

# **MODULE 2**

## **Foot Printing & Reconnaissance**



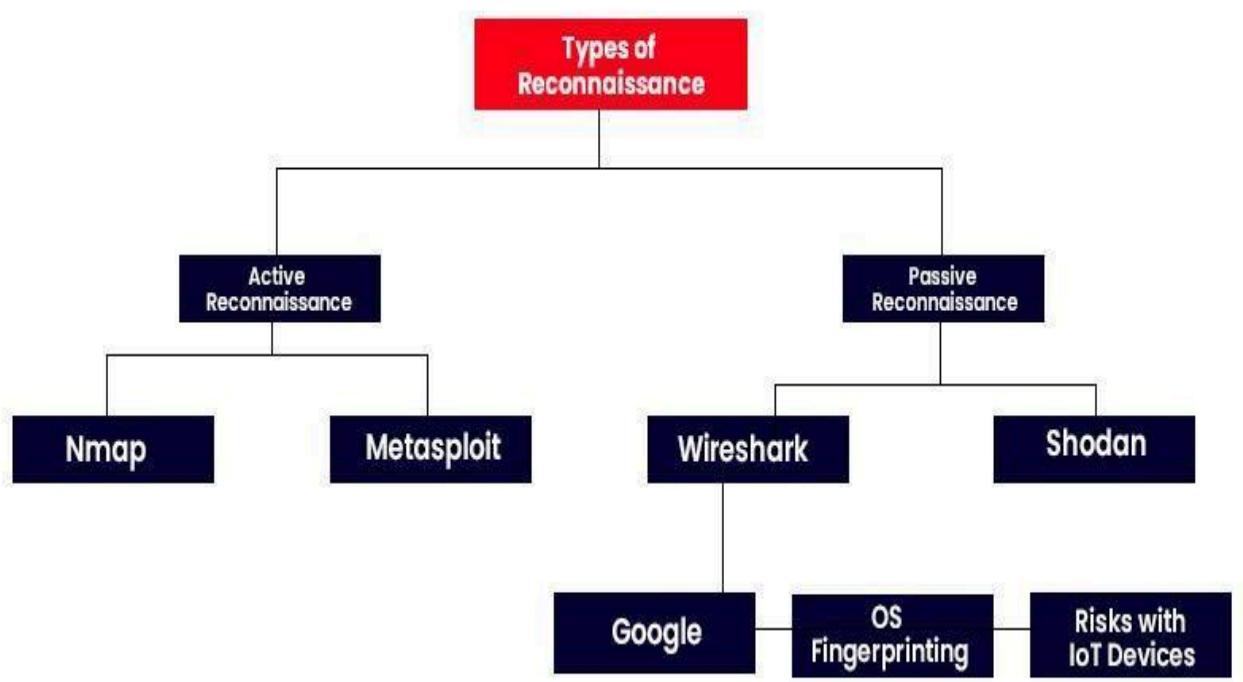
**Name: Omkar Hundekari**

**Course: CEH Practical**

**Training Subject: Cybersecurity**

## Foot-Printing Concepts:

Reconnaissance in ethical hacking is the preliminary information-gathering phase where ethical hackers collect data about a target system to understand its infrastructure, vulnerabilities, and potential points of compromise. This "digital detective work" involves both passive methods (without direct interaction, like using search engines) and active methods (direct interaction, like port scans). The gathered information, forming a detailed intelligence report, helps identify weaknesses that can be exploited to improve security and reduce risks for organizations.



## Types of Foot-Printing /Reconnaissance :

## □ Passive Foot-Printing:

Passive Foot-Printing is the initial phase of ethical hacking or penetration testing where an attacker gathers information about a target without direct interaction or engagement with its systems. It involves using publicly available information and indirect methods, such as searching a target's website or employee social media profiles on search engines like Google, to build a comprehensive profile of the target's infrastructure, potential vulnerabilities, and overall network environment.

## □ Active Foot-Printing:

Active Foot-Printing are an intrusive method of foot-printing (information gathering) that directly interacts with a target system to gather data, potentially triggering Intrusion Detection Systems (IDS) and leaving logs. Tools such as Nmap, Nessus, and even basic commands like ping or traceroute are used for active foot-printing to discover details like IP addresses, open ports, operating systems, and network topologies. While passive foot-printing gathers information from public sources, active foot-printing uses direct queries and actions to collect deeper, non-public information that can't be obtained passively.

## ■ What Kind of Information needed:

## □ Network Information

**Network Information** involves gathering details like IP addresses, network ranges, active machines, open ports, and network topology to identify weaknesses in a target's infrastructure before launching an attack or for security testing. This reconnaissance helps attackers understand a network's layout, discover exploitable services, and identify potential vulnerabilities in the target's network.

- Information Gathered

- **Network Topology:** Understanding the layout and structure of the network.
- **IP Address Ranges:** Identifying the IP addresses used by the network.
- **Hostnames and Exposed Hosts:** Discovering the names of machines on the network and any that are directly accessible.
- **Operating Systems:** Identifying the specific operating systems running on various hosts.
- **Applications and Services:** Determining which applications and services are running and their versions.
- **Open Ports:** Discovering which ports are open and listening for connections.

- What is Important ?

- **For Attackers:**

To understand the target's security posture and find vulnerabilities to exploit.

- **For Defenders (Ethical Hacking/Penetration Testing):**

To identify their own weaknesses and improve their security before malicious actors can exploit them.

## □ System Information:

**System information** in foot-printing is the collection of details about a computer system to understand its security posture and identify weaknesses, using active or passive methods. This includes discovering IP addresses, open ports, operating system versions, running services, and network topology, which aids in planning an attack or, for ethical hackers, in strengthening defences.

### ● What is discovered:

- **Basic Details:** IP addresses, network ranges, and active devices.
- **Software & Services:** Operating system types and versions, and the specific services running on them.
- **Network Architecture:** Creating a map of the network to understand its topology.
- **User & Company Information:** Names of employees, their contact details, and other publicly available corporate data.

- **What is Important ?**

- **Security Analysis:**

Organizations use foot-printing to identify and address security weaknesses before an attacker does.

- **Attack Planning:**

Attackers use this information to design and execute more effective attacks.

- **Organization Information:**

In foot-printing, **Organization information** refers to any data gathered about a target company to understand its systems, network infrastructure, users, and potential security vulnerabilities. This information is collected through passive (e.g., public sources like websites) or active (e.g., network scanning) methods to build a profile of the organization's security posture for purposes ranging from ethical hacking to unauthorized cyberattacks.

- **What Information is collected ?**

- **Network Infrastructure:** Details about the organization's network topology, devices, and open ports.

