

## 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 intrusion detection system (IDS) and may be logged.

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

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

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

. Here are some Google hacks for Information Gathering:

- o **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.

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.

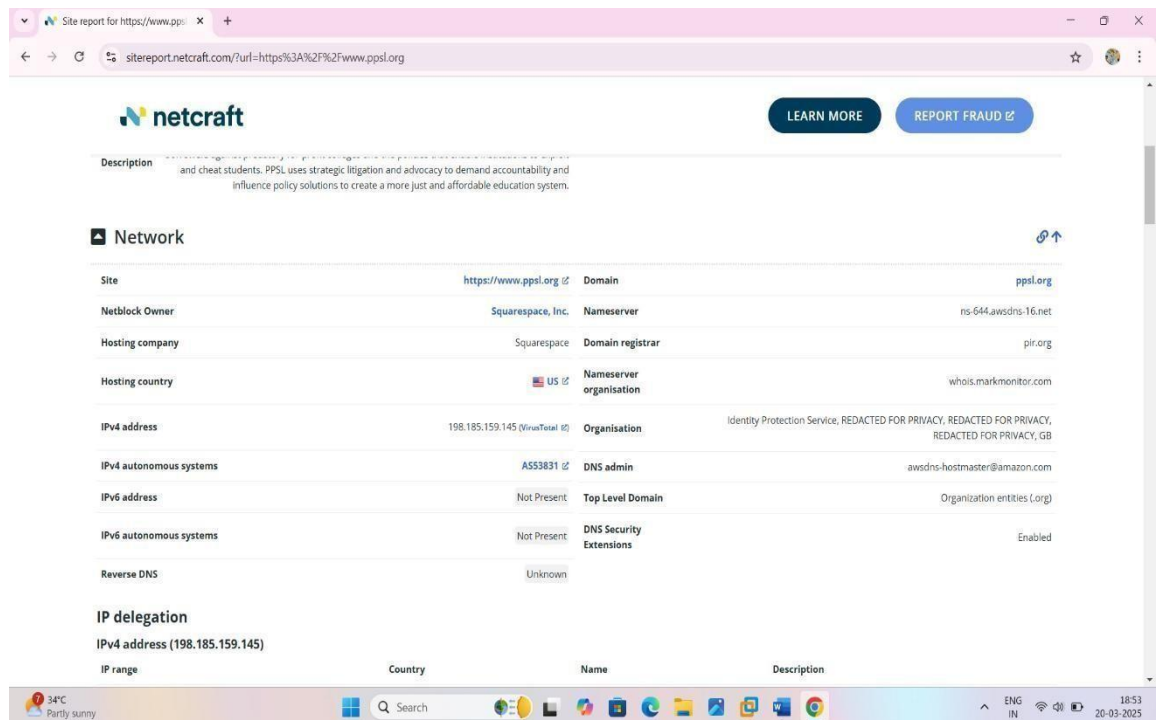
- **Transparency & Reporting:**

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



- o **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.

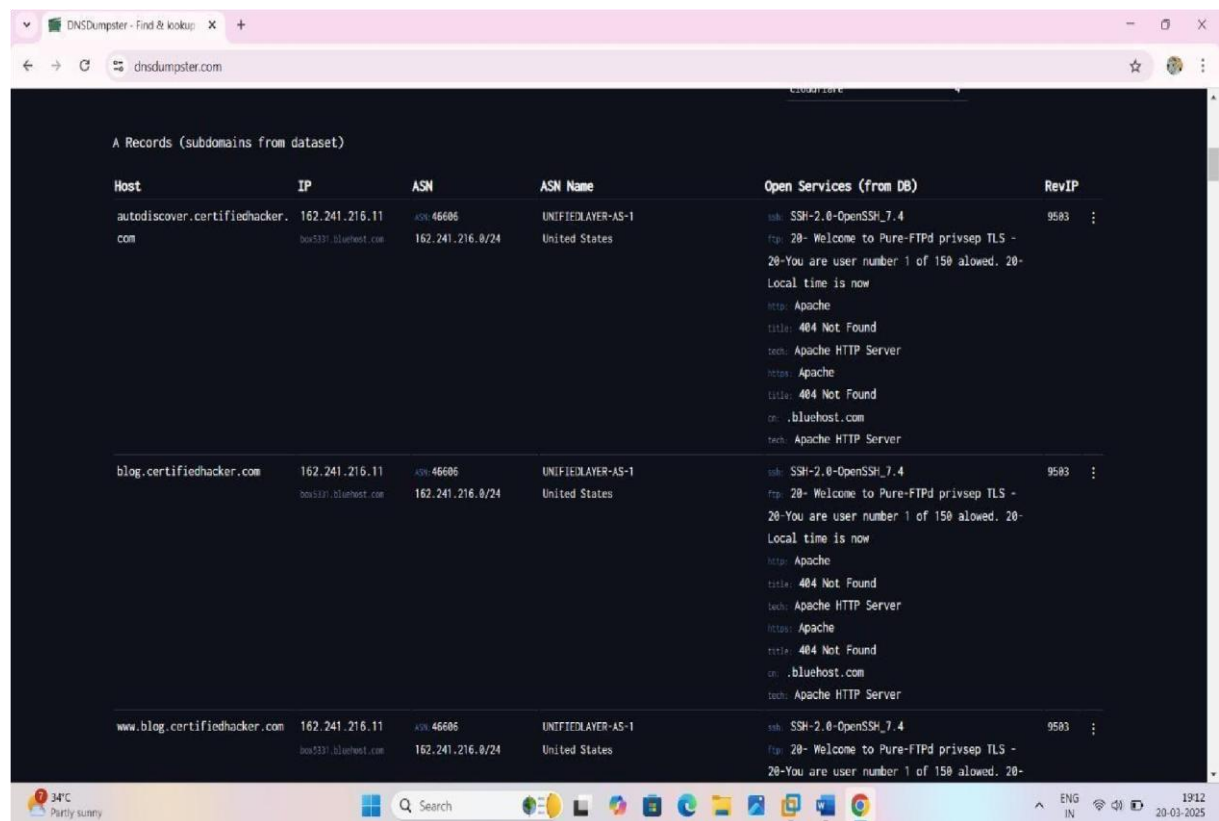
- **Free and Plus Options:**

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.

The screenshot displays the who.is website interface for a WHOIS lookup of 'certifiedhacker.com'. The browser's address bar shows 'who.is/whois/certifiedhacker.com'. The website header includes navigation links like 'Premium Domains', 'Transfer', 'Features', 'Login', and 'Sign Up', along with a search bar. The main content area is titled 'certifiedhacker.com' and 'whois information', with tabs for 'Whois', 'RDAP', 'DNS Records', 'Uptime', and 'Diagnostics'. The 'Whois' tab is active, showing details under 'Registrar Info' and 'Important Dates'. The 'Registrar Info' section lists the Name as 'Network Solutions, LLC', Whois as 'whois.networksolutions.com', Referral URL as 'http://networksolutions.com', and Status as 'clientTransferProhibited https://icann.org/epp#clientTransferProhibited'. The 'Important Dates' section shows 'Expires On' as '2025-07-30', 'Registered On' as '2002-07-30', and 'Updated On' as '2024-05-30'. On the right, the 'Site Status' section shows 'Status' as 'Active' and 'Server Type' as 'nginx/1.25.5'. Below this, a 'Suggested Domains for certifiedhacker.com' section lists several domain options with their prices, such as 'certified-hacker.live' for \$3.99. A 'Purchase Selected Domains' button is at the bottom of this list. The footer of the website includes an 'Ads by Google' section with a 'Send feedback' link and a 'Why this ad?' link. The browser's taskbar at the bottom shows various application icons and the system clock indicating '19:15' on '20-03-2025'.

Registrar Info	
Name	Network Solutions, LLC
Whois	whois.networksolutions.com
Referral URL	http://networksolutions.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates	
Expires On	2025-07-30
Registered On	2002-07-30
Updated On	2024-05-30

Site Status	
Status	Active
Server Type	nginx/1.25.5

Suggested Domains for certifiedhacker.com	
<input type="checkbox"/> certified-hacker.live	\$3.99
<input type="checkbox"/> certifiedhackers.live	\$3.99
<input type="checkbox"/> statehacker.live	\$3.99
<input type="checkbox"/> showhacker.live	\$3.99
<input type="checkbox"/> licensehacker.live	\$3.99

Name : Kunal jawale

The screenshot shows the 'Registrar Data' page on who.is. The page displays contact information for the registrar, Perfect Privacy, LLC. The data is organized into two sections: Registrant Contact Information and Administrative Contact Information. Both sections list the same details: Name (PERFECT PRIVACY, LLC), Organization (PERFECT PRIVACY, LLC), Address Line 1 (5335 Gate Parkway care of Network Solutions PO Box 459), Address Line 2 (Jacksonville), City (Jacksonville), State/Province (FL), Postal Code (32256), Country (US), Phone (+1.5707088622), Fax (+1.5707088622), Email (kq9t994x73e@networksolutionsprivateregistration.com), and Full Address (5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, FL, 32256, US). A green button labeled 'Make Private Now' is visible in the top right corner of the data section. Below the data, there is a large blue banner with the text 'Try Our 30 Day Free Trial'. The page also features a search bar at the top right and a navigation menu at the top left.

Registrar Data

We will display stored WHOIS data for up to 30 days.

[Make Private Now](#)

**Registrant Contact Information:**

Name: PERFECT PRIVACY, LLC

Organization: PERFECT PRIVACY, LLC

Address Line 1: 5335 Gate Parkway care of Network Solutions PO Box 459

Address Line 2: Jacksonville

City: Jacksonville

State/Province: FL

Postal Code: 32256

Country: US

Phone: +1.5707088622

Fax: +1.5707088622

Email: kq9t994x73e@networksolutionsprivateregistration.com

Full Address: 5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, FL, 32256, US

**Administrative Contact Information:**

Name: PERFECT PRIVACY, LLC

Organization: PERFECT PRIVACY, LLC

Address Line 1: 5335 Gate Parkway care of Network Solutions PO Box 459

Address Line 2: Jacksonville

City: Jacksonville

State/Province: FL

Postal Code: 32256

Country: US

Phone: +1.5707088622

Fax: +1.5707088622

Email: kq9t994x73e@networksolutionsprivateregistration.com

Full Address: 5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, FL, 32256, US

[Try Our 30 Day Free Trial](#)

Ads by Google

[Send feedback](#) [Why this ad?](#)

The screenshot shows the 'Tech Contact Information' page on who.is. The page displays contact information for the registrar, Perfect Privacy, LLC. The data is organized into two sections: Registrant Contact Information and Tech Contact Information. Both sections list the same details: Name (PERFECT PRIVACY, LLC), Organization (PERFECT PRIVACY, LLC), Address Line 1 (5335 Gate Parkway care of Network Solutions PO Box 459), Address Line 2 (Jacksonville), City (Jacksonville), State/Province (FL), Postal Code (32256), Country (US), Phone (+1.5707088622), Fax (+1.5707088622), Email (kq9t994x73e@networksolutionsprivateregistration.com), and Full Address (5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, FL, 32256, US). A green button labeled 'Make Private Now' is visible in the top right corner of the data section. Below the data, there is a large blue banner with the text 'About the WHOIS Protocol'. The page also features a search bar at the top right and a navigation menu at the top left.

Tech Contact Information

Name: PERFECT PRIVACY, LLC

Organization: PERFECT PRIVACY, LLC

Address Line 1: 5335 Gate Parkway care of Network Solutions PO Box 459

Address Line 2: Jacksonville

City: Jacksonville

State/Province: FL

Postal Code: 32256

Country: US

Phone: +1.5707088622

Fax: +1.5707088622

Email: kq9t994x73e@networksolutionsprivateregistration.com

Full Address: 5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, FL, 32256, US

[About the WHOIS Protocol](#)

- o **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.

