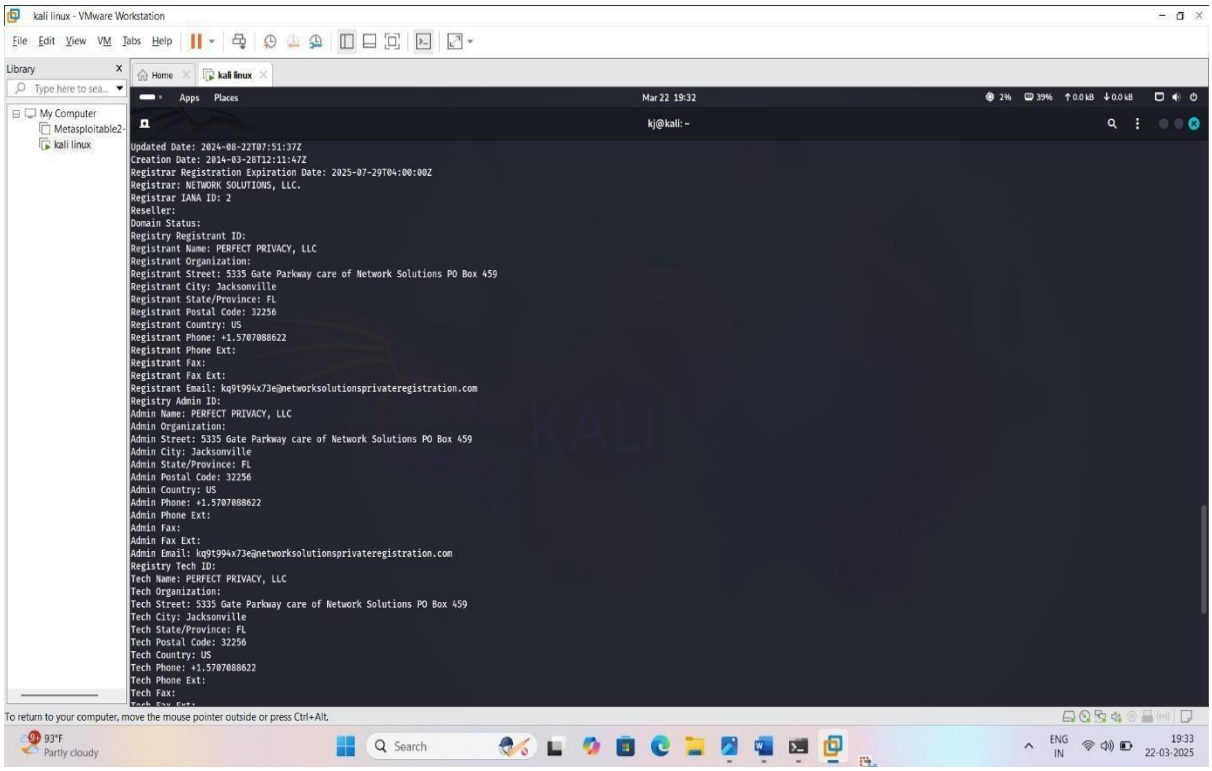
Name : Kunal jawale



- **Whois –** this tool is helps you to find information about domain names , IP address and autonomous systems its used for veriety of purposes including > domain research , background checks ,fraud prevention , tracking spam and identifying domain status.
  Command is : whois (domain name or IP).