- **Systems:** Information on servers, operating systems, and software used.
  - **Users:** Data on employee accounts and how they interact with the system.
  - **Security Posture:** A profile of the organization's security weaknesses and defences.
- 
- Why is this Information important ?
- **Vulnerability Identification:** To find security weaknesses and loopholes in an organization's systems.
  - **Ethical Hacking:** To simulate attacks and identify security deficiencies before malicious actors exploit them.
  - **Malicious Attacks:** To build a comprehensive profile of a target organization for unauthorized access and exploitation.

## How to Perform Foot-Printing:

- **Through Search Engines:**
  - **Through Social networking sites**
  - **Through official websites**
  - **Direct communication with Targets**
  - **Through Job Portals**
  - **Through DNS enumeration**
- 
- Machines used for Foot-Printing:

# Machines Used for Footprinting



Windows 11



VirtualBox



Parrot



Metasploitable 2

## □ Search Engines in Foot-Printing:

**Search Engines** are specialized search engines or tools designed to help cybersecurity professionals and researchers find information related to cybersecurity threats, vulnerabilities, solutions, and other relevant topics.

- Advanced Google Hacking Techniques:

- **Specific Domain:**

- a) Site:Certifiedhacker.com
- b) Site:\*.certifiedhacker.com

a)

The screenshot shows a Google search results page for the query "certifiedhacker.com". The first result is a link to the official website, which includes a navigation menu with links like "Our website", "Administrative Portal Sign in to ...", "Online Booking", "Contact us", and "About us". Below the website link is a WHOIS lookup result from Who.is, followed by a ZoomInfo entry.

b)

The screenshot shows a Google search results page for the query "\*certifiedhacker.com". The results are identical to the previous screenshot, displaying the official website, WHOIS information, and a ZoomInfo entry.

- Find Keywords inside a URL:

- a) inurl:login
- b) inurl:admin

## c) inurl:dashboard

a)

The screenshot shows a Google search results page with the query "inurl:login". The results include:

- Dictionary**: Definition from Oxford Languages - Learn more. Shows the word "login" with a speaker icon and the definition "an act of logging in to a computer, database, or system." It also lists "a password or code used when logging in." and the quote "you need to remember your user login".
- Wikipedia**: https://en.wikipedia.org/wiki/Login. Shows the Wikipedia article title "Login" and a brief description: "Logging in (or logging on, signing in, or signing on) is the process by which an individual gains access to a computer system or program". Below the description are buttons for "Login (disambiguation)", "Login session", "Social login", and "Login spoofing".
- Login - Instagram**: https://www.instagram.com/accounts/login/. Shows the Instagram login page with the heading "Welcome back to Instagram. Sign in to check out what your friends, family & interests have been capturing & sharing around the world."

The browser interface at the bottom includes a weather widget showing "Cloudy" and "27°C", a taskbar with various icons, and a status bar indicating "ENG IN" and the date "30-08-2025".

b) Image next page

inurl:admin - Google Search

Google

inurl:admin

All Mode All Images Videos News Short videos Shopping More Tools

Dictionary Definitions from Oxford Languages Learn more

admin / admin/ noun INFORMAL • BRITISH the administration of a business, organization, etc. "day-to-day admin"

Feedback See more >

Google Admin https://admin.google.com :: Sign in - Google Accounts Not your computer? Use Guest mode to sign in privately. Learn more about using Guest mode. Next. Create account. For my personal use; For work or my ...

User admin Sign in. Use your Google Account. Email or phone. Forgot email ...

Email or phone Sign in. Use your Google Account. Email or phone. Forgot email ...

Admin With Admin Console, you can manage Workspace for your ...

Cloudy 27°C ENG IN 30-08-2025 12:35

c)

inurl: dashboard - Google Search

Google

inurl: dashboard

All Mode All Images Videos Shopping Short videos News More Tools

Google Dashboard Sign in to see and manage the data in your Google Account. Sign in. Google Account settings. Search. Clear search. Close search. Main menu. Google apps. Missing: inurl: | Show results with: inurl:

People also ask :

- What is the dashboard URL?
- How do I check my Gmail dashboard?
- How to download dashboard app?
- What is dashboard in settings?
- What is a dashboard UI?
- How to create a dashboard link?
- How to use Google Dashboard?
- How to find person details by Gmail ID?
- How do I restore my photos?

News for you This 27-year-old... ENG IN 30-08-2025 12:35

## • Search for Keywords in page titles:

- a) Intitle:“index of”**
- b) Intitle: “test environment”**

**a)**

Name	Last modified	Size	Description
Parent Directory	-	-	
1-000-times-good-night/	2023-10-26 01:55	-	
1-autumn-3-winters/	2023-10-26 01:55	-	
21-paradise/	2025-04-08 20:21	-	
37/	2023-10-26 01:54	-	
100-yen-love/	2025-04-24 00:54	-	
200-meters/	2023-10-26 01:55	-	
578-magnum/	2024-02-25 22:44	-	
1944/	2023-10-26 01:55	-	
1981/	2023-10-26 01:54	-	
20000-species-of-bees/	2024-10-22 18:09	-	
Mussolini-legacy/	2025-02-24 21:46	-	
P9129457b.jpg	2025-04-08 20:21	808K	
B9279793.JPG	2025-04-08 20:21	612K	
a-bag-of-marbles/	2023-10-26 01:54	-	
a-balance/	2024-01-30 17:08	-	
a-bottle-in-the-gaza-sea/	2023-10-26 01:54	-	
a-call-girl/	2023-10-26 01:55	-	
a-dangerous-game/	2023-10-26 01:54	-	
a-girl-missing/	2023-10-26 01:55	-	
a-good-woman-is-hard-to-find/	2023-10-26 01:55	-	
a-life-for-ballet/	2023-10-26 01:55	-	
a-life-in-dirty-movies/	2023-10-26 01:54	-	
a-long-way-from-home/	2023-10-26 01:54	-	
a-midsummer-night-s-dream/	2023-10-26 01:54	-	
a-nice-jewish-boy/	2025-07-21 20:59	-	
a-say-thing/	2023-10-26 01:54	-	
a-peck-on-the-cheek/	2023-10-26 01:55	-	
a-radiant-girl/	2023-10-26 01:55	-	
a-reggae-session/	2023-10-26 01:54	-	
a-regular-woman/	2023-10-26 01:55	-	
a-screaming-man/	2023-10-26 01:55	-	

**b)image on next page**

**Test Environment: A Beginner's Guide**

Last Updated : 23 Jul, 2025

As we know for the development of a software application/product the development team follows a set of steps that are performed in different phases of the [Software Development Life Cycle \(SDLC\)](#). In SDLC Software testing is one of the important phases as it ensures the quality of the product. So, for that different types of [software testing](#) are performed to check different parameters or test cases. During the testing phase depending upon the type of testing different members are involved like the developer, the tester, and sometimes the customer/client also. But the basic thing to perform testing is a test environment. Because it provides a perfect setup for testing teams as a testing environment is equipped with various testing-related tools and other elements that support test execution with hardware, software, and network configured. The article focuses on discussing the test environment in detail.