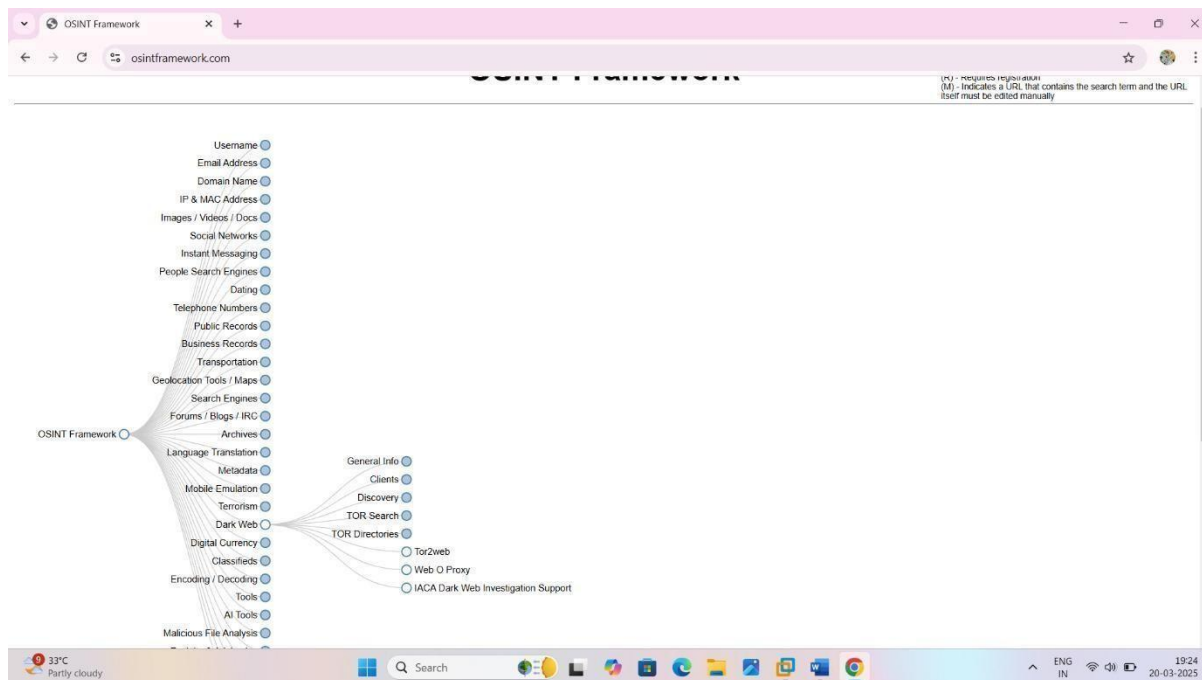
- **CrowdStrike's OSINT methodology:**

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.



- o **emkei.cz** – this tool is very useful to sent fake mail using any mail id. 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

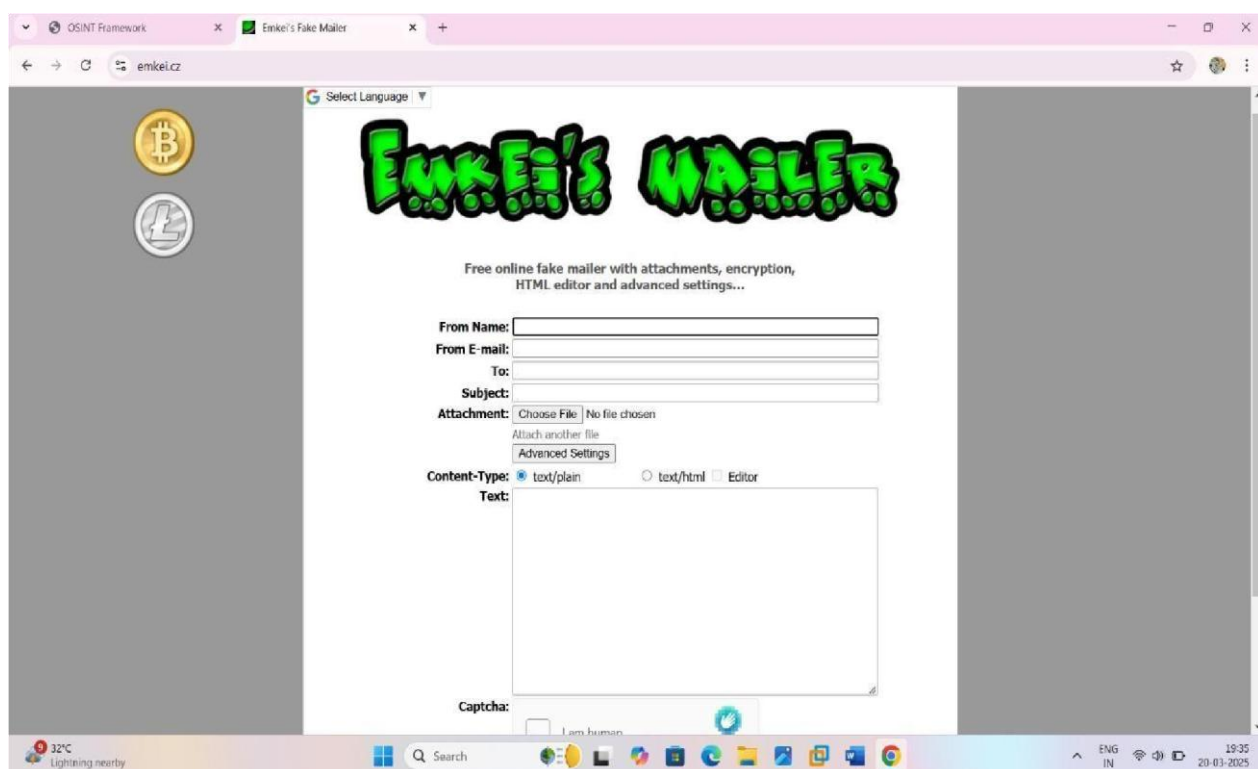
This type of email spoofing can be used for various malicious purposes, including:

- **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.

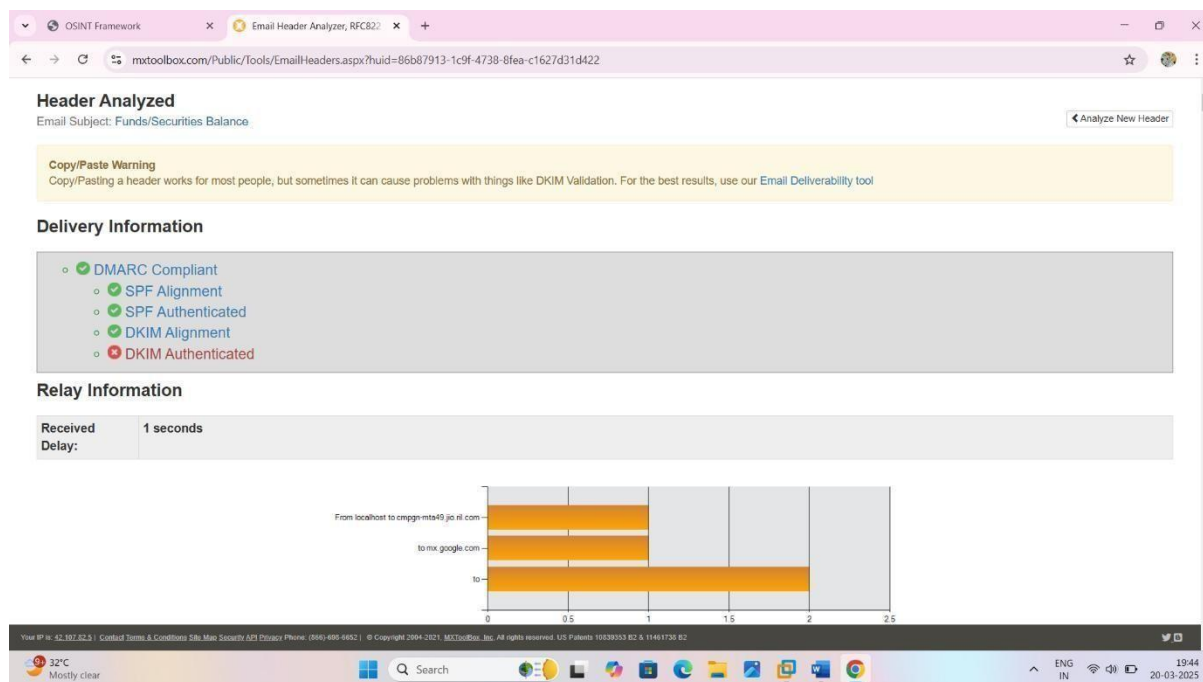
- **"Received:" Lines:**

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..

The screenshot shows the 'Email Header Analyzer' tool interface with the 'Header Name' and 'Header Value' table. The table contains the following data:

Header Name	Header Value
Delivered-To	jawalekunal85@gmail.com
X-Google-Smtp-Source	AGHT+EVseHP9f7wXTdASXclhDAIzbw7bdcRqjEy8tz4gm1tzUProX8UM4jPbIRXyv10DUe2t
X-Received	by 2002.a05.6a00.802.b0.736.ab48.3823 with SMTP id d2e1a72fcca58-7376d5e2d72mr6511600b3a.1.1742432096886, Wed, 19 Mar 2025 17:54:56 -0700 (PDT)
ARC-Seal	i=1, a=rsa-sha256, t=1742432096, cv=none, d=google.com, s=arc-20240605, b=CiUUYEof/nNg2qRhCB80bnYrCCB6T5bEFk8UXmxGr921TIEz+ey7mrSUGAq61c yhWENNipG+N3X93j0XWPVXg527BaQl3jEZ8dFxn0bc +nnHRDV+LNGwTQUuDB+vSRni 4b70zyZtZQPVIEsF0zyjth1TM+horHpOpoQdG+HjU3R5shah3ZrPqnsQK1eafNm shYXDKXR12BybEwRuUSab78Fy02NB5zDL3pOudAyLMuWcCnOZuhJraP8n5KJro1o tMITEhyRX4 1wI4pN8sIC0xTmgdV9qSPhgmdQBvccB9CjERZzhWjccU0AV4ywJ sswy==
ARC-Message-Signature	i=1, a=rsa-sha256, c=relaxed/relaxed, d=google.com, s=arc-20240605, h=subject:to:from:message-id:reply-to:date:mime-version:dkim-signature, bh=shDiOXZl8u5tNWd74j8MmdRFc0cX7E5fDE34XVzw=: fh=wOIXWCunx H7LeWvLGl5tZ9vq7AU59qKbjelCRss=: b=PGKcC0vwyqY1LY8Mh03Yj7K9RGWGGKL2o5E56CCK9x7YXmnPRn4n7WmZVSUK8l +JaWEFQc4IXPKK7S791EzeO1XKZK7RN8chupCD6DNIPqMcKdWJ7v3JTEdXglO6O LLwks uonJBryJnYonV+F4XBUKK61KleltuCiswtyGFv5dkWvOGQJESz4aQ+wjpHN3+dBj evrBqSyyuQVoYu307Xow+MqWYcyx8u6PdFzRZk9m3opiAYK28OpK7g56mHMMTxxm0nV pSBIZIAotKV+pgHw3vAPvSL5EcB5xR PeWHtbZKKuXWkKq2Wa1huB0hrHYw27vY3uDAEt KD5w=: data=google.com
ARC-Authentication-Results	i=1, mx.google.com, dkim=pass header i=@esisc.nse.co.in header s=mtaescisc header b=yaYBI8qO, spf=pass (google.com: domain of nse_alerts@esisc.nse.co.in designates 116.50.98.49 as permitted sender) smtp.mailfrom=nse_alerts@esisc.nse.co.in, dmarc=pass (p=REJECT sp=REJECT dis=NONE) header from=nse.co.in
Return-Path	<nse_alerts@esisc.nse.co.in>
Received-SPF	pass (google.com: domain of nse_alerts@esisc.nse.co.in designates 116.50.98.49 as permitted sender) client-ip=116.50.98.49;
Authentication-Results	mx.google.com, dkim=pass header i=@esisc.nse.co.in header s=mtaescisc header b=yaYBI8qO, spf=pass (google.com: domain of nse_alerts@esisc.nse.co.in designates 116.50.98.49 as permitted sender) smtp.mailfrom=nse_alerts@esisc.nse.co.in, dmarc=pass (p=REJECT sp=REJECT dis=NONE) header from=nse.co.in
DKIM-Signature	v=1, a=rsa-sha256, c=relaxed/relaxed, d=esisc.nse.co.in, i=@esisc.nse.co.in, q=dns/txt, s=mtaescisc, t=1742432094, h=mime-version:date:reply-to:message-id:from:to:subject:content-type:from, bh=shDiOXZl8u5tNWd74j8MmdRFc0cX7E5fDE34XVzw=: b=yaYBI8qOaVH5yqteFEb73EX5lQnCyMoBmGYWAWsNzJmWfVmeWjvcj5VvQ2wpa5Zx Oc38A85y9wC8YP4JsiNuYcnAbva5ahuPQXXKcMOGJKmzztGCJXOPp9gYBSxdmNeGz m3pNzT +DnYx4Q7s+djSK3j4+mI0E1nVH4=
Mime-Version	1.0
Date	Thu, 20 Mar 2025 06:24:54 +0530
Reply-To	nse_alerts@esisc.nse.co.in
Message-ID	<nseil0195ae87-aae2-7d55-8adb-d89f70bd4fa5/transactional/swift/nse_alerts@esisc.nse.co.in>
From	nse_alerts <nse_alerts@nse.co.in>
To	jawalekunal85@gmail.com