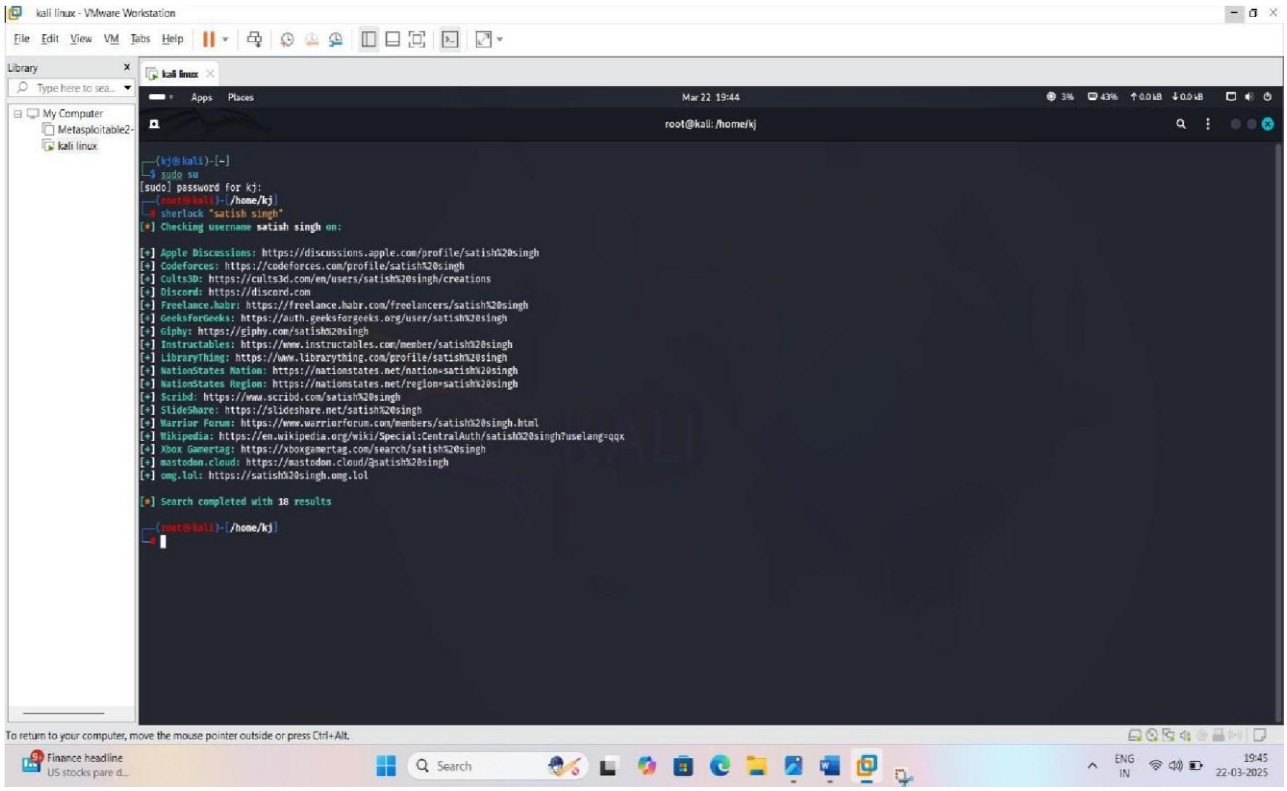


Name : Kunal jawale



- **Sherlock-** this tool is used for hunt name or number in social media

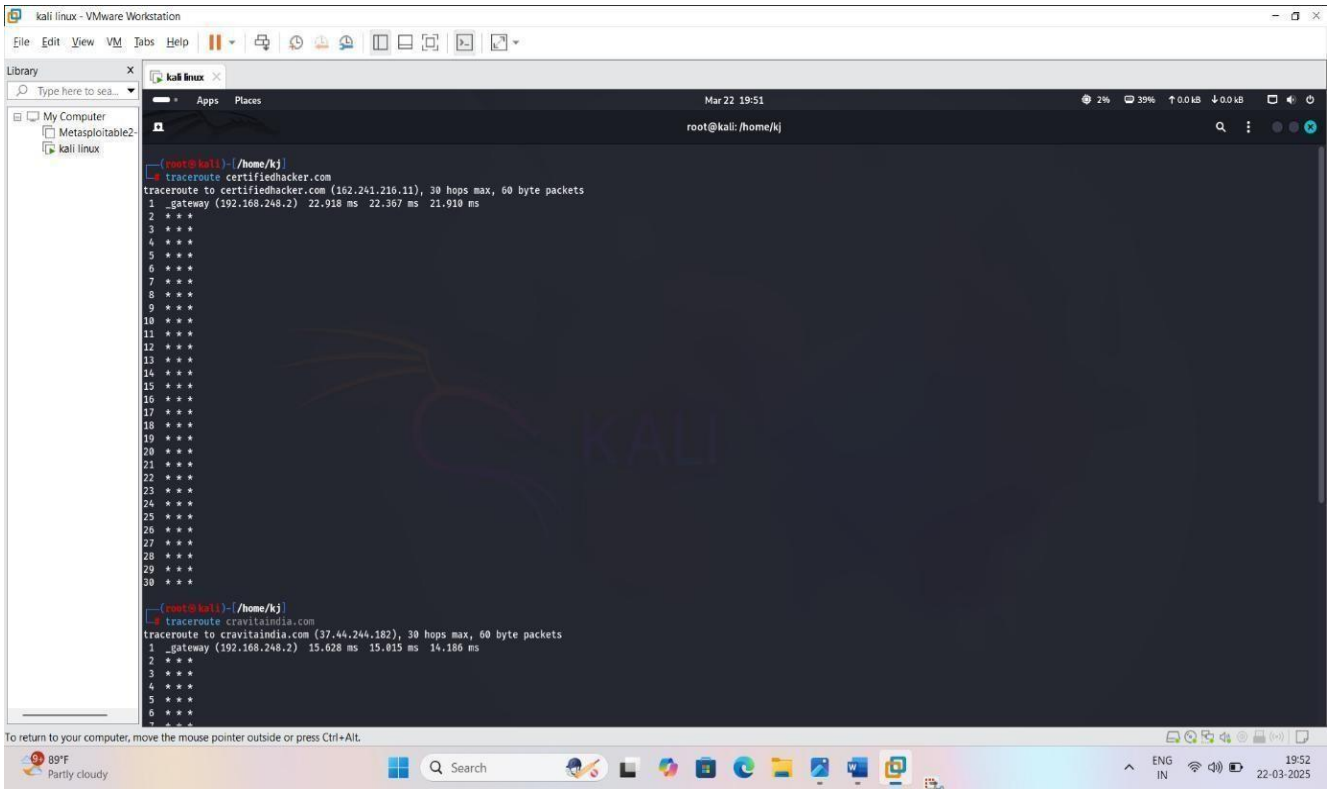
  Command : sherlock (name or number or mail id)



Name : Kunal jawale

- **Traceroute –** this tool is used for trace the path network packets take from your computer to a destination IP address or hostname ,identifying each hop (router) along the way and measuring the round-trip time for each hop.