**What is a Test Environment?**

The test environment is the hardware and software set up for the testing teams to run test cases. This test environment setup varies from product to product and its configuration completely depends on the application under test requirement. The easiest way to organize a test environment is through automation.

- The test environment is used by the testing teams to test the software, identify the bugs, and find a possible fix for the bugs.
- A test environment is used to check the quality of the software and the impact of the application before release.
- It enables the tester to check the different parts of the application using different configurations and data setups.

**Test Bed** is very similar to Test Environment with a small difference. The test bed is also a type of test environment that consists of test data to verify the functionalities of the software applications.

The staging environment is a copy of the production environment for software testing. This is used before the actual deployment of the software so that final tests can be executed.

**Importance of Test Environment**

Knowing about the quality and functionality of applications under process in a test environment is very important. Because it provides a dedicated environment for us to isolate the code and examine the application so that other actions have no

- Find the files with specific extension:

- a) filetype:pdf penetration tester 3<sup>rd</sup> edition
- b) filetype:xls

- a) Image on next page

filetype:pdf penetration tester 3rd edition

AI Mode All Shopping Images Videos Short videos Forums More Tools

**R** ResearchGate https://www.researchgate.net › publication › links PDF : Google Hacking for Penetration Testers 11 Sept 2001 — Penetration Testers, Third Edition. Copyright Elsevier 2016 This book has been licensed to Billy Gardner (bill.gardner@gmail.com). Page 4. Page ... 237 pages

**A** Anarchopy https://edu.anarchopy.org › Metasploit Penetrat... PDF : Metasploit Penetration Testing Cookbook Third Edition Welcome to Metasploit Penetration Testing Cookbook, Third Edition. This book covers various recipes of performing penetration testing over different ... 416 pages

**S** The Swiss Bay https://theswissbay.ch › pdf › Security › Syngress... PDF : Penetration Tester's Open Source Toolkit world for penetration testing, learn how those toolkits are built and how to modify CHAPTER Penetration Tester's Open Source Toolkit, Third Edition DOI ... 465 pages

**D** digitvbg.com https://digitvbg.com › files › books-for-hacking PDF : The Hacker Playbook 3: Practical Guide To Penetration Testing 1 May 2018 — This is the third iteration of The Hacker Playbook (THP) series. Below is an overview of all the new vulnerabilities and attacks that will ... 264 pages

Zenk - Security - Repository https://www.zenk-security.com › Penetration Toolkit PDF : Zenk - Security - Repository

b)

Google search results for "filetype:xls penetration tester".

Results:

- State of Mississippi (.gov)  
https://fis.its.ms.gov/Procurement/rips.xls
- Penetration Testing  
Vendor must provide application penetration testing services to detect, evaluate the security, quantify and prioritize security vulnerabilities associated with ...
- People also ask :
  - What does a penetration tester do?
  - What are the 5 stages of pentesting?
  - What are the 7 penetration testing?
  - What is the salary of a penetration tester?
- Life Insurance Corporation of India  
https://icidia.in/documents/Non-Hazardous... xls
- Infra and Security Requirements  
Is Vulnerability Assessment and Penetration Testing (VAPT) and certification by a third party auditor conducted periodically? 110, 109, Is an audit trail for ...
- search.org  
https://www.search.org/files.xls; SEARCHITS... xls
- SEARCH IT Security Self- and Risk-Assessment Tool  
... penetration testing? 16, 2,15 Are security alerts and security incidents ... 6 Is penetration testing

- Google Hacking Database:



- Examples of Google Dorks from GHDB

Here are some typical classes of GHDB queries:

- **Login Admin Portals**

inurl:admin login

inurl:login.php [Cybrvaul+1](#)

- **Exposed Database Dumps or Credentials**

filetype:sql intext:"INSERT INTO"

intext:"password" filetype:txt [Cybrvaul+1](#)

- **Directory Listings and Open Folders**

intitle:"index of" "parent directory" [Cybrvaul+1](#)[Onion Linux](#)

- **Sensitive Documents & PDFs**

filetype:pdf intext:"confidential"

filetype:docx intext:"restricted" [Cybrvaul+1](#)[Intellipaat](#)

- **Security Cameras & Devices**

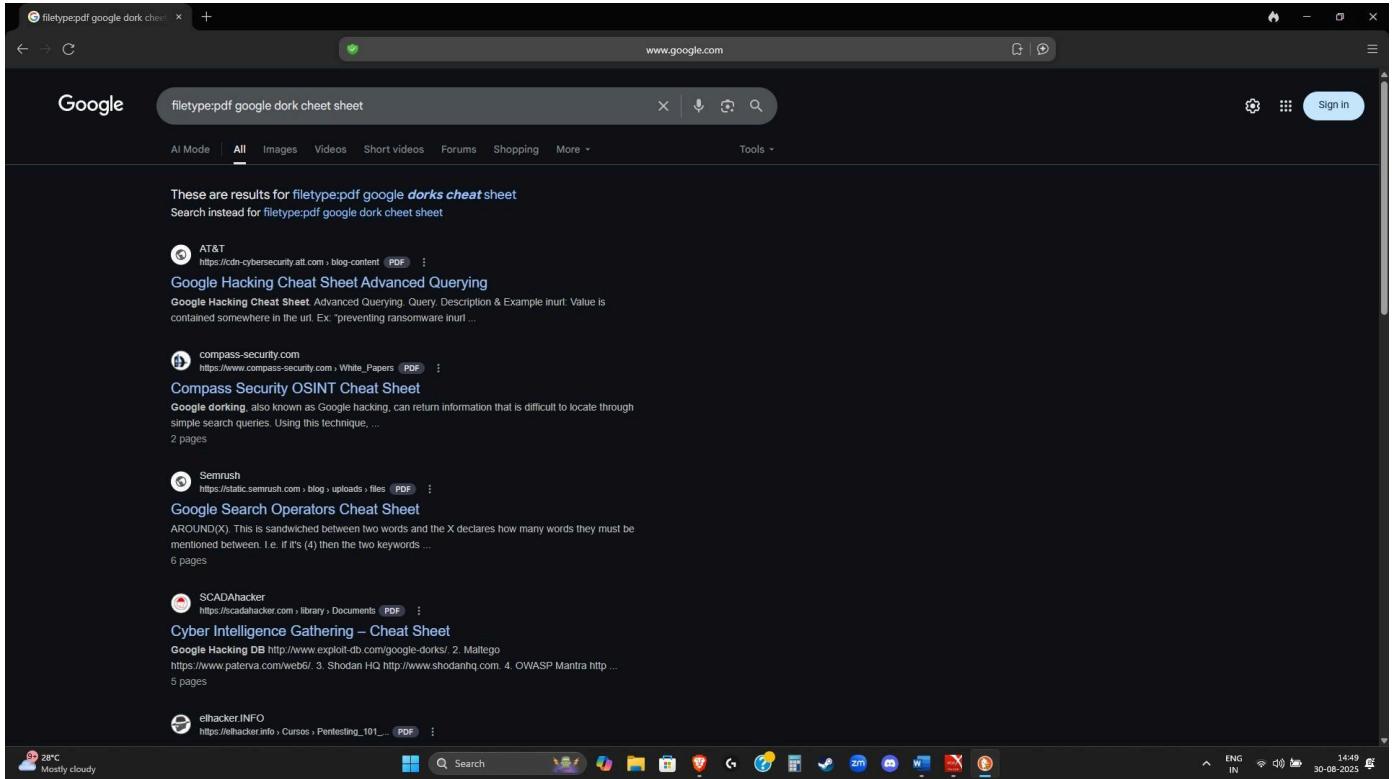
inurl:"view/view.shtml"