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](https://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

The screenshot shows the IP2LOCATION website interface. At the top, there's a navigation bar with links like Home, Solutions, Products, Pricing, Resources, and a Log In button. Below the navigation bar, the main heading reads "Understanding Internet traffic via IP lookup" with a subtext "Experience the IP address lookup to access your visitors' detailed geolocation information". A search bar contains the IP address "42.180.224.192" and a "LOOK UP" button. The results are displayed in a grid format with the following data:

<b>Your IP Address</b> 42.180.224.192	<b>Country</b> India	<b>Region</b> Maharashtra	<b>City</b> Pune
<b>Coordinates</b> 18.519663, 73.854508	<b>ISP</b> Vodafone Idea Ltd	<b>Time Zone</b> UTC +05:30	<b>Local Time</b> 2025-03-22 12:49:07
<b>Domain</b> vodafoneidea.com	<b>Net Speed</b> DSL	<b>IDD &amp; Area Code</b> (91) 020	<b>ZIP Code</b> 412415
<b>Weather Station</b> Poona (INXX0164)	<b>Mobile Carrier</b> Vodafone IN	<b>Mobile Country Code</b> 404	<b>Mobile Network Code</b> 01/05/11/13/15/20/27/30/43/46/60/84/86/88/66/67/750/751/752/753
<b>Elevation</b> 555m	<b>Usage Type</b> (MOB) Mobile ISP	<b>Address Type</b> (U) Unicast	<b>Category</b> (IAB19-6) Cell Phones
<b>District</b> Pune Division	<b>ASN</b> AS38266 Vodafone Idea Ltd. (VIL)	<b>Is Proxy</b> No	<b>Proxy Type</b> -
<b>Proxy ASN</b> -	<b>Security Threat</b> -	<b>Proxy Last Seen</b> -	<b>Proxy Provider</b> -

**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:**

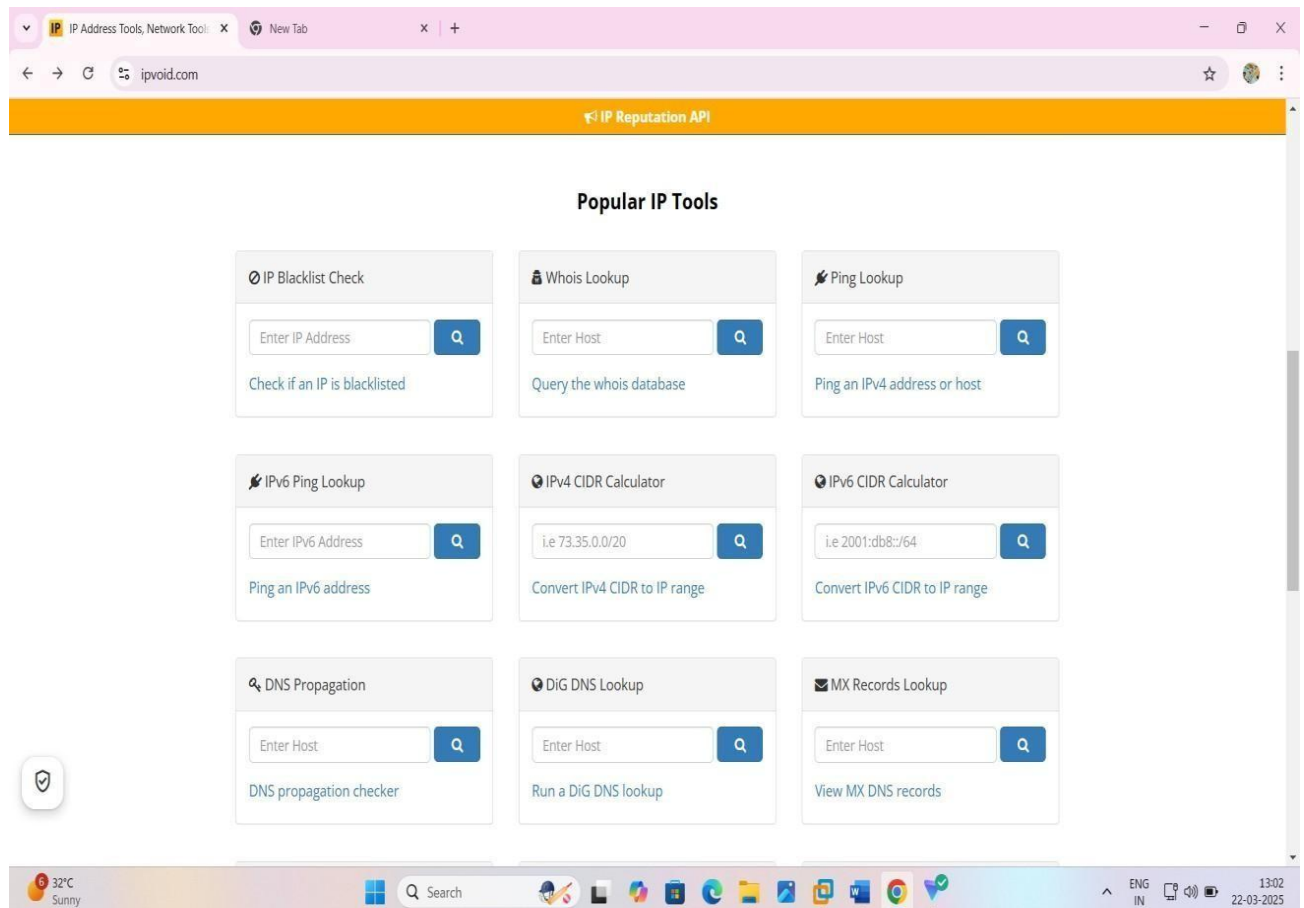
The tool can also detect if an IP address is associated with a proxy or Tor network, which are often used for anonymous browsing and can be associated with malicious activities.

- **Threat Intelligence APIs:**

Name : Kunal jawale

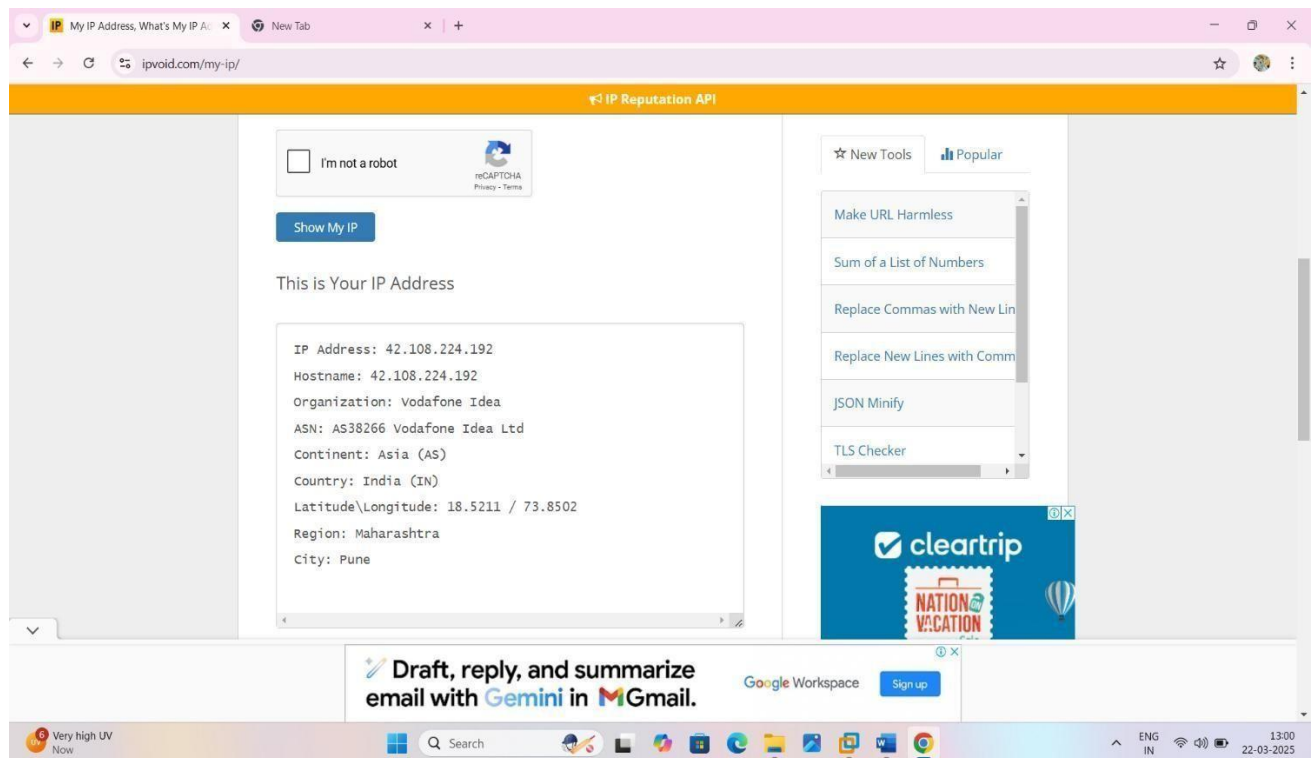
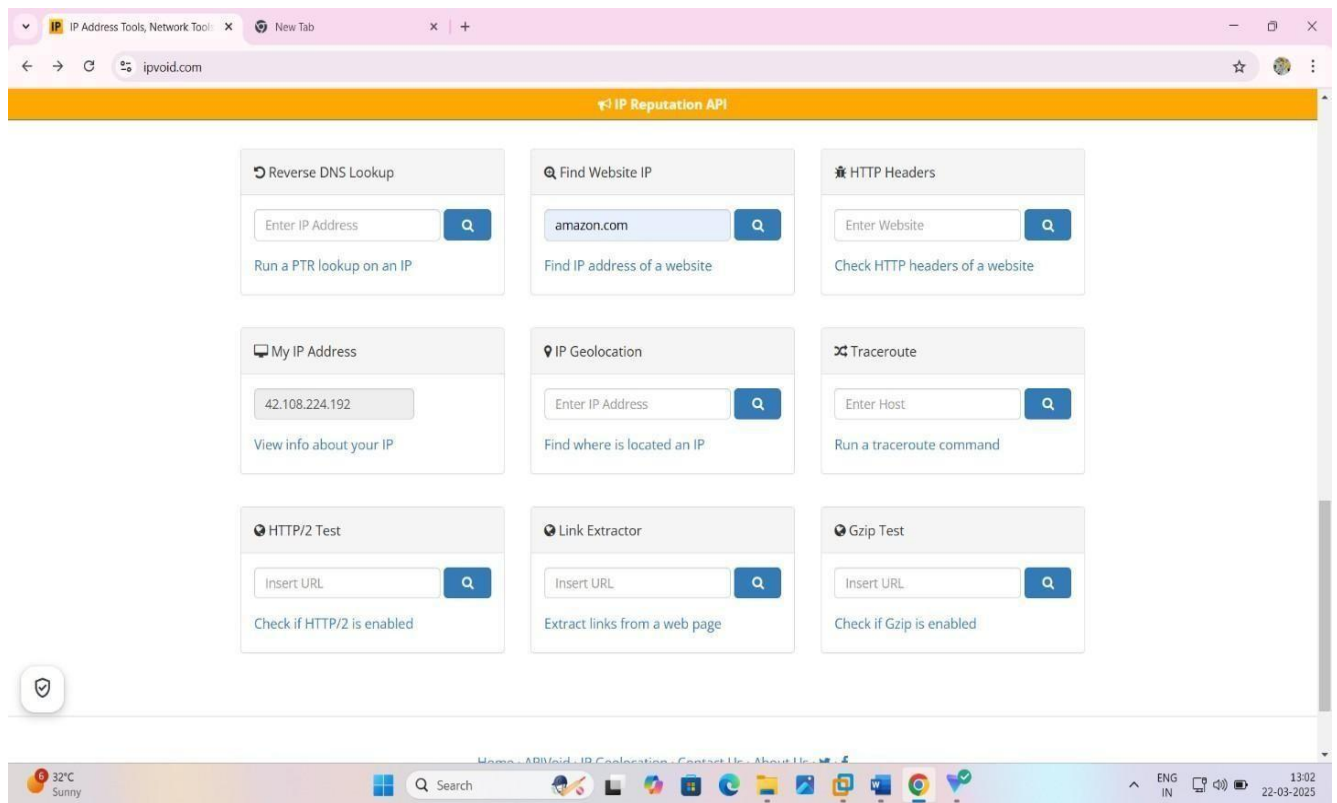
IPVoid offers APIs that allow developers to integrate their threat intelligence capabilities into their systems. These APIs can be used to automatically detect malicious IP addresses and other threats.