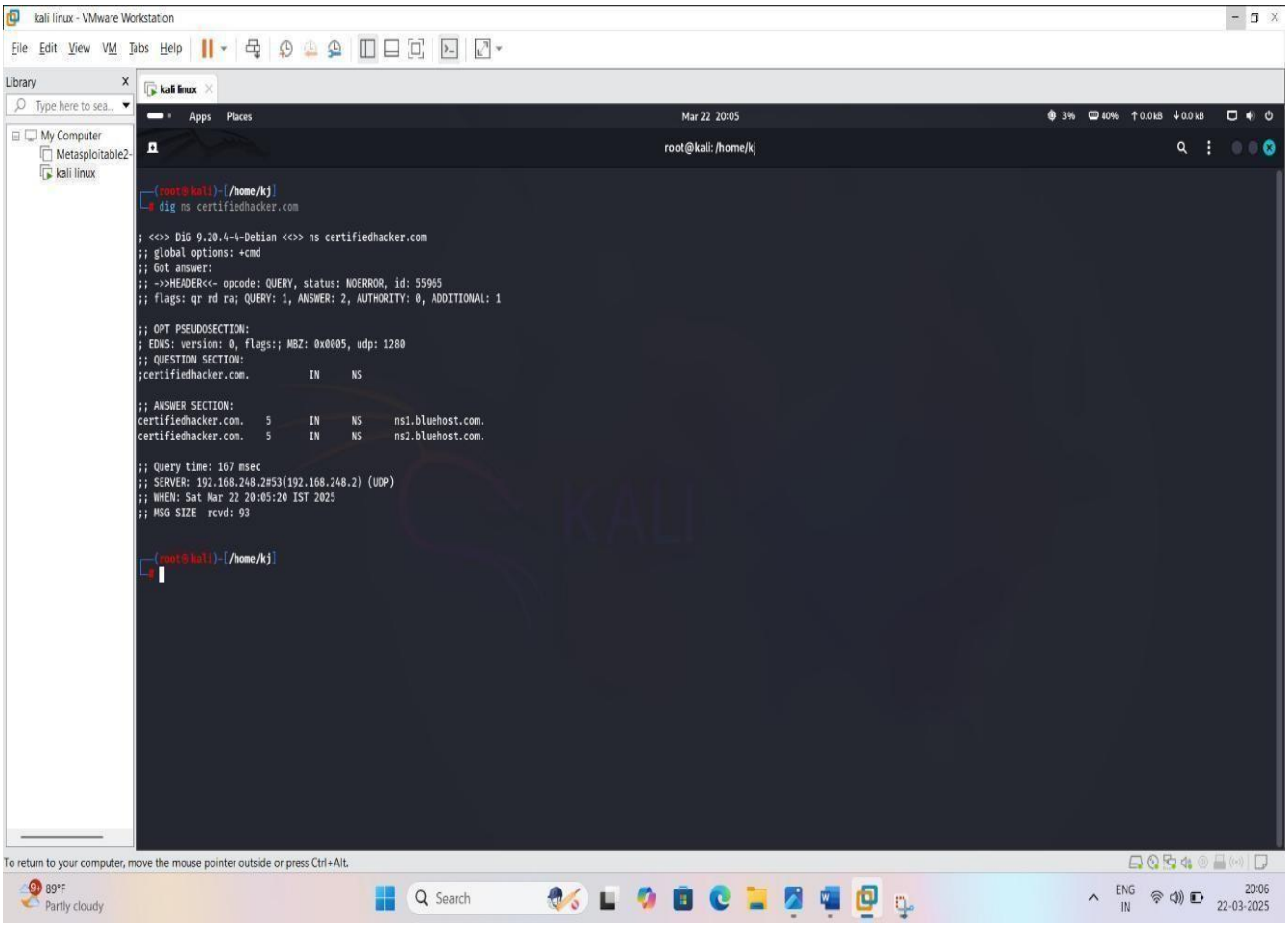
  Command : traceroute (domain)



DNS Information gathering

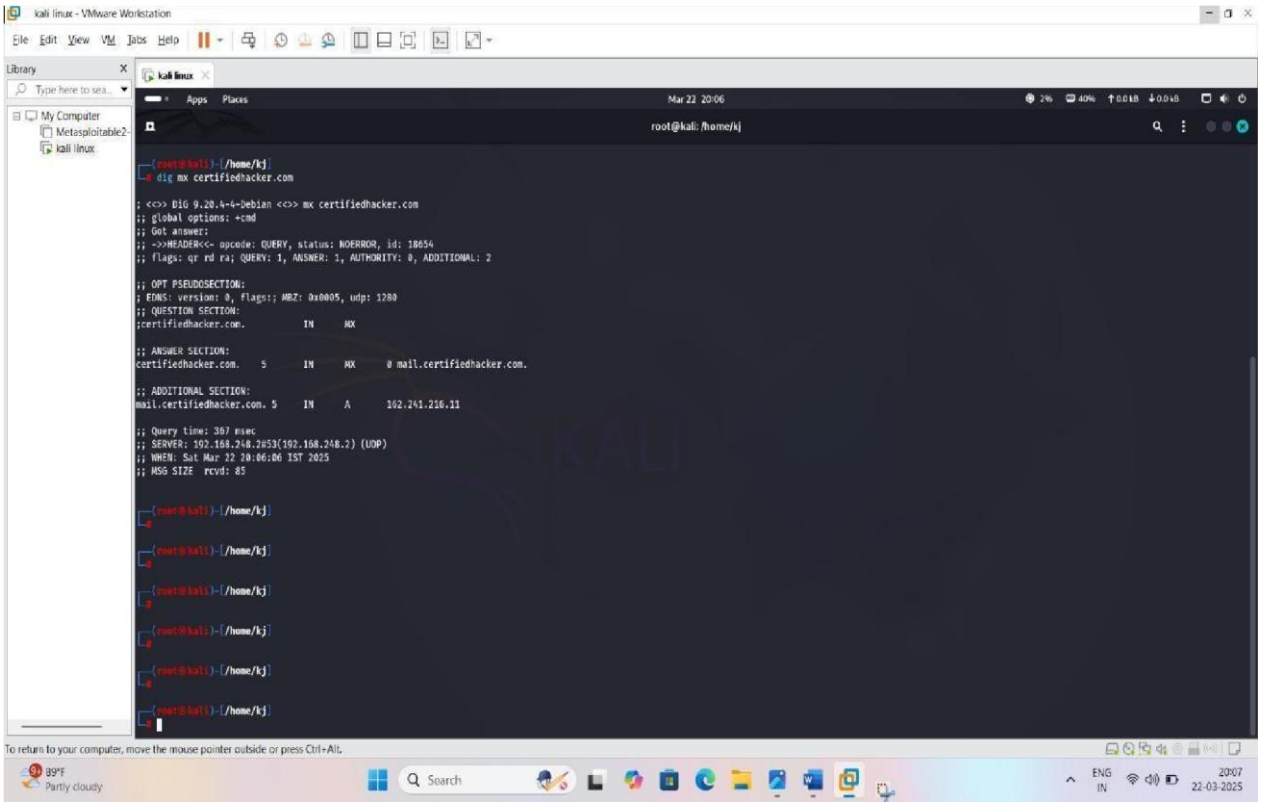
- **Dig –** this is a powerful tool for querying the domain name system and information about domain names and their associated records ,like IP addresses ,mail servers and name servers helping with DNS troubleshooting and verification **Here are some commands in dig . dig ns (domain)-** to find the nameservers (NS records) responsible for a specific domain.