inurl:/view.shtml intext:admin [Cybrvaul](#)[Intellipaat](#)[Onion Linux](#)

- **Server Configs / Error Messages**

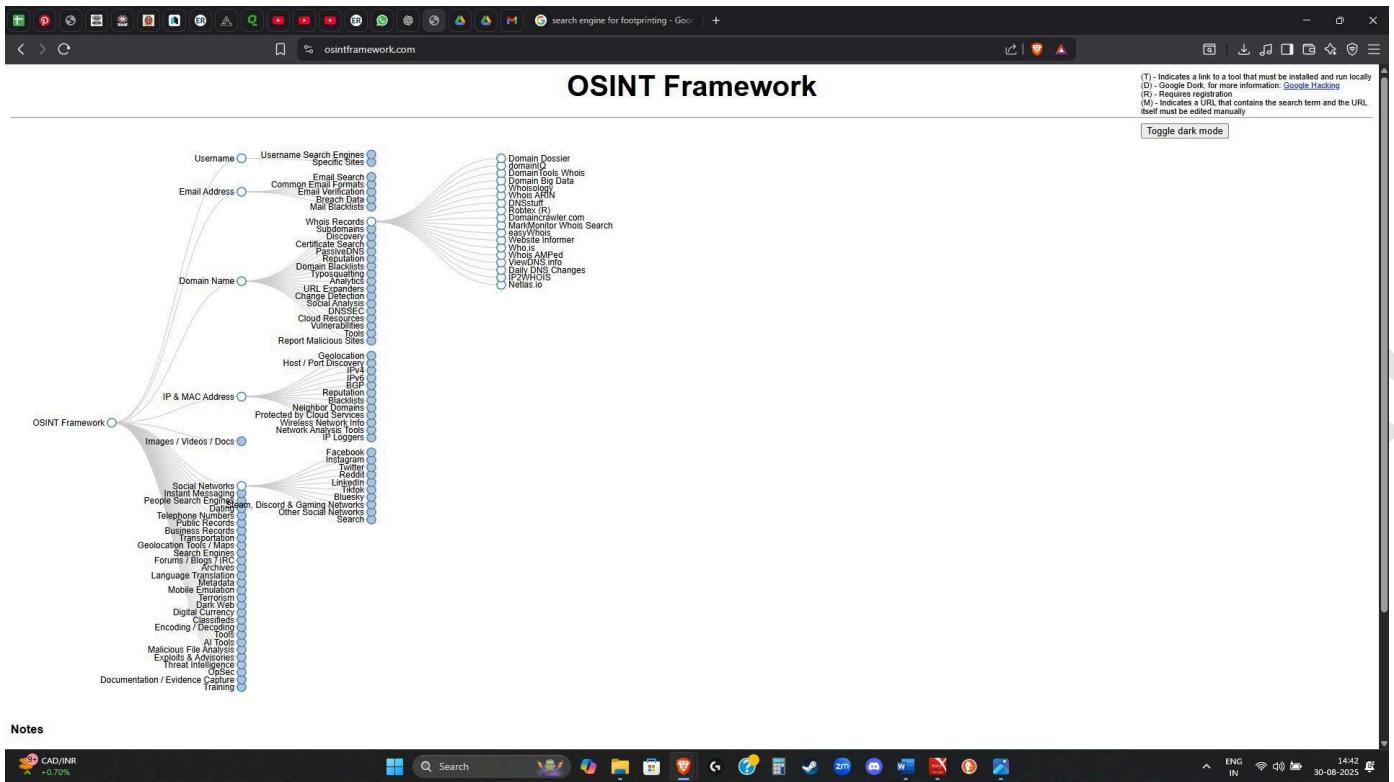
filetype:log

intext:"DB\_PASSWORD" filetype:env (common in exposed config files) [WebAsha](#)[Intellipaat](#)



## ▪ OSINT Framework:

**OSINT & Bug Bounties:** Valuable for locating sensitive data faults that researchers can report. It's also widely used in real-world red teaming scenarios



## ▪ Summary Table

Aspect	Details
What it is	A curated collection of advanced Google search queries (Google Dorks)
Origin	Created by Johnny Long (2004), maintained on Exploit-DB by Offensive Security
Use cases	Reconnaissance, vulnerability discovery, OSINT, bug bounty, red teaming
Popular categories	Admin portals, credentials leaks, open directories, sensitive documents, camera feeds