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



- o **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. :

MITRE | ATT&CK®

Assets | MITRE ATT&CK®

Overview

Application Server

Control Server

Data Gateway

Data Historian

Field I/O

Human-Machine Interface (HMI)

Intelligent Electronic Device (IED)

Jump Host

Programmable Logic Controller (PLC)

Remote Terminal Unit (RTU)

Routers

Safety Controller

Virtual Private Network (VPN)

Although originally represented under the platform field in ATT&CK, Assets are distinctly separate from platforms. Platforms generally describe the operating system or application (i.e., Microsoft Windows) while Assets represent the device which includes considerations for hardware, software, architecture, and intended function. Assets may leverage platforms to describe a device's commonly observed operating system.

Assets: 14

ID	Name	Domain	Description
A0008	Application Server	ICS	Application servers are used across many different sectors to host various diverse software applications necessary to supporting the ICS. Example functions can include data analytics and reporting, alarm management, and the management/coordination of different control servers. The application server typically runs on a modern server operating system (e.g., MS Windows Server).
A0007	Control Server	ICS	Control servers are typically a software platform that runs on a modern server operating system (e.g., MS Windows Server). The server typically uses one or more automation protocols (e.g., Modbus, DNP3) to communicate with the various low-level control devices such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs). The control server also usually provides an interface/network service to connect with an HMI.
A0009	Data Gateway	ICS	Data Gateway is a device that supports the communication and exchange of data between different systems, networks, or protocols within the ICS. Different types of data gateways are used to perform various functions, including: <ul style="list-style-type: none"><li><b>Protocol Translation:</b> Enable communication to devices that support different or incompatible protocols by translating information from one protocol to another.</li><li><b>Media Converter:</b> Convert data across different Layer 1 and 2 network protocols / mediums, for example, converting from Serial to Ethernet.</li><li><b>Data Aggregation:</b> Collect and combine data from different devices into one consistent format and</li></ul>

MITRE | ATT&CK®

MITRE ATT&CK®

Get Started

Take a Tour

Contribute

Blog

FAQ

Random Page

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world – by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

layout: side

show sub-techniques

hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (3)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing		Boot or Logon Autostart Execution (14)		BITS Jobs	Credentials from Password	Browser Information Discovery	Lateral Tool	Audio Capture



Name : Kunal jawale

The screenshot shows the MITRE ATT&CK website, specifically the 'Enterprise Techniques' section. The page has a red header with the MITRE logo and navigation links. A sidebar on the left lists various technique categories like Reconnaissance, Resource Development, Initial Access, etc. The main content area is titled 'Enterprise Techniques' and includes a brief introduction. Below this is a table with three columns: ID, Name, and Description. The table lists three techniques: T1548 (Abuse Elevation Control Mechanism), T1548.001 (Setuid and Setgid), and T1548.002 (Bypass User Account Control). Each technique has a detailed description of how an adversary might use it. The bottom of the page shows a Windows taskbar with the date 22-03-2025 and time 13:13.

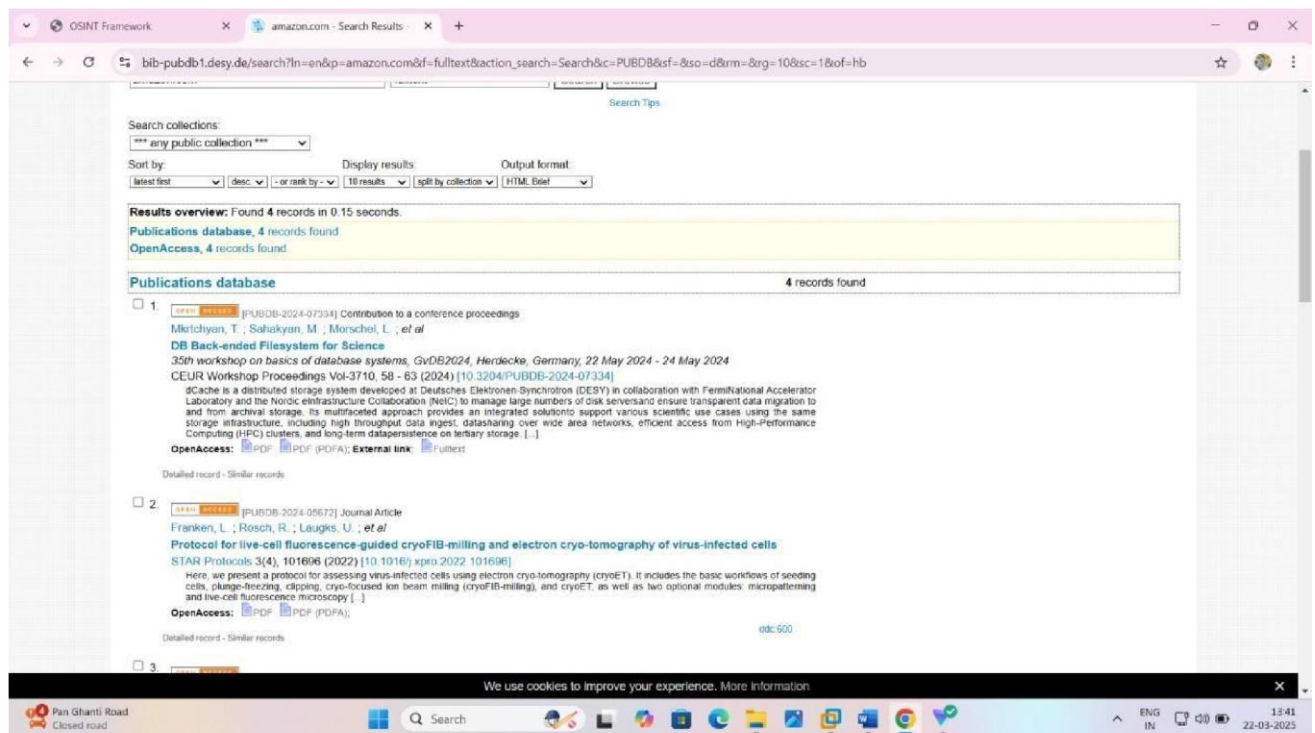
ID	Name	Description
T1548	Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.
.001	Setuid and Setgid	An adversary may abuse configurations where an application has the setuid or setgid bits set in order to get code running in a different (and possibly more privileged) user's context. On Linux or macOS, when the setuid or setgid bits are set for an application binary, the application will run with the privileges of the owning user or group respectively. Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them may not have the specific required privileges.
.002	Bypass User Account Control	Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.

- o **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.

The screenshot shows the WhatWeb website, which is a next-generation web scanner. The page features a large, stylized 'WHATWEB' logo at the top. Below the logo, there is a section titled 'WhatWeb is a next generation web scanner.' followed by a description of what the tool recognizes. A search bar with the text 'Enter a domain to analyze:' and a 'Go' button is present. Below the search bar, there are links for 'Download' and 'Wiki'. The main content area displays the results of a scan for the domain 'http://certifiedhacker.com'. The results are shown in a code block, listing various technologies detected, such as Apache, Country[UNITED STATES][US], HTTPServer[Apache], IP[162.241.216.11], RedirectLocation[https://certifiedhacker.com/], Title[301 Moved Permanently], https://certifiedhacker.com/ [200 OK] Country[UNITED STATES][US], HTTPServer[nginx/1.25.5], IP[162.241.216.11], JQuery[1.4], Meta-Authn[Parallelus], PasswordField[RevealPassword], Script[text/javascript], Title[Certified Hacker], UncommonHeaders[host-header,x-server-cache,x-proxy-cache], and nginx[1.25.5]. The bottom of the page shows a Windows taskbar with the date 22-03-2025 and time 13:38.

- **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 :

```
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-leafia.net.unifiedlayer.com [162.144.240.127]
 19  462 ms  509 ms  511 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

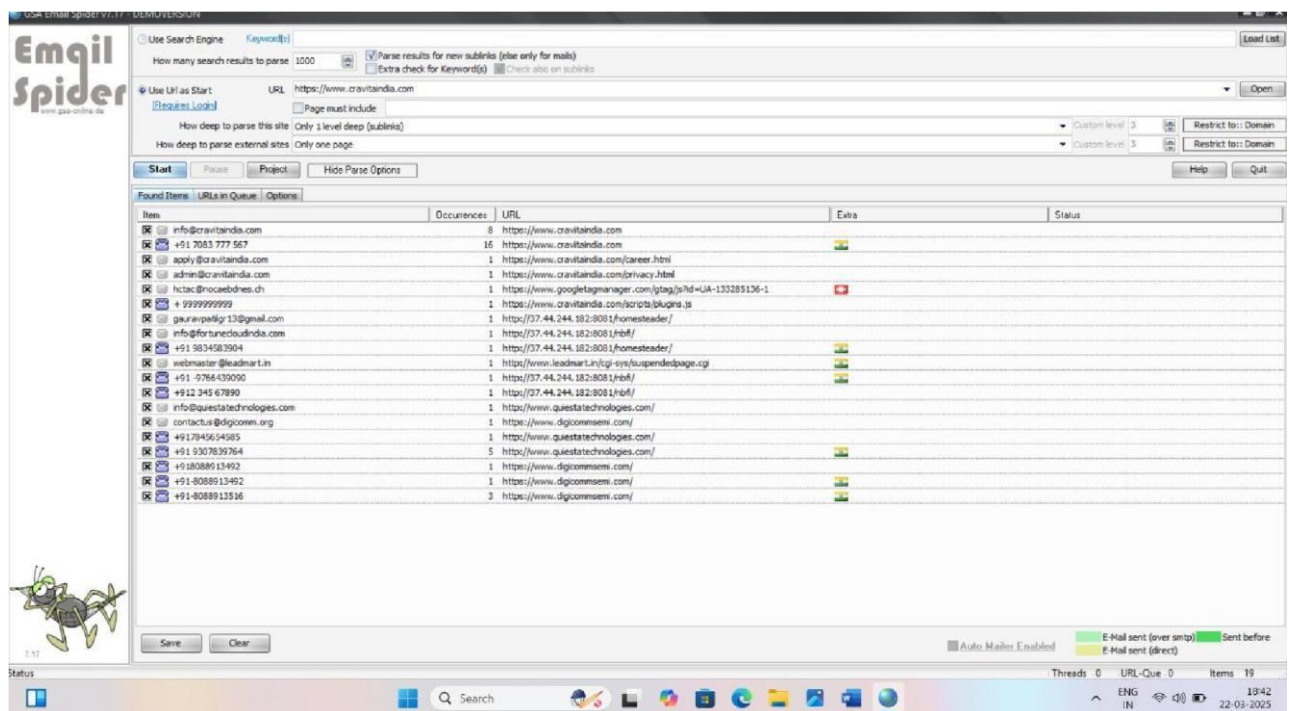
C:\Users\HP>
```