Name : Kunal jawale

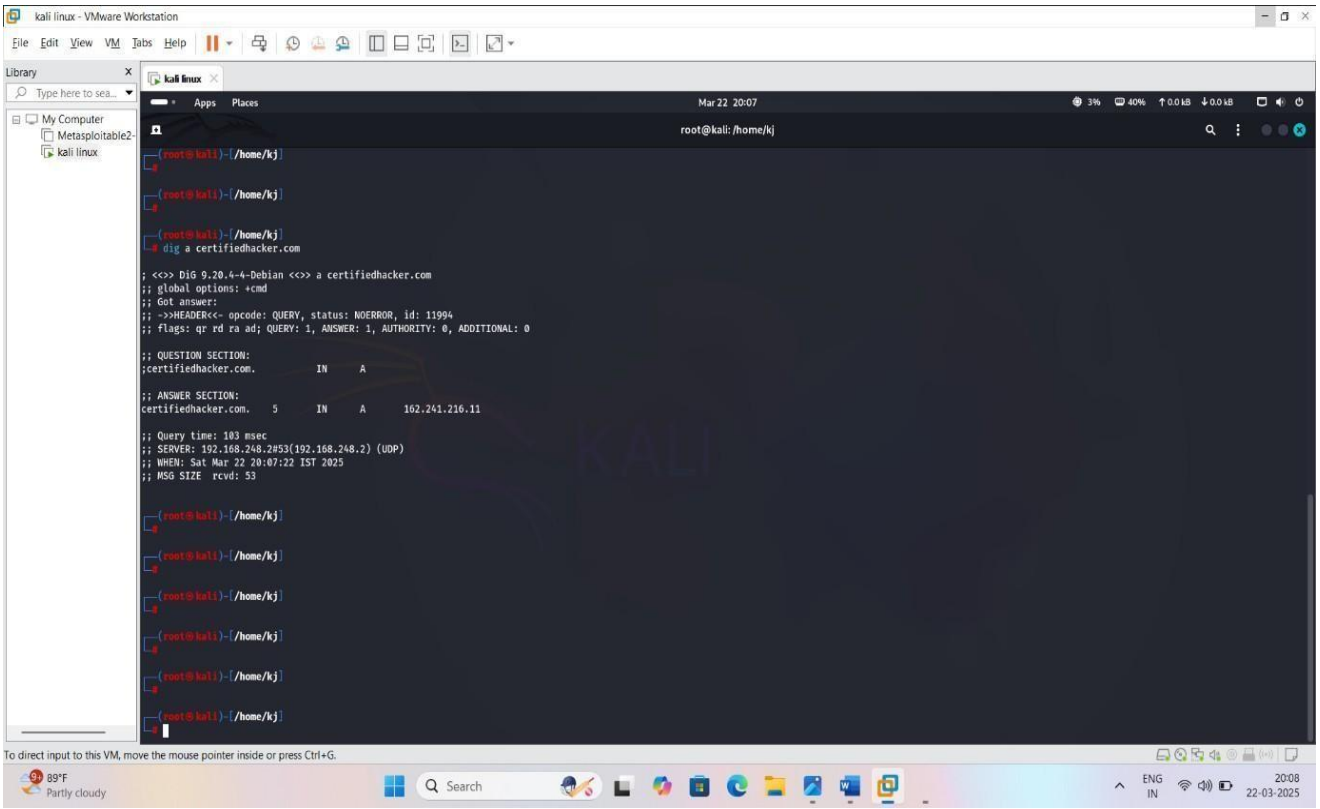


. dig mx (domain)- to retrieve and display the mail exchange (MX) records for given domain , which specify the mail servers responsible for handling email for the domain.