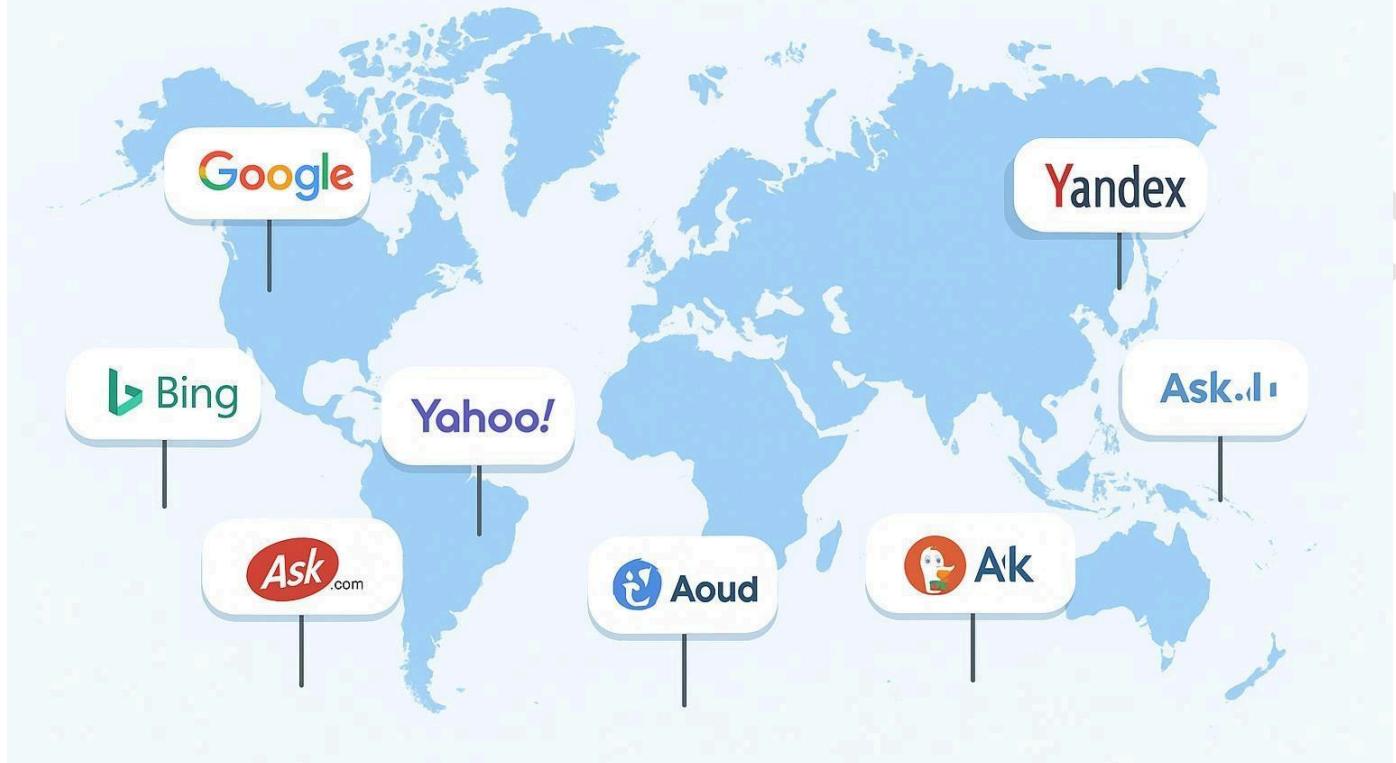
## Legal considerations

Only use with authorization—misuse may violate laws like CFAA and GDPR

- **Examples of Major Search Engines:**

- **Google** – Most widely used global search engine.
- **Bing** – Microsoft's search engine.
- **Yahoo! Search** – Older but still in use.
- **Baidu** – Popular in China.
- **Yandex** – Popular in Russia.
- **DuckDuckGo** – Privacy-focused search engine.
- **Ask.com** – Question-answer based search platform.
- **AOL Search** – Legacy search engine.

# GLOBAL SEARCH ENGINES MAP



## Foot-Printing using Advanced Google Hacking Database:

Screenshot of the Exploit-DB Google Hacking Database interface.

The page title is "Google Hacking Database".

Filter options include "Show 15" and "Quick Search" (search term: password).

The main table displays 15 entries from a total of 401, filtered from 7,944 total entries. The columns are Date Added, Dork, Category, and Author.

Date Added	Dork	Category	Author
2024-03-25	intitle: index of /concrete/Password	Sensitive Directories	Gautam Rawat
2024-01-23	(site:jsonformatter.org   site:codebeautify.org) & (intext:aws   intext:bucket   intext:password   intext:secret   intext:username)	Files Containing Juicy Info	letmewin cyber
2022-06-16	site:com.* inttitle:"index of" *admin.password	Files Containing Juicy Info	Girish B O
2022-06-15	# Description: site:gov.in filetype:xlsx "password"	Files Containing Juicy Info	Mangesh Pandhare
2021-11-18	db_password filetype:eml	Files Containing Juicy Info	Thiru kumaran
2021-11-15	site:reentry.co inttext:"password"	Files Containing Passwords	Anirudh Kumar Kushwaha
2021-11-15	site:controlc.com inttext:"password"	Files Containing Passwords	Anirudh Kumar Kushwaha
2021-11-15	site:pastebin.com "admin password"	Files Containing Passwords	SaumyaJeet Das
2021-11-11	inurl:forgotpassword.php	Files Containing Juicy Info	Krishna Agarwal
2021-11-10	site:pastebin.com "password"	Files Containing Passwords	Krishna Agarwal
2021-11-09	site:forgotpassword.php	Files Containing Juicy Info	Anirudh Kumar Kushwaha
2021-11-09	site:pastebin.com *@mail.com password"	Files Containing Juicy Info	Anirudh Kumar Kushwaha
2021-11-08	site:gitlab.* inttext:password inttext:@gmail.com   @yahoo.com   @hotmail.com	Files Containing Juicy Info	Jorge Manuel Lozano Gómez
2021-11-08	inttext:"Index of" inttext:"password.zip"	Files Containing Passwords	Parshwa Bhavsar
2021-11-08	inttitle:index of" "username" "password" filetype:xlsx	Files Containing Juicy Info	Onkar Deshmukh

Pagination controls: FIRST, PREVIOUS, 1, 2, 3, 4, 5, ..., 27, NEXT, LAST.

Footer links: Databases, Links, Sites, Solutions.

Page footer includes weather (26°C, Mostly cloudy), search bar, taskbar icons, and system status (ENG IN 19:22 03-09-2025).

# Description: site:gov.in filetype:xlsx "password"

AI Mode All Images Videos Short videos Shopping News More Tools

tmc.gov.in https://tmc.gov.in › event › upload XLS Sheet1 Power-on password, administrator password 65, Systems Management Software, The server should come with systems management software to provide update management ...

Government of Tamil Nadu https://onlinappa.tn.gov.in › sites › default › files XLS General Manual Parameter Description/Layer Description, Layer content, Colour code, 3 ... PASSWORD : p@ssw0rd. New Layers A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R ...