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

## 2 Angry IP scanner

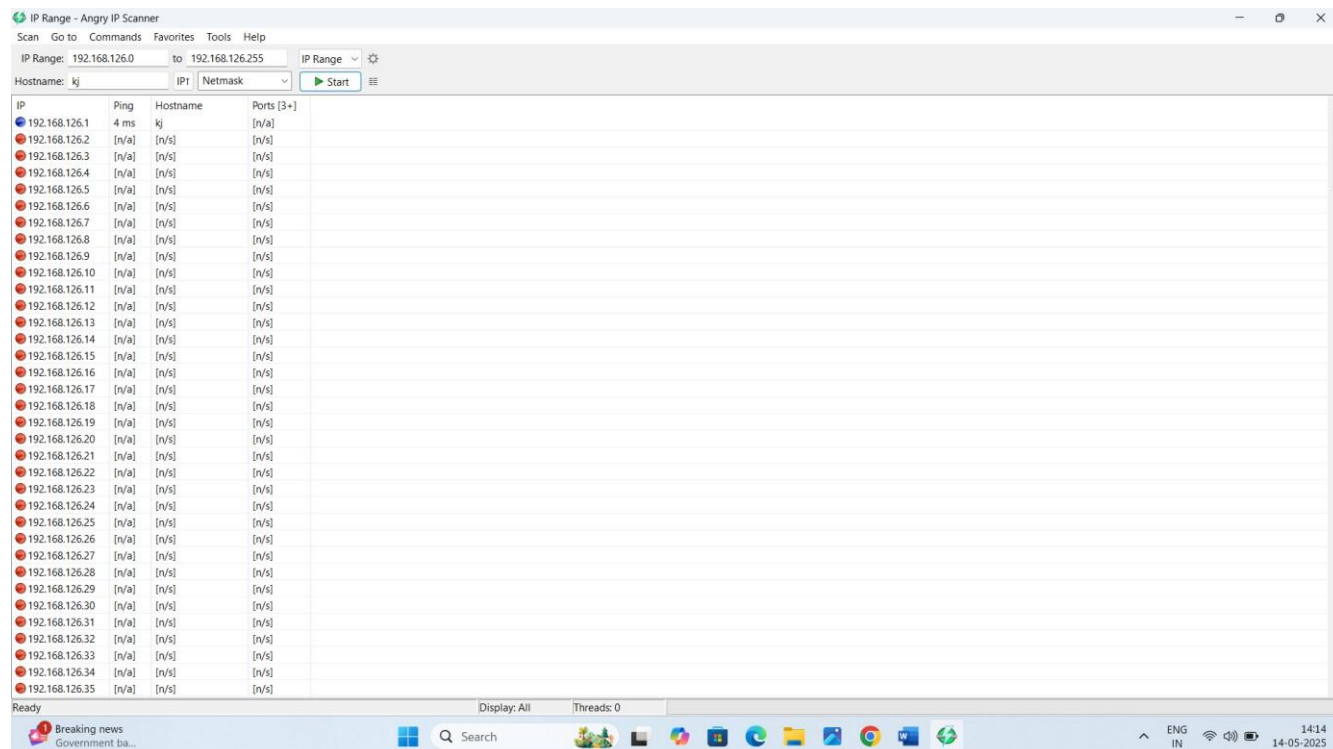
- 1 **GSA email spider** :- The GSA Email Spider is collecting E-Mails as well as phone and fax numbers from websites. It can locate websites by keywords using search engines or when you import or add URLs to parse.

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 .

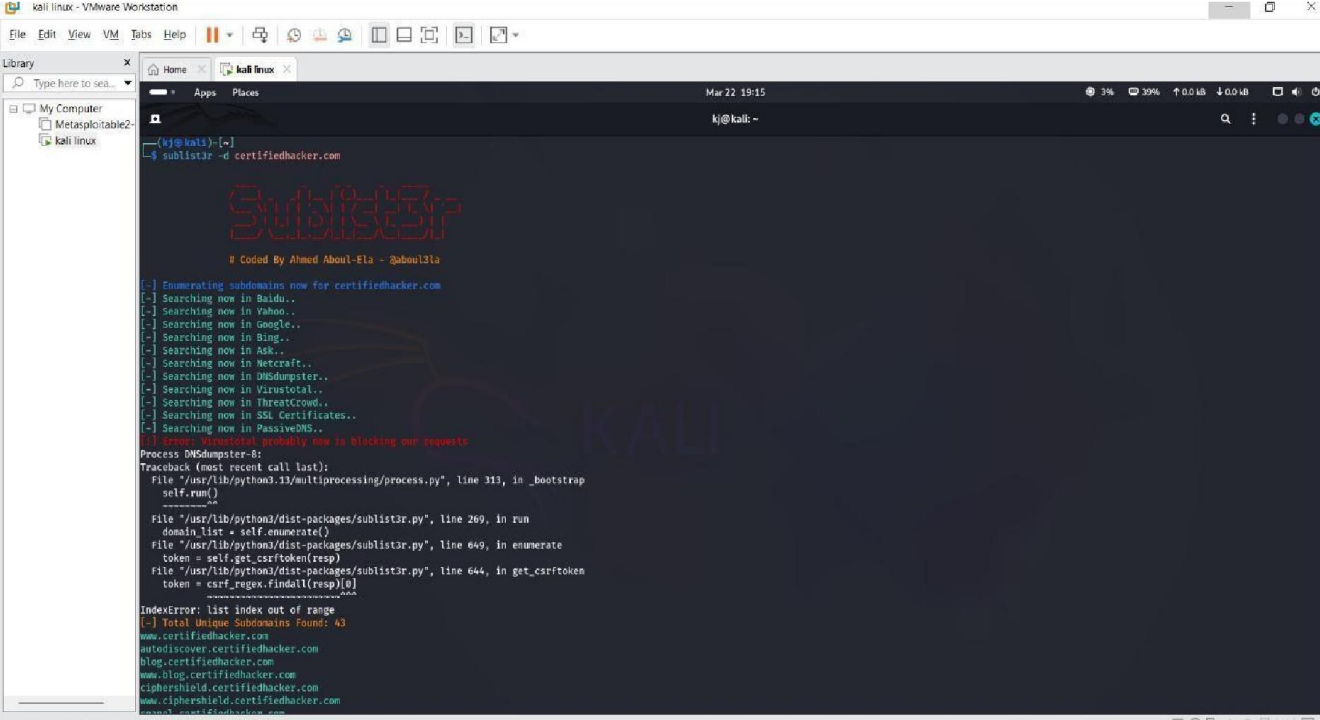
- o **Sublist3r** – this tool is used for manual and automated subdomain enumeration , this is very Useful to find subdomains for a given domain: **Command is :**

**Sublist3r -d ( domain name )**

**-d** is used for domain



Name : Kunal jawale

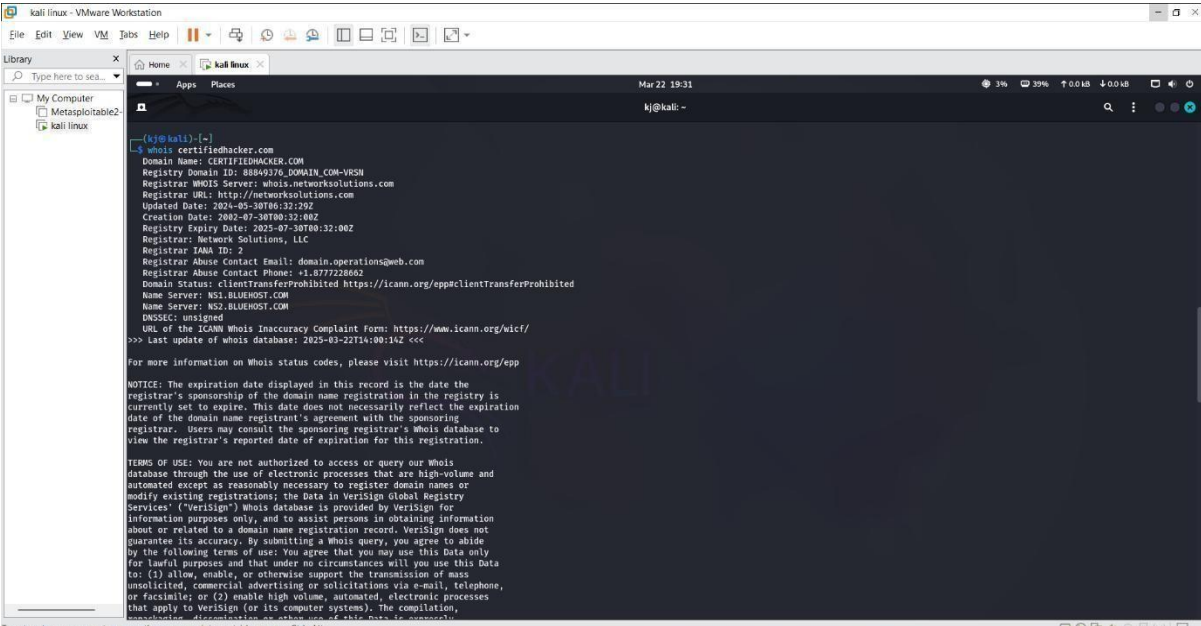


```
kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2
kali linux
Home
Apps
Places
Mar 22 19:15
k@kali: ~
(kali@kali) ~$ sublist3r -d certifiedhacker.com

Sublist3r
Coded By Ahmed Aboul-El* @aboul3la

[-] Enumerating subdomains now for certifiedhacker.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in Threatcrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Error: VirusTotal probably now is blocking our requests
Process DNSdumpster-8
Traceback (most recent call last):
  File "/usr/lib/python3.11/multiprocessing/process.py", line 113, in _bootstrap
    self.run()
  File "/usr/lib/python3.11/multiprocessing/process.py", line 136, in run
    self._target(*self._args, **self._kwargs)
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    domain_list = self.enumerate()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
    token = self.get_csrf_token(resp)
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrf_token
    token = csrf_regex.findall(resp)[0]
IndexError: list index out of range
[-] Total Unique Subdomains Found: 43
www.certifiedhacker.com
autodiscover.certifiedhacker.com
blog.certifiedhacker.com
www.blog.certifiedhacker.com
ciphershield.certifiedhacker.com
www.ciphershield.certifiedhacker.com
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```

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



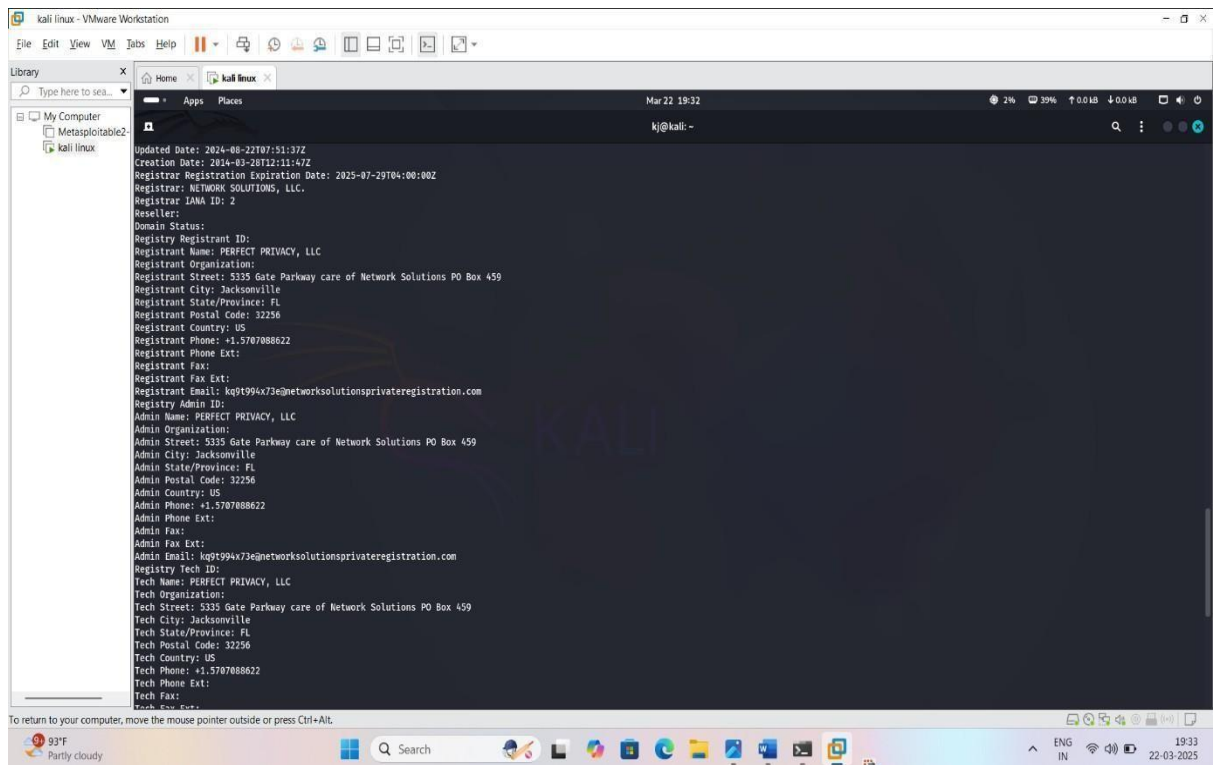
```
kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2
kali linux
Home
Apps
Places
Mar 22 19:31
k@kali: ~
(kali@kali) ~$ whois certifiedhacker.com
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88649376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2024-05-30T06:32:29Z
Creation Date: 2002-07-30T00:32:00Z
Registry Expiry Date: 2025-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: domain.operations@web.com
Registrar Abuse Contact Phone: +1.877.228.6602
Domain Status: clientTransferProhibited https://icann.org/epp/clientTransferProhibited
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-03-22T14:00:14Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
distribution, use, or reproduction of this Data is prohibited.
```

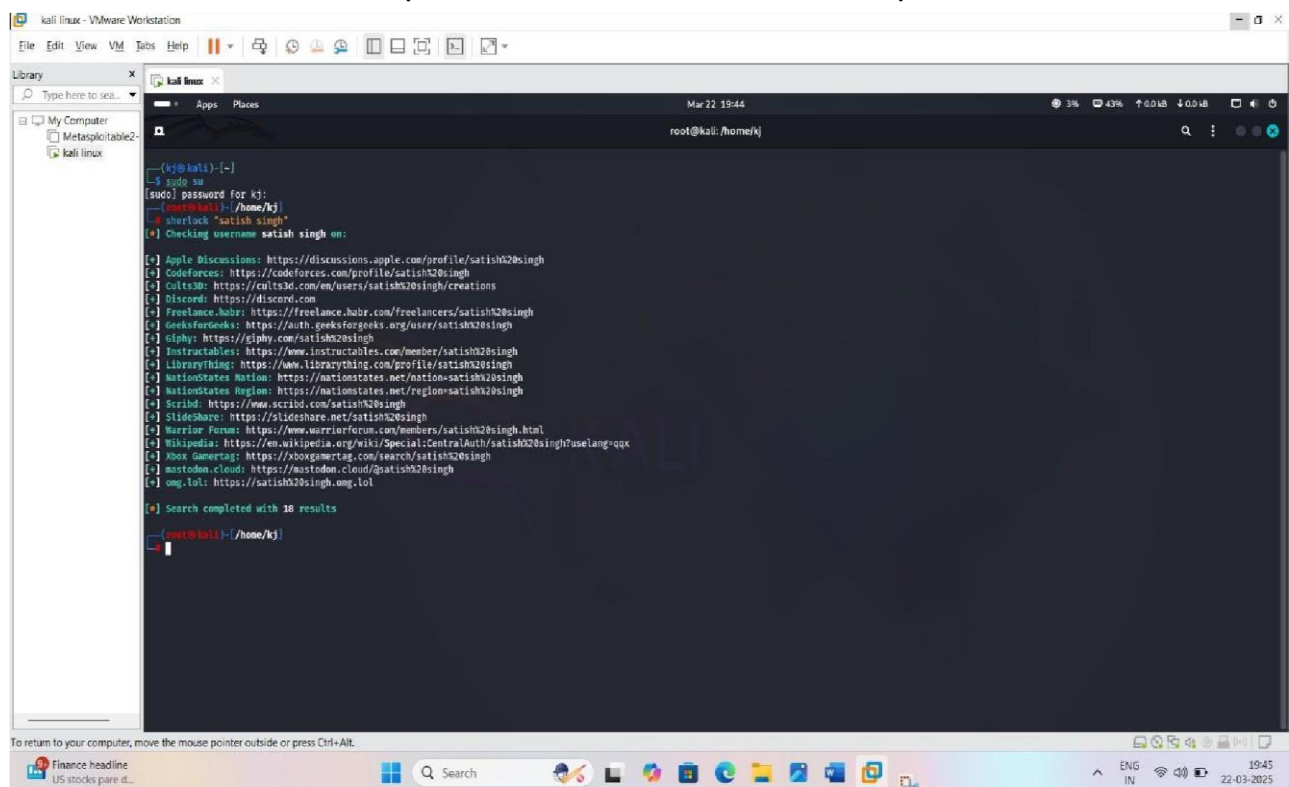
Name : Kunal jawale