Name : Kunal jawale

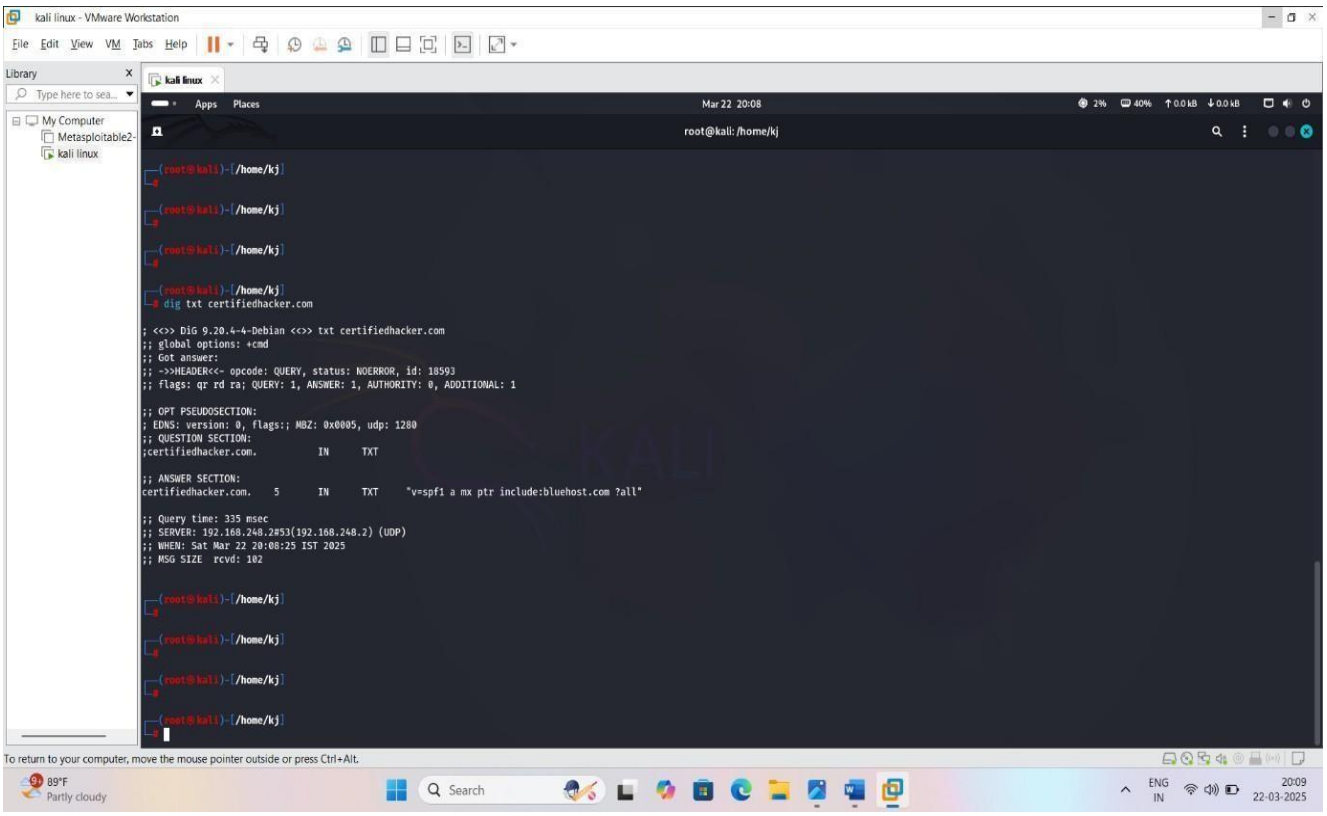


.dig A (domain)- this command querying the DNS to find the IPv4 address (A record) associated with given domain name .

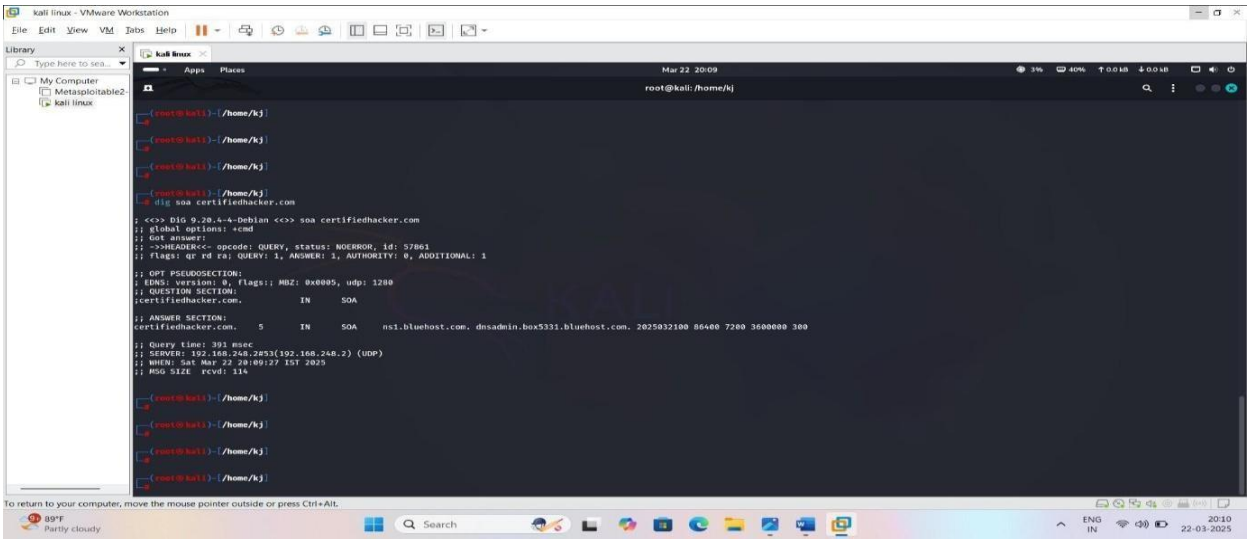


Name : Kunal jawale

. dig txt (domain)- to retrieve and display the text records associated with given domain which can include information like SPF, DKIM, and DMARC records.