Openforge https://openforge.gov.in › 5465-UMAANG XLS Sheet1 ENTER VALID NUMBER AND VALID PASSWORD AND CLICK ON LOGIN BUTTON, VALID URL AND TEST DATA, MOBILE NUMBER:99119XXXXX MPIN:1907, USER SHOULD BE ABLE TO SEE HOME ...

mahagst.gov.in https://mahagst.gov.in › file › download XLS https://mahagst.gov.in/en/file/8542/download?token... Password Expired for migrated user. Fixed. 19. User needs to go to Forgot password link and reset password to resolve the issue. 20, 11, Enrollment/Migration ...

Chief Minister - Index https://cm.karnataka.gov.in › uploads XLS login functionality Enter Userid & Password, Credential can be entered, As Expected, Pass. 20, 4, Enter CAPTCHA(Or bypass this field), Captcha should be identified and entered, As ...

26°C Mostly cloudy ENG IN 19:21 03-09-2025

"Camera Live Image" inurl:"guestimage.html"

GHDB-ID: 6467 Author: ALEXANDROS PAPPAS

Published: 2020-08-07

Google Dork Description: "Camera Live Image" inurl:"guestimage.html"  
Google Search: "Camera Live Image" inurl:"guestimage.html"

# Google Dork: "Camera Live Image" inurl:"guestimage.html"  
# Various online devices (webcams).  
# Date: 07/08/2020  
# Exploit Author: Alexandros Pappas

Databases	Links	Sites	Solutions
Exploits	Search Exploit-DB	OffSec	Courses and Certifications
Google Hacking	Submit Entry	Kali Linux	Learn Subscriptions
Papers	SearchSploit Manual	VulnHub	OffSec Cyber Range
Shellcodes	Exploit Statistics		Proving Grounds
			Penetration Testing Services

26°C Mostly cloudy ENG IN 19:28 03-09-2025

## Foot-Printing using Shodan- IoT's Hacking:

## Foot-Printing using FTP Search Engine for Hacking:

# Foot-Printing using Video Search Engine(YouTube) for

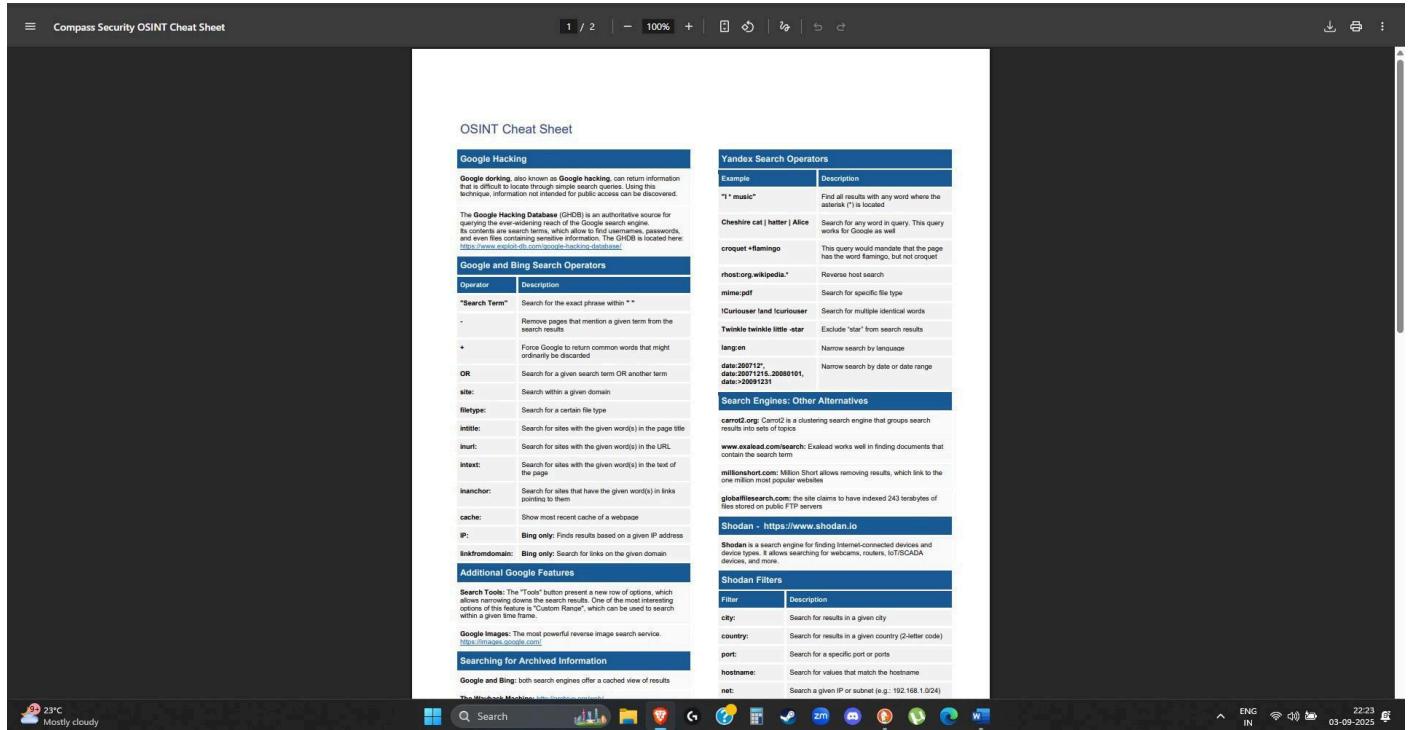
## Hacking:

The screenshot shows a search results page for "youtube video metadata". The top result is from mattw.io, titled "MW Metadata - mattw.io". It describes the service as quickly gathering metadata about videos, playlists, or channels from the YouTube API. Below this, there are sections for "Bulk" and "Location Search". Another result is "YouTube Data Viewer | YTLarge", which provides a data viewer for YouTube metadata. The browser's address bar shows "Videos for youtube video metadata". The taskbar at the bottom includes icons for various applications like File Explorer, Edge, and Task View.

This screenshot shows a detailed view of a video's metadata. The title is "SAIYARA TITLE SONG" by Ahaan Panday, Aneet Padda, Tanishk Bagchi, Faheem A, Arslan N, and Irshad Kamil. It was published on June 3, 2025. The video has over 375 million views. The snippet includes JSON-like code for the video's properties. Below the video thumbnail, there is a list of tags such as "saifyara song", "saifyara movie song", "saifyara full song", "ahaan panday song", "aneet padda song", "mohit suri new movie song", "faheem abdullah songs", "saifyara tu toh badla nahi hai", "mausam zara sa rootha hua hai", "new song 2025", "new hindi songs", "new movie song", "sad songs", "heartbroken song", "heart touching song", "breakup song", "love songs", "heart break song", "yrf new song", "faheem abdullah ishq", "yrf new movie song", "new movie love song", and "new bollywood movie song". The browser's address bar shows "mattw.io". The taskbar at the bottom includes icons for File Explorer, Edge, and Task View.