```
kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitabie2
kali linux
Mar 22 19:32
kj@kali: ~
Updated Date: 2024-08-22T07:51:37Z
Creation Date: 2014-03-26T12:11:47Z
Registrar Registration Expiration Date: 2025-07-29T04:00:00Z
Registrar: NETWORK SOLUTIONS, LLC.
Registrant IANA ID: 2
Reseller:
Domain Status:
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707088622
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: kq01994x73e@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Admin City: Jacksonville
Admin State/Province: FL
Admin Postal Code: 32256
Admin Country: US
Admin Phone: +1.5707088622
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: kq01994x73e@networksolutionsprivateregistration.com
Registry Tech ID:
Tech Name: PERFECT PRIVACY, LLC
Tech Organization:
Tech Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Tech City: Jacksonville
Tech State/Province: FL
Tech Postal Code: 32256
Tech Country: US
Tech Phone: +1.5707088622
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```

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

**Command :** sherlock ( name or number or mail id )



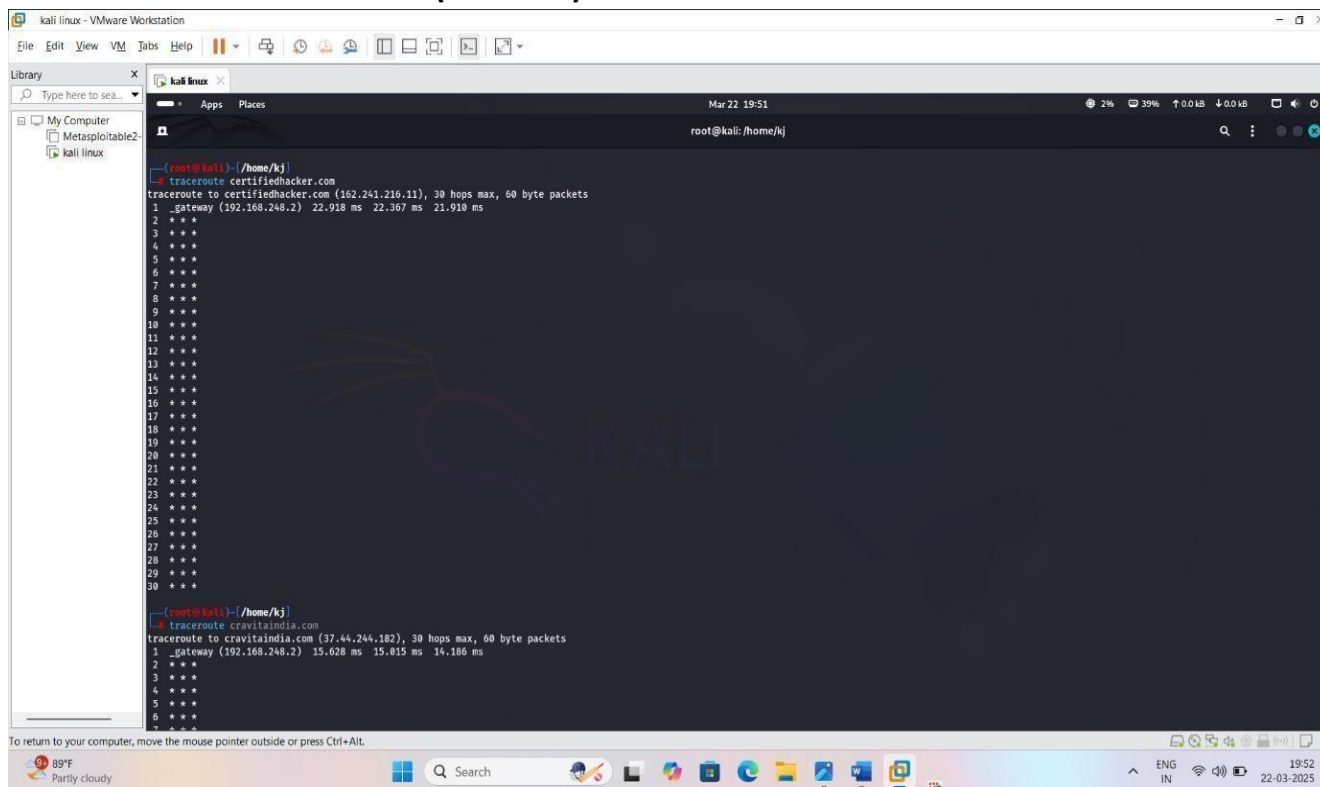
```
kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitabie2
kali linux
Mar 22 19:44
root@kali: /home/kj
(kj@kali)~$ sudo su
[sudo] password for kj:
root@kali: /home/kj
root@kali:~# sherlock "satish singh"
[*] Checking username satish singh on:
[*] Apple Discussions: https://discussions.apple.com/profile/satish20singh
[*] Codeforces: https://codeforces.com/profile/satish20singh
[*] Cults3d: https://cults3d.com/en/users/satish20singh/creations
[*] Discord: https://discord.com
[*] Freelance.habr: https://freelance.habr.com/freelancers/satish20singh
[*] GeeksforGeeks: https://auth.geeksforgeeks.org/user/satish20singh
[*] Github: https://github.com/satish20singh
[*] Instructables: https://www.instructables.com/member/satish20singh
[*] LibraryThing: https://www.librarything.com/profile/satish20singh
[*] NationStates Nation: https://nationstates.net/region=satish20singh
[*] NationStates Region: https://nationstates.net/region=satish20singh
[*] Scribd: https://www.scribd.com/satish20singh
[*] SlideShare: https://slideshare.net/satish20singh
[*] Warrior Forum: https://www.warriorforum.com/members/satish20singh.html
[*] Wikipedia: https://en.wikipedia.org/wiki/Special:CentralAuth/satish20singh?uselang=qqx
[*] Xbox Gamertag: https://xboxgamertag.com/search/satish20singh
[*] mastodon.cloud: https://mastodon.cloud/@satish20singh
[*] omg.lol: https://satish20singh.omg.lol
[*] Search completed with 38 results
root@kali:~#
```