. dig Soa (domain)- this command indicates what the name server is for that domain .SOA stands for “start of authority”.



- **theHarvester –**

Name : Kunal jawale

theHarvester command is used for OSINT (open source Intelligence) gathering . it helps in collecting information about domains , emails , subdomains , Ips , and usernames from public source like

. **search engines (**google,bing,yahoo**)**

. **social media (**LinkedIn,Twitter**)**

. **Public database (**shodan , PGP key servers**)**

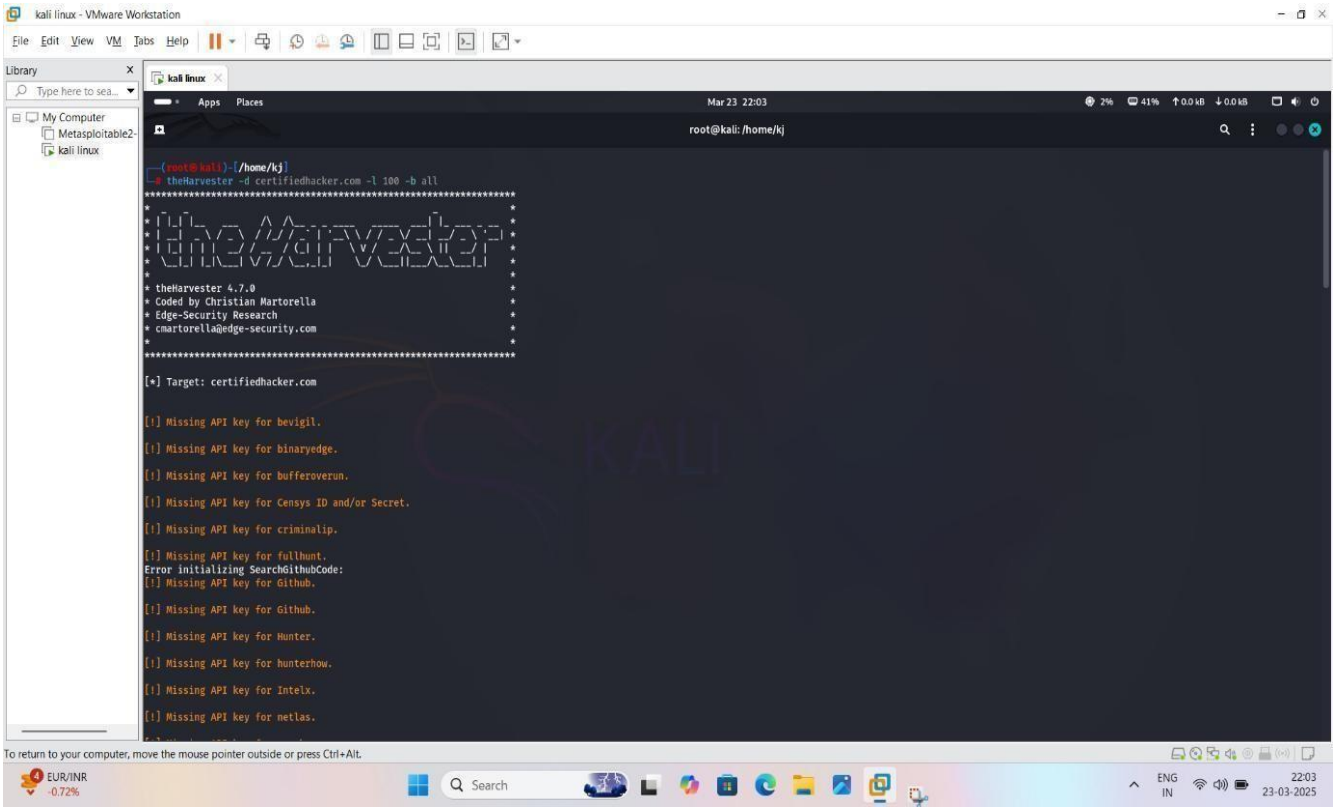
. **threat intelligence platforms**

Command : theHarvester -d (domain name) -l 200 -b all

-d for domain name

-l for limit

-b for source (google,yahoo,Baidu)