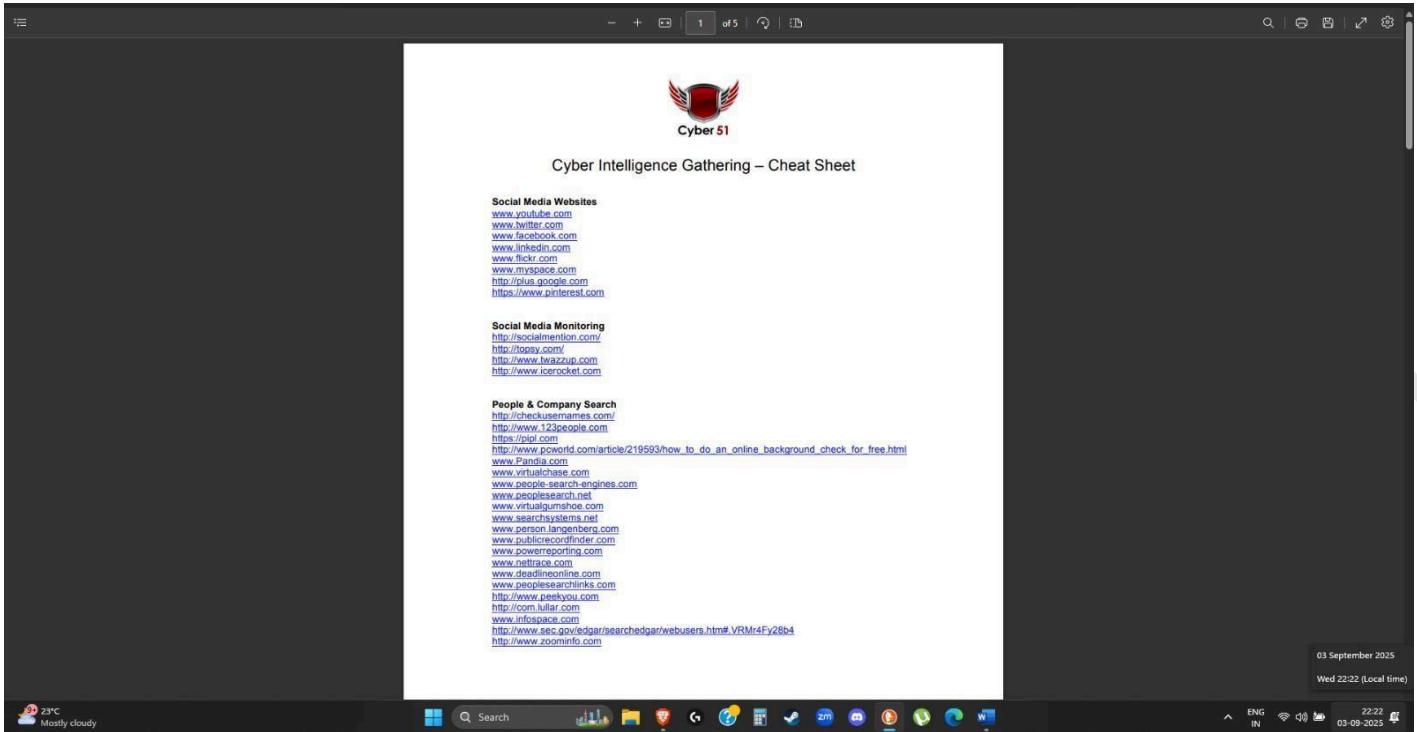
## Foot-Printing using Cheat Sheets for Hacking:

- Like OSINT cheat sheet:



## Foot-Printing using Cyber Intelligence Gathering-Cheat Sheet for Hacking:

- CIG cheat sheet:



## Foot-Printing using Through Internet Research Services for Hacking:

Find Company's Domains, Sub-Domains and Hosts using Netcraft and DNSdumpster:

□ Extracting Company Domains and Sub-Domains using Netcraft tools:

GUIDE: The Total Economic Impact™ of Netcraft Brand Protection | Download now →

Pricing Contact Us Report Fraud Login

**netcraft**

Platform Solutions Why Netcraft Resources Company GET DEMO

THREAT INTELLIGENCE AND DIGITAL RISK PROTECTION

# Trusted Brand Protection at Any Scale

More than threat intelligence — detect, disrupt, and take down threats with unmatched speed, visibility, and accuracy to protect your brand and customers.

GET DEMO REQUEST PRICING →

Globally-trusted threat intelligence and brand protection from phishing, fraud, and scams.

GUIDE: The Total Economic Impact™ of Netcraft Brand Protection | Download now →

Pricing Contact Us Report Fraud Login

**netcraft**

Platform Solutions Why Netcraft Resources Company GET DEMO

## Resources

**Blog**  
Insights, trends, and research on the latest cyber threats

**Guides**  
Step-by-step resources to help you understand and prevent threats

**Research Tools**  
Advanced tools to analyze phishing sites, scams, and tactics

**Case Studies**  
Expert insights on cybersecurity, phishing, and threat prevention.

**Apps & Extensions**  
Detect and block phishing sites with browser extensions and apps

**Webinars**  
Check out the latest insights from our expert webinar series

**Glossary**  
Gain a better understanding of how we talk about cybercrime

**RESOURCE CENTER →**

and customers.

GET DEMO REQUEST PRICING →

Globally-trusted threat intelligence and brand protection from phishing, fraud, and scams.

**netcraft**

LEARN MORE REPORT FRAUD ↗

## What's that site running?

Find out the infrastructure and technologies used by any site using results from our internet data mining

Example: <https://www.netcraft.com>

LOOK UP

© 1995 - 2024 Netcraft Ltd All Rights Reserved. Privacy Policy | Terms and Conditions

23°C Mostly cloudy Search 22:33 03-09-2025 ENG IN

**netcraft**

Site report for <http://eccouncil.org>

▶ 🔎 Look up another site?