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)**



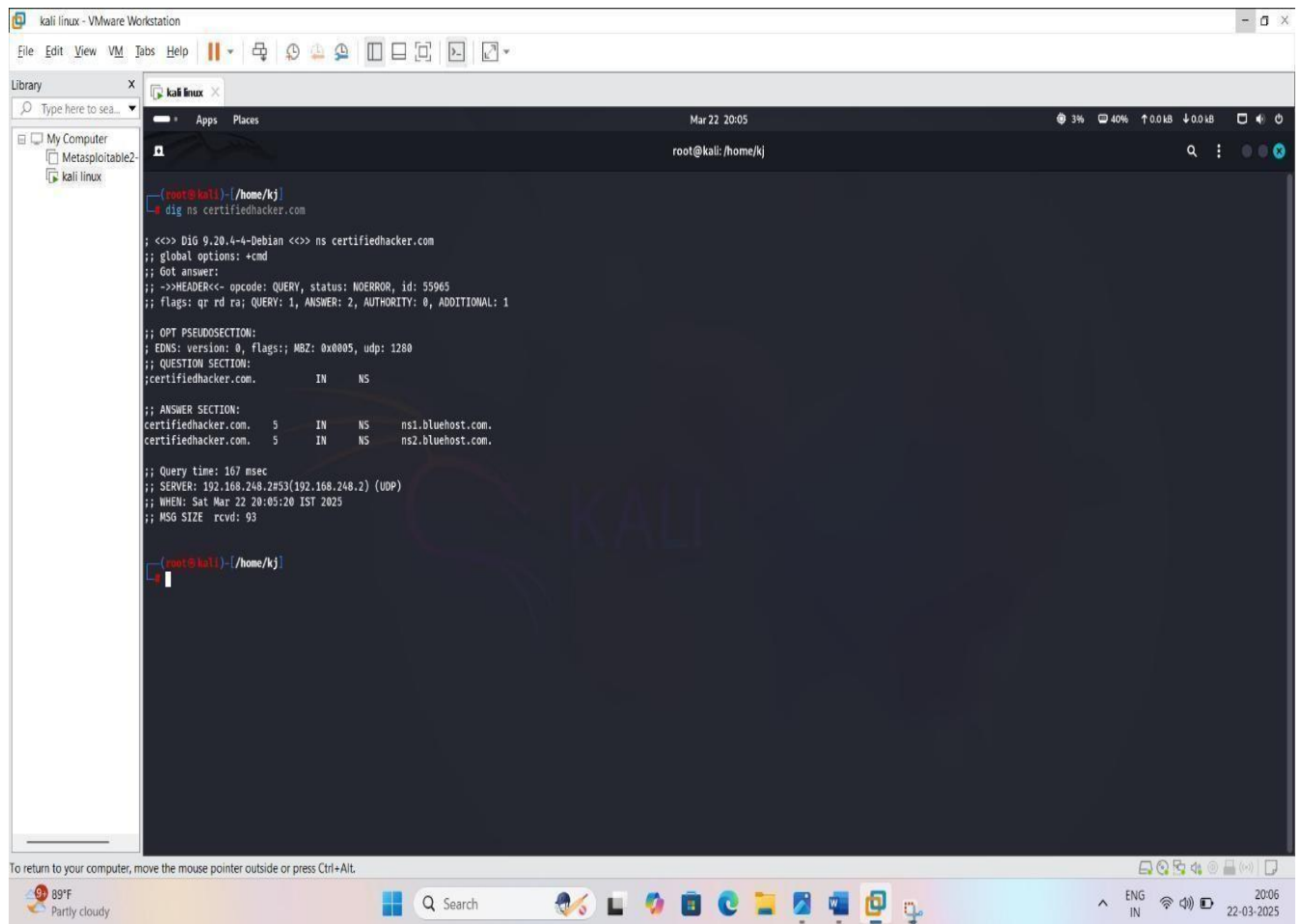
```
root@kali: /home/kj
traceroute certifiedhacker.com
traceroute to certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1 _gateway (192.168.248.2)  22.918 ms  22.367 ms  21.918 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

root@kali: /home/kj
traceroute cravitaIndia.com
traceroute to cravitaIndia.com (37.44.244.182), 30 hops max, 60 byte packets
 1 _gateway (192.168.248.2)  15.628 ms  15.015 ms  14.186 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
```

## 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



The screenshot shows a Kali Linux terminal window with the following output for the command `dig ns certifiedhacker.com`:

```
(root@kali)-[/home/kj]
└─$ dig ns certifiedhacker.com

;<> DiG 0.20.4-Debian <> ns certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 55965
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: 0, HBZ: 0x0005, udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com.      IN      NS

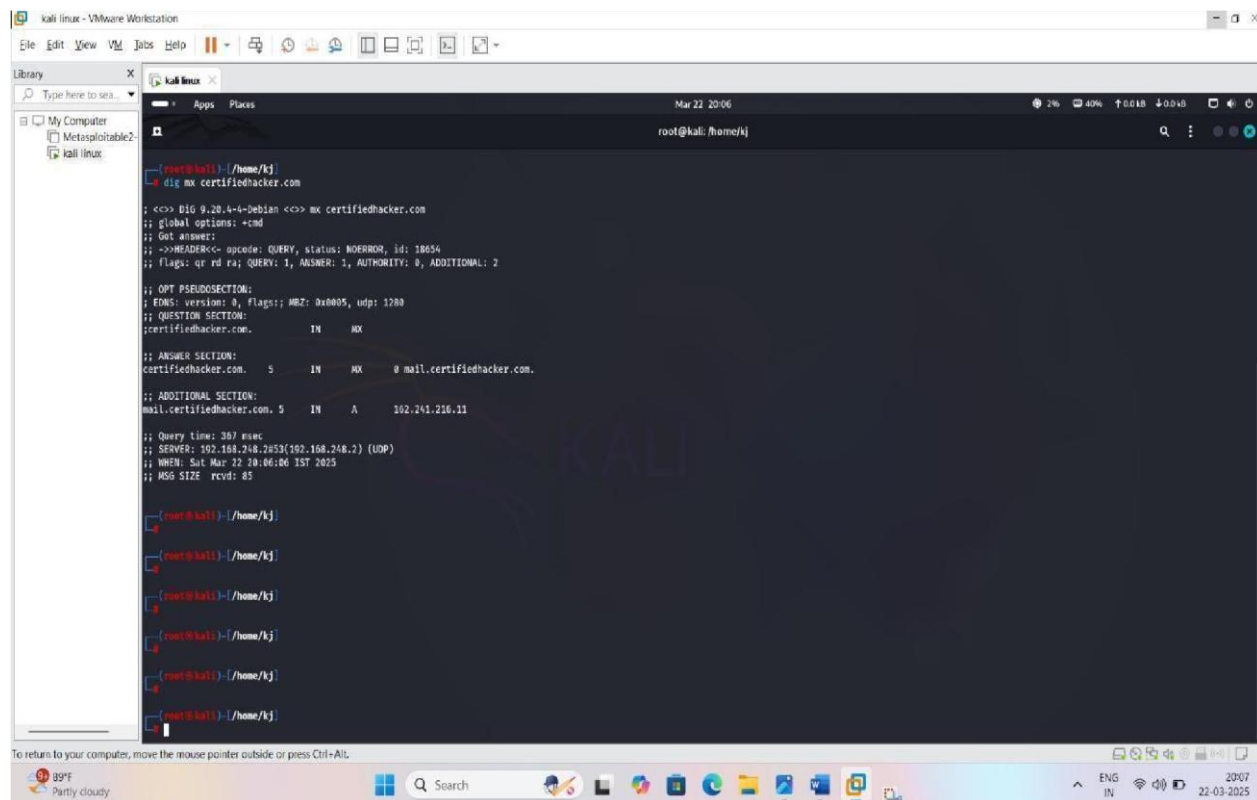
;; ANSWER SECTION:
certifiedhacker.com.  5      IN      NS      ns1.bluehost.com.
certifiedhacker.com.  5      IN      NS      ns2.bluehost.com.

;; Query time: 167 msec
;; SERVER: 192.168.248.2#53(192.168.248.2) (UDP)
;; WHEN: Sat Mar 22 20:05:20 IST 2025
;; MSG SIZE rcvd: 93

(root@kali)-[/home/kj]
```

. **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



```
root@kali: ~/home/kj
# dig mx certifiedhacker.com

;<>> Dig 9.20.4-4-Debian <>> mx certifiedhacker.com
;; global options: +cmd
;; Got answer:
;;->HEADER<<- opcode: QUERY, status: NOERROR, id: 18654
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version 0, flags: 0, MBZ: 0x0000, udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com.      IN      MX

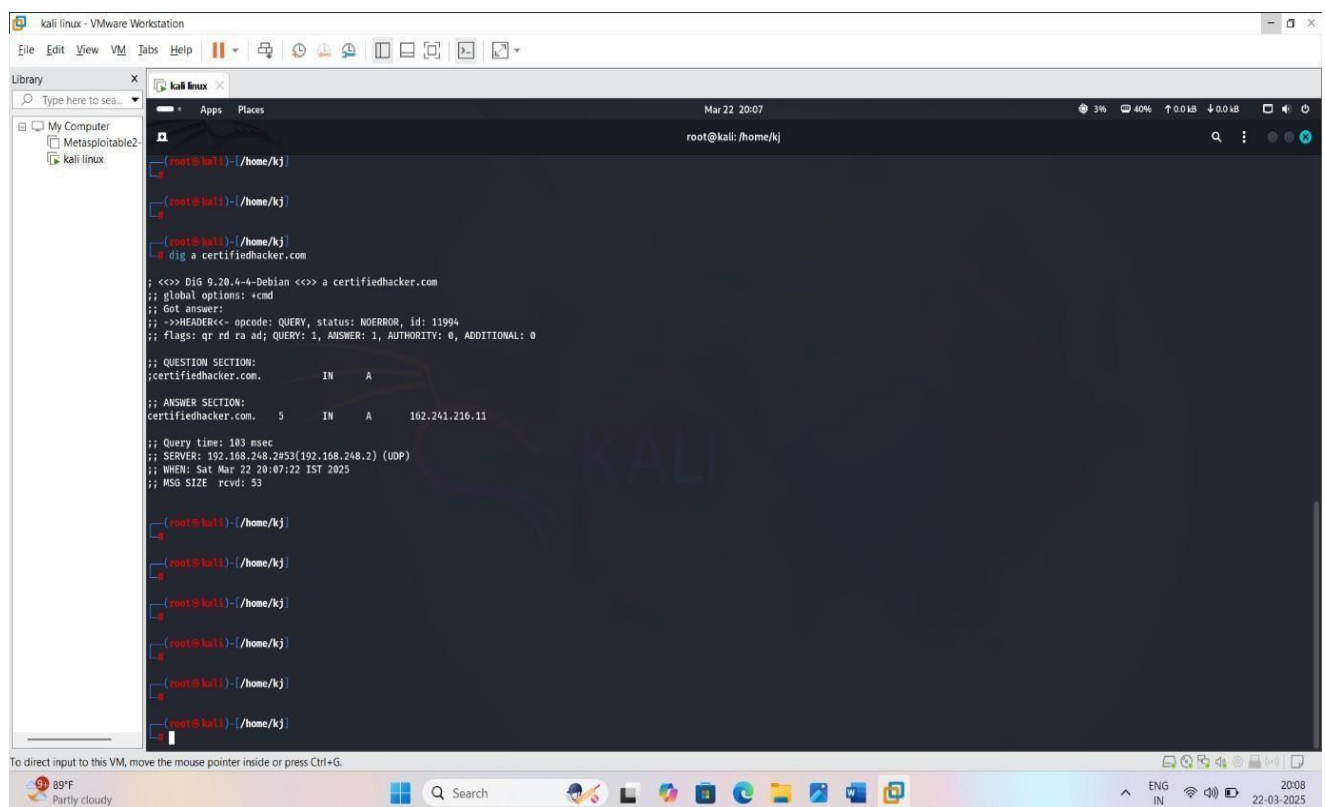
;; ANSWER SECTION:
certifiedhacker.com.      5       IN      MX      0 mail.certifiedhacker.com.

;; ADDITIONAL SECTION:
mail.certifiedhacker.com. 5       IN      A       102.241.216.11

;; Query time: 387 msec
;; SERVER: 192.168.248.2#53(192.168.248.2) (UDP)
;; WHEN: Sat Mar 22 20:06:06 IST 2025
;; MSG SIZE rcvd: 85

root@kali:~/home/kj
root@kali:~/home/kj
root@kali:~/home/kj
root@kali:~/home/kj
root@kali:~/home/kj
root@kali:~/home/kj
```

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



```
root@kali:~/home/kj
# dig a certifiedhacker.com

;<>> Dig 9.20.4-4-Debian <>> a certifiedhacker.com
;; global options: +cmd
;; Got answer:
;;->HEADER<<- opcode: QUERY, status: NOERROR, id: 11994
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

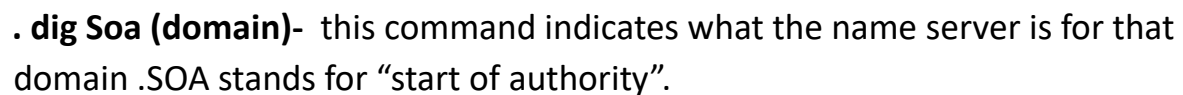
;; QUESTION SECTION:
;certifiedhacker.com.      IN      A

;; ANSWER SECTION:
certifiedhacker.com.      5       IN      A       102.241.216.11

;; Query time: 183 msec
;; SERVER: 192.168.248.2#53(192.168.248.2) (UDP)
;; WHEN: Sat Mar 22 20:07:22 IST 2025
;; MSG SIZE rcvd: 53

root@kali:~/home/kj
root@kali:~/home/kj
root@kali:~/home/kj
root@kali:~/home/kj
root@kali:~/home/kj
root@kali:~/home/kj
```