. here are some types of command for theHarvester

1 . gather mails and subdomains from bing

Command : theHarvester -d example.com -b bing

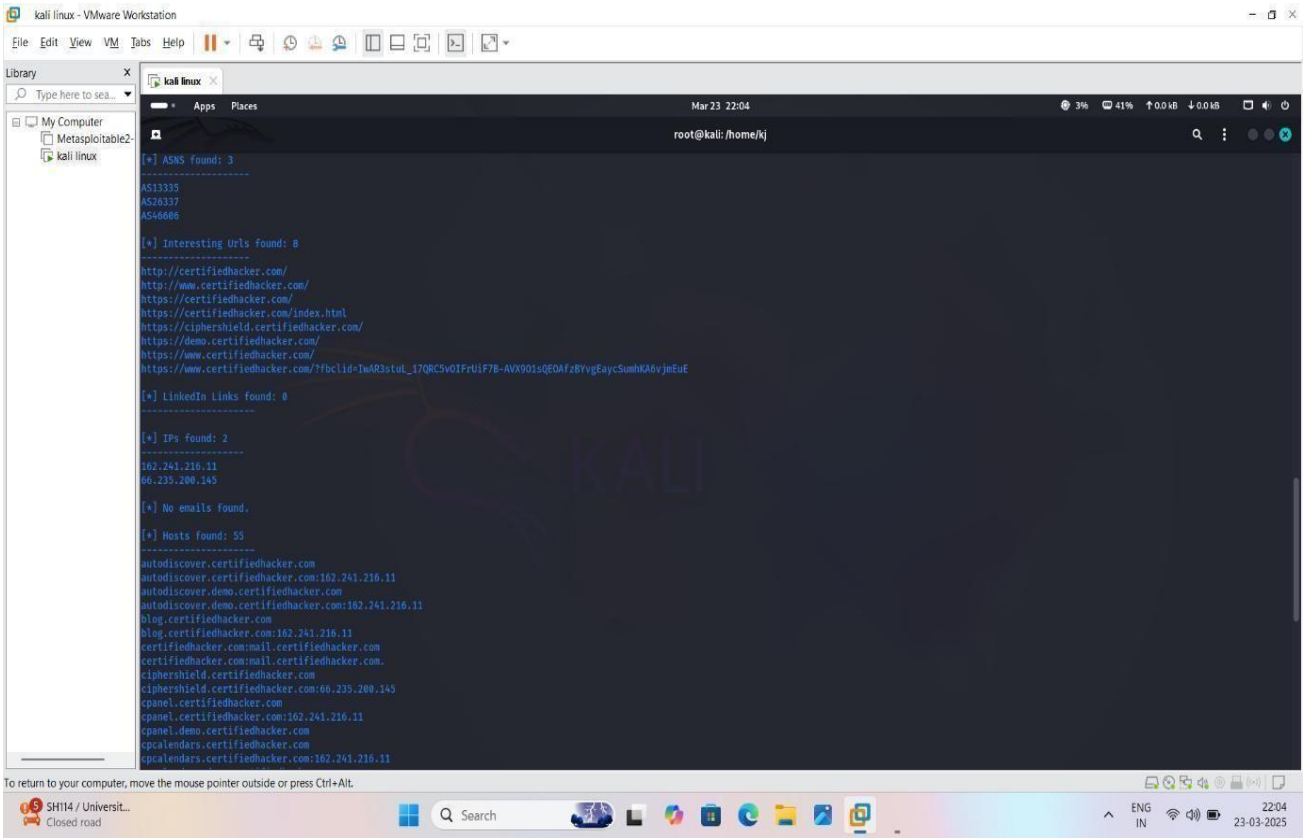
2. *use multiple source*

Name : Kunal jawale

Command : theHarvester -d example.com -b all

3. *save the results to a file* theHarvester -d example.com -b all -f output.txt

4. *scan for hosts and DNS records* theHarvester -d example.com -b dnsdumpster.



 Recon-ng – Recon-ng is free and open source tool available on GitHub. Reconng is based upon Open Source Intelligence (OSINT), the easiest and useful tool for reconnaissance. Recon-ng interface is very similar to Metasploit 1 and Metasploit 2.Recon-ng provides a command-line interface that you can run on Kali Linux. This tool can be used to get information about our target(domain). The interactive console provides a number of helpful features, such as
command **completion and contextual** help. Recon-ng is a Web Reconnaissance tool written in Python. It has so many modules, database interaction, built-in convenience functions, interactive help, and command completion, Recon-ng provides a powerful

environment in which open source webbased **reconnaissance** can be conducted, and we can gather all information.

this tool is use for automating and streamlining the process of gathering information about the target during security assessments.

/ here are some command and their uses :

. marketplace install all - to install all recon-ng files .

. modules search – to check workspaces.

. **workspaces create (name)** – to create new workspaces .

. **workspaces list** – to check how many workspaces is there .

. **workspaces load (name)** – to inter in given workspace.

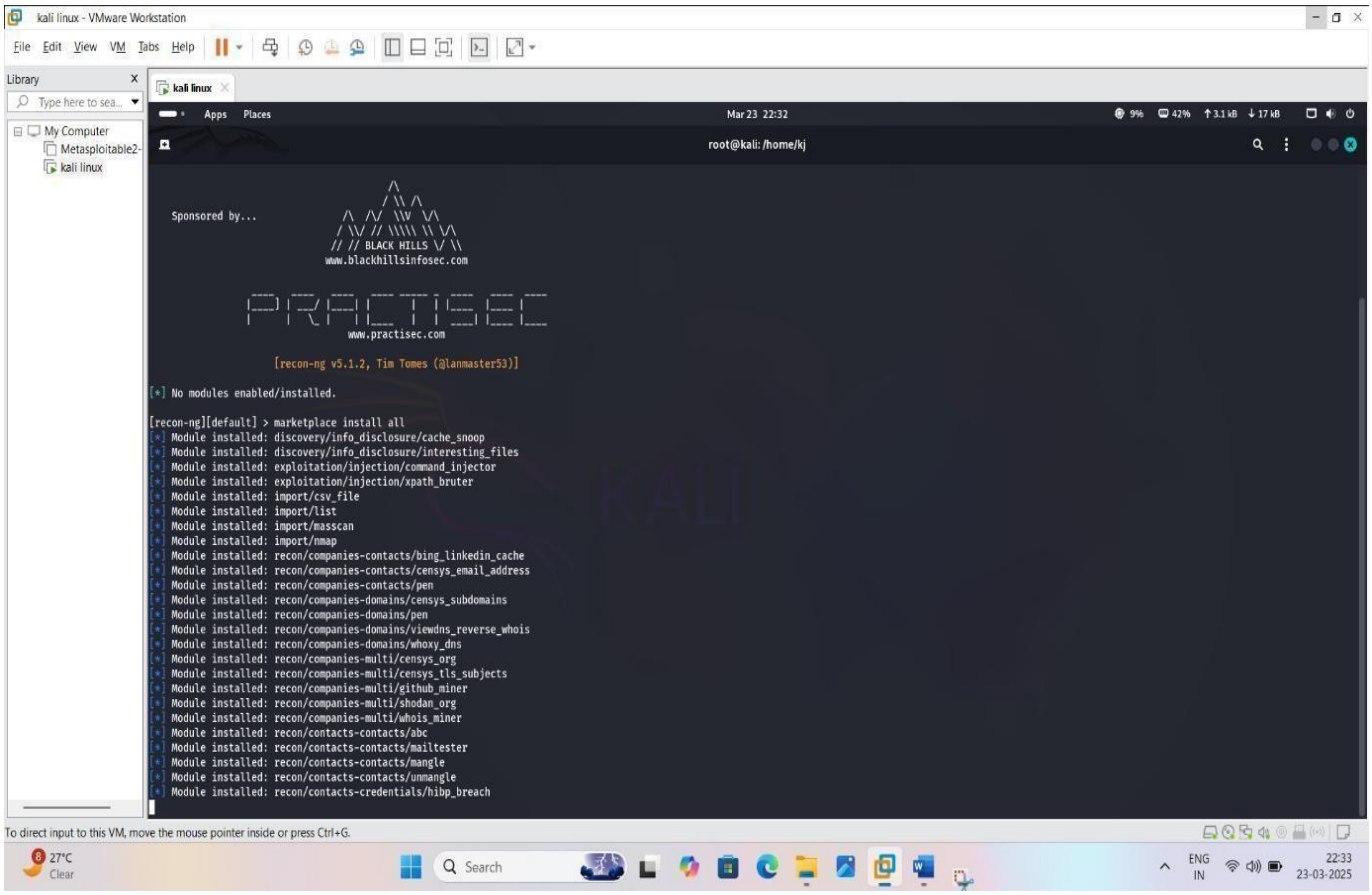
. db insert domains – to create the domain and domain name .