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



Name : Kunal jawale

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

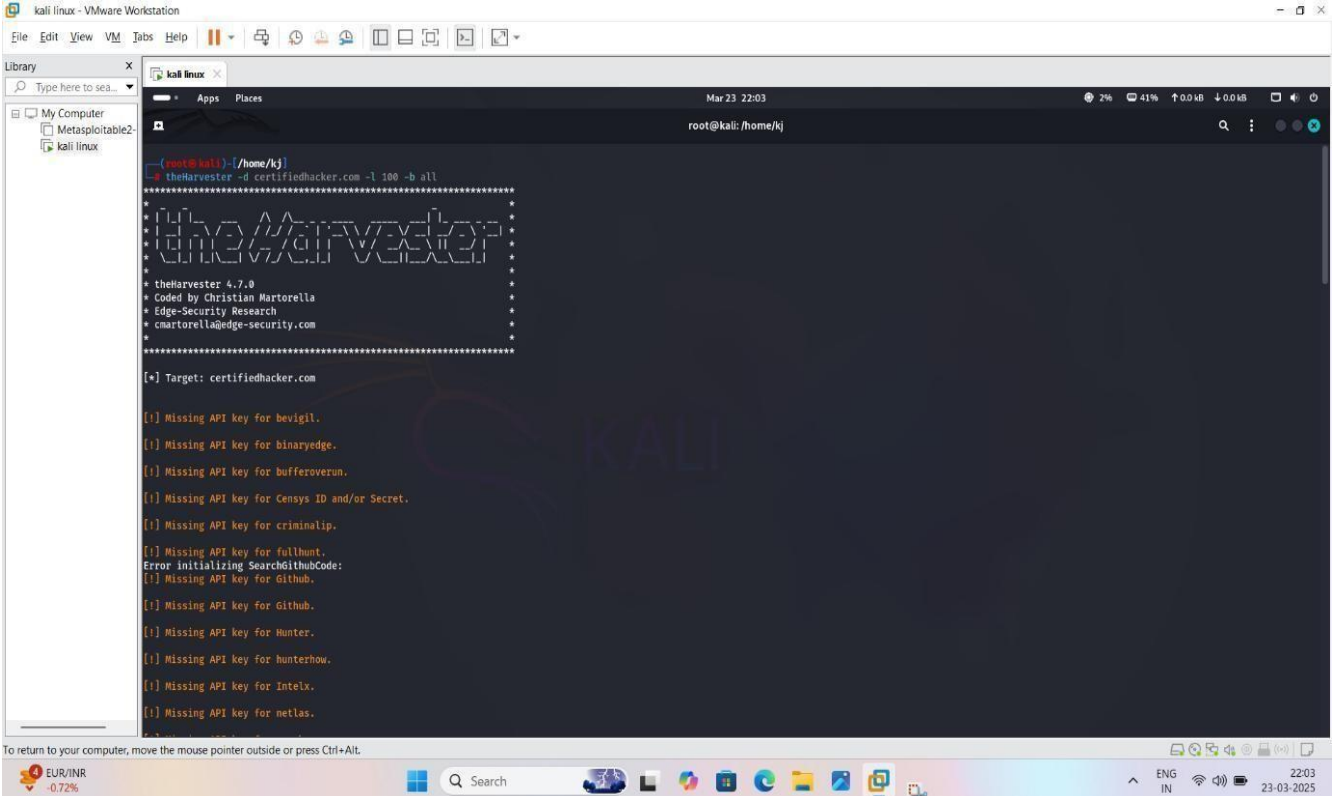
- . search engines (google,bing,yahoo)
- . social media (LinkedIn,Twitter)
- . Public database (shodan , PGP key servers)
- . threat intelligence platforms

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

*-d for domain name*

*-l for limit*

*-b for source ( google,yahoo,Baidu)*



```
(root@kali) [/home/kj]
theHarvester -d certifiedhacker.com -l 100 -b all
*****
* theHarvester *
* theHarvester 4.7.0 *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorell@edge-security.com *
*****

[*] Target: certifiedhacker.com

[!] Missing API key for bevigil.
[!] Missing API key for binaryedge.
[!] Missing API key for bufferoverrun.
[!] Missing API key for censys ID and/or Secret.
[!] Missing API key for criminalip.
[!] Missing API key for fullhunt.
Error Initializing Search6GithubCode:
[!] Missing API key for Github.
[!] Missing API key for Hunter.
[!] Missing API key for hunterhow.
[!] Missing API key for intelx.
[!] Missing API key for metlas.
```

*. here are some types of command for theHarvester*

1 . gather mails and subdomains from bing

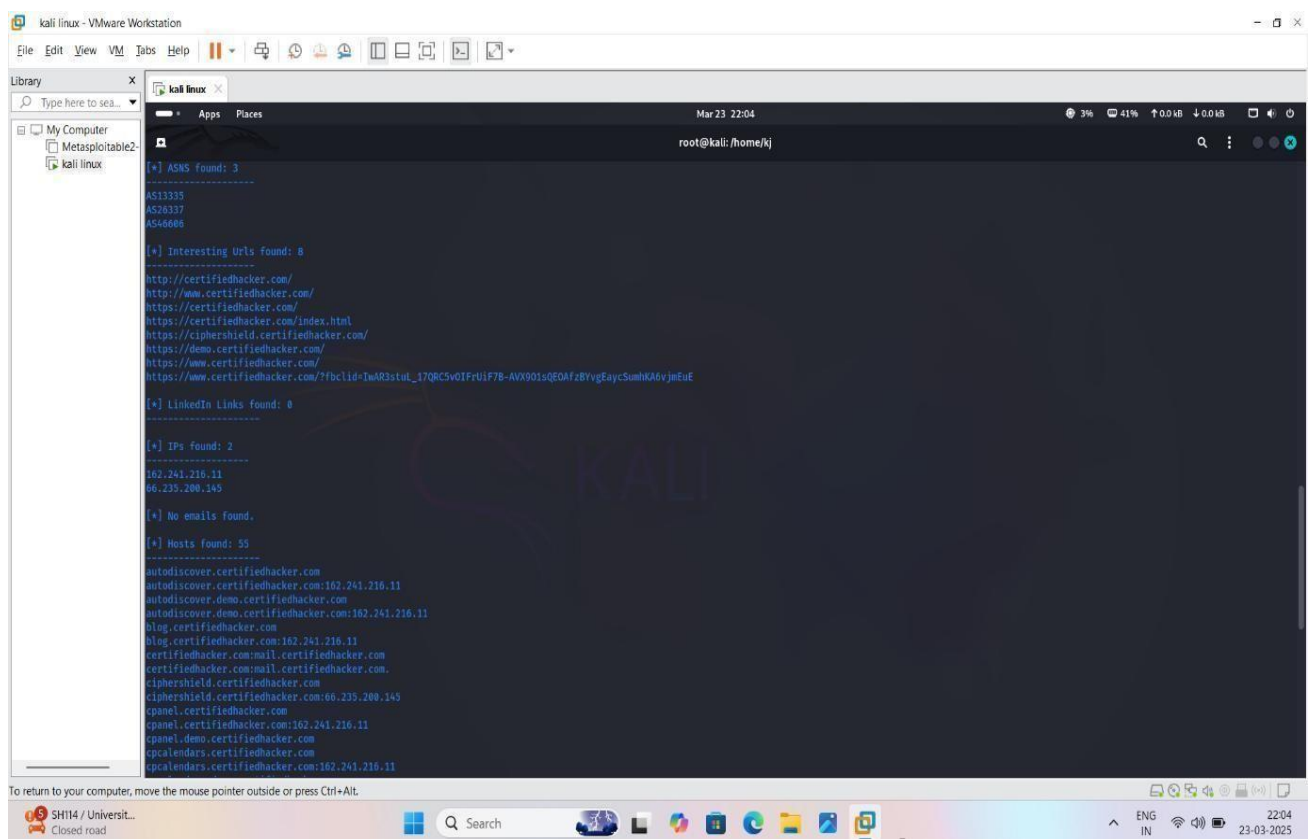
Command : theHarvester -d example.com -b bing

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  
dnscmdumpster.



```
kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Metasploitable2
kali linux
Apps Places
Mar 23 22:04
root@kali: /home/kj
[*] ASNs found: 3
-----
AS13395
AS28337
AS46686
[*] Interesting URLs found: 8
-----
http://certifiedhacker.com/
http://www.certifiedhacker.com/
https://certifiedhacker.com/
https://certifiedhacker.com/index.html
https://ciphershield.certifiedhacker.com/
https://demo.certifiedhacker.com/
https://www.certifiedhacker.com/
https://www.certifiedhacker.com/?fbclid=IwAR3stul_17QKCSv0IFruiF7B-AVX901sQE0AfzBYvgEaycSunhKA6vjEeE
[*] LinkedIn Links found: 0
-----
[*] IPs found: 2
-----
162.241.216.11
66.235.200.145
[*] No emails found.
[*] Hosts found: 55
-----
autodiscover.certifiedhacker.com
autodiscover.certifiedhacker.com:162.241.216.11
autodiscover.demo.certifiedhacker.com
autodiscover.demo.certifiedhacker.com:162.241.216.11
blog.certifiedhacker.com
blog.certifiedhacker.com:162.241.216.11
certifiedhacker.com:mail.certifiedhacker.com
certifiedhacker.com:mail.certifiedhacker.com
ciphershield.certifiedhacker.com
ciphershield.certifiedhacker.com:66.235.200.145
cpanel.certifiedhacker.com
cpanel.certifiedhacker.com:162.241.216.11
cpanel.demo.certifiedhacker.com
cpalendars.certifiedhacker.com
cpalendars.certifiedhacker.com:162.241.216.11
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```

🔗 **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

Name : Kunal jawale

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

```
kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Metasploitable2
kali linux
Mar 23 22:32
root@kali: /home/kj
Sponsored by...
BLACK HILLS
www.blackhillsinfosec.com
PRACTISEC
www.practisec.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installed.
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedln_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-multi/censys_org
[*] Module installed: recon/companies-multi/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
[*] Module installed: recon/contacts-contacts/abc
[*] Module installed: recon/contacts-contacts/mailtester
[*] Module installed: recon/contacts-contacts/mangle
[*] Module installed: recon/contacts-contacts/unmangle
[*] Module installed: recon/contacts-credentials/hibp_breach
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Metasploitable2
kali linux
Mar 23 22:42
root@kali: /home/kj
| rowid | domain | notes | module |
| 1 | certifiedhacker.com | user_defined |
1 rows returned
[recon-ng][cehv13] > modules load brute
[*] Multiple modules match 'brute'.
Exploitation
-----
exploitation/injection/xpath_bruter
Recon
-----
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_suffix
[recon-ng][cehv13] > modules load recon/domains-domains/brute_suffix
[recon-ng][cehv13][brute_suffix] > run
CERTIFIEDHACKER.COM
[*] certifiedhacker.0 => No record found.
[*] certifiedhacker.01 => No record found.
[*] certifiedhacker.02 => No record found.
[*] certifiedhacker.03 => No record found.
[*] certifiedhacker.1 => No record found.
[*] certifiedhacker.10 => No record found.
[*] certifiedhacker.11 => No record found.
[*] certifiedhacker.12 => No record found.
[*] certifiedhacker.13 => No record found.
[*] certifiedhacker.14 => No record found.
[*] certifiedhacker.15 => No record found.
[*] certifiedhacker.16 => No record found.
[*] certifiedhacker.17 => No record found.
[*] certifiedhacker.18 => No record found.
[*] certifiedhacker.19 => No record found.
[*] certifiedhacker.2 => No record found.
[*] certifiedhacker.20 => No record found.
[*] certifiedhacker.3 => No record found.
[*] certifiedhacker.3com => No record found.
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```

Name : Kunal jawale