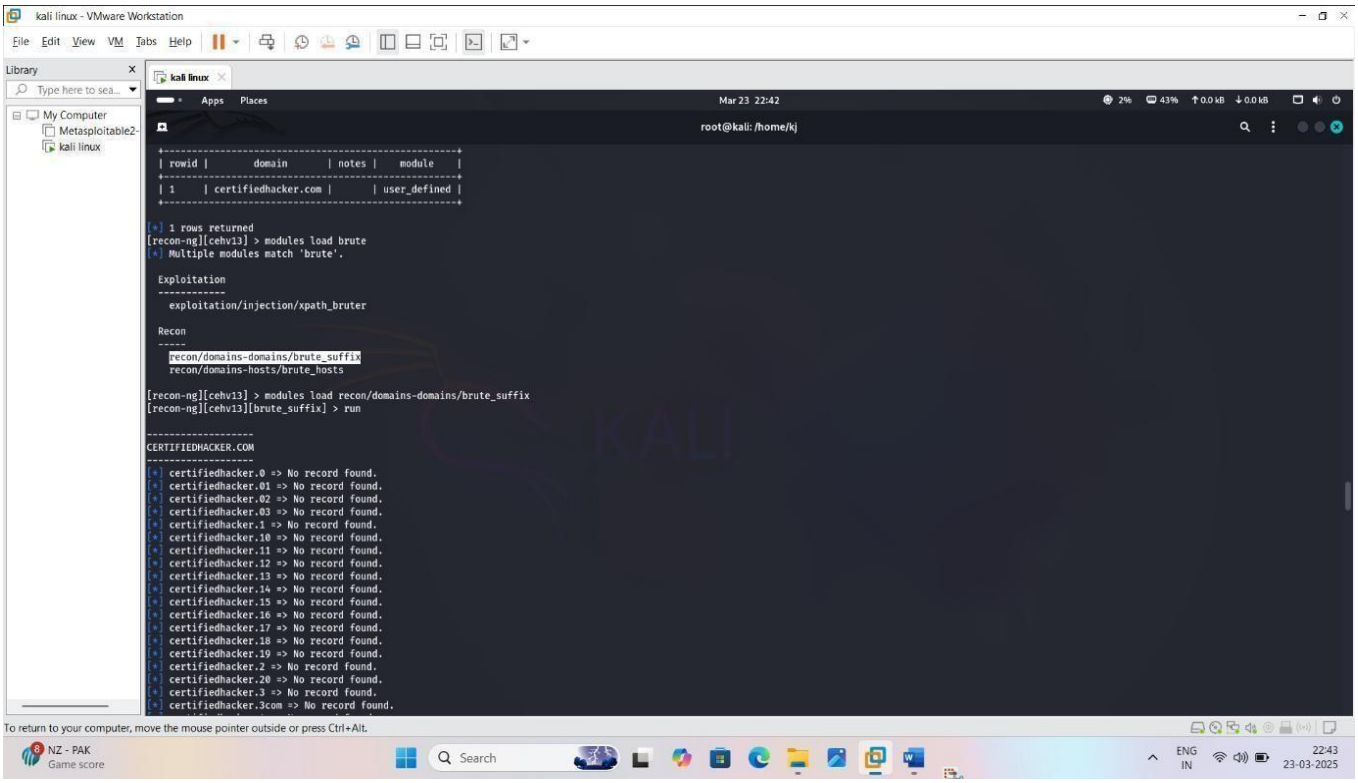
. show domains – to see which or how many domain we created .

. modules load brute – this is used for bruteforce attack **. modules load** and copy the brute recon **. run** – to capture all subdomains .

. back – to back to workspace .

Name : Kunal jawale





Name : Kunal jawale