Share: [🔗](#) [X](#) [f](#) [in](#) [Y](#)

### Background

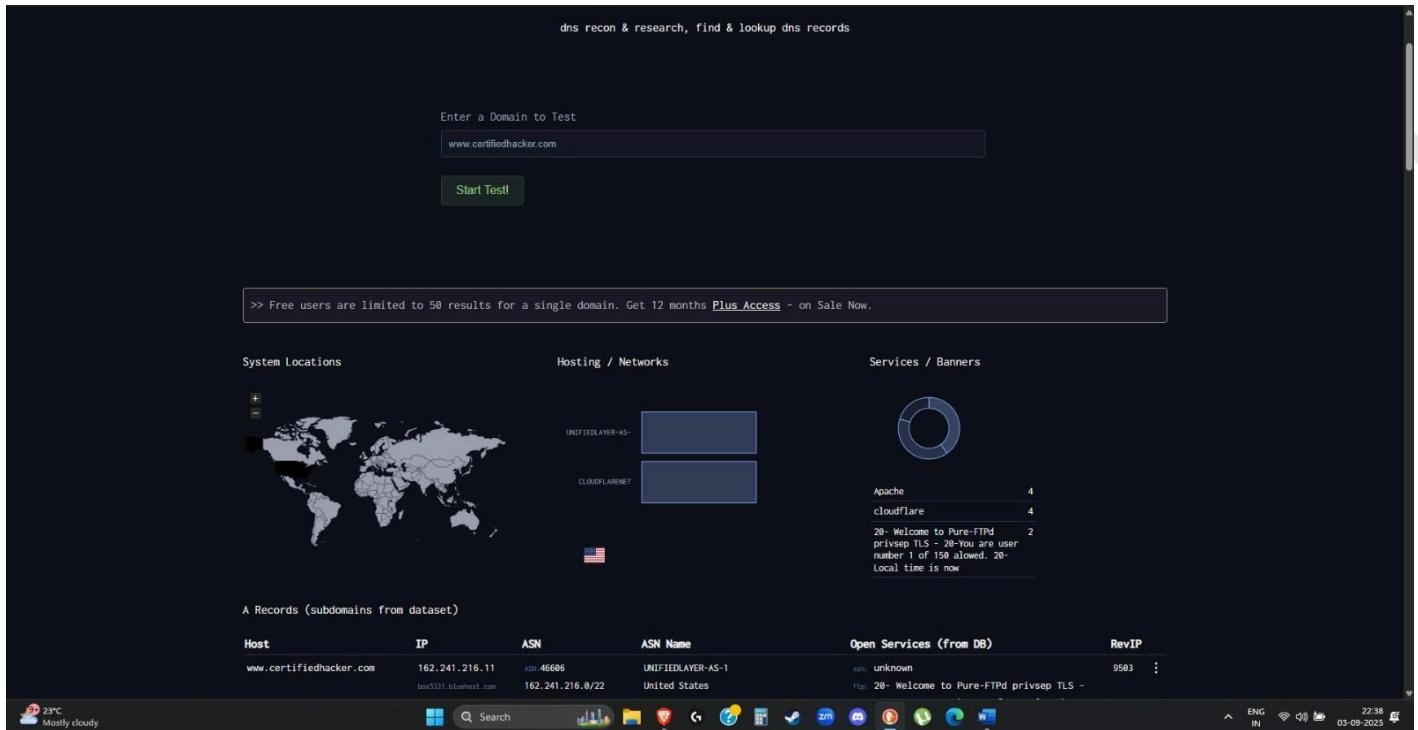
Site title	Best Cyber Security Courses Online   Cybersecurity Training   EC-Council	Date first seen	February 2002
Site rank	294793	Primary language	English
Description	Enroll in the best cyber security courses online by EC-Council. Boost your career with one of the top cybersecurity training program. Get certified now!		

### Network

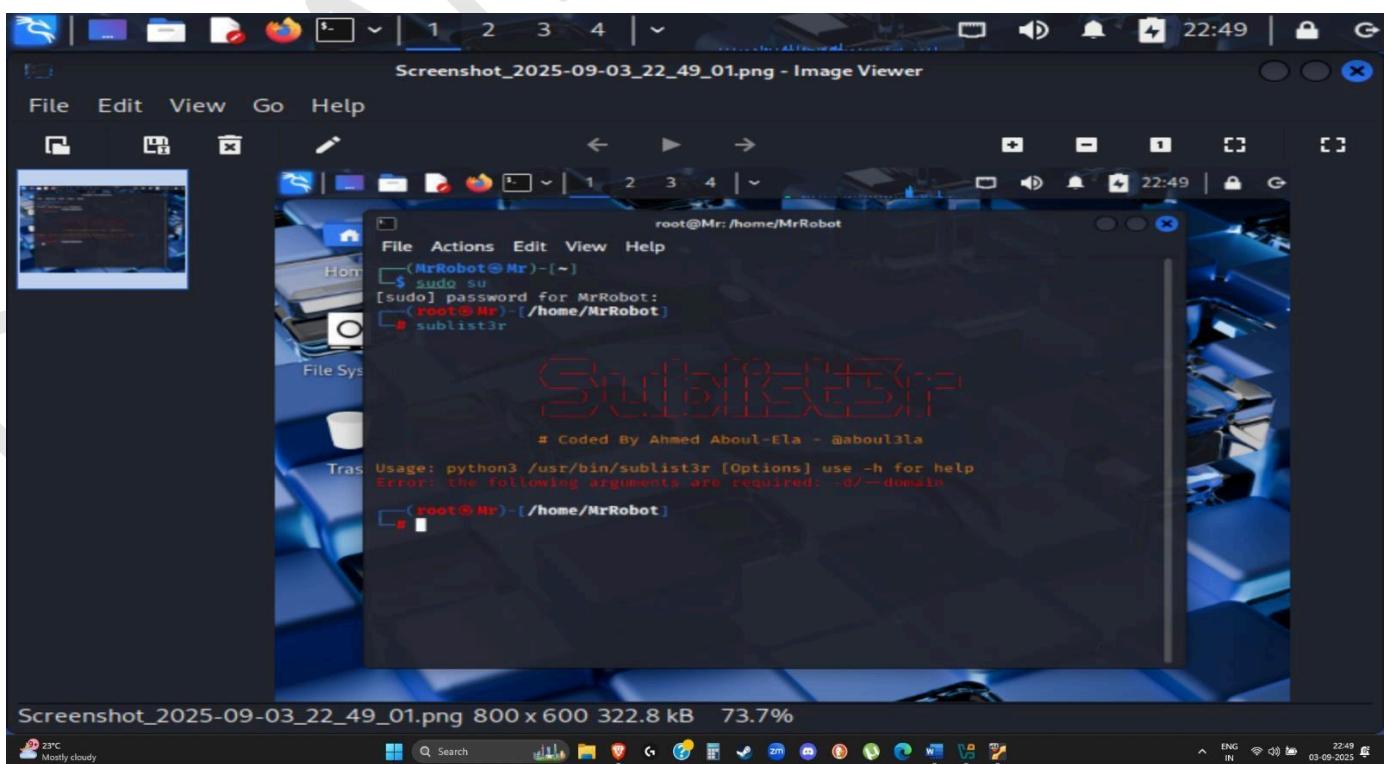
Site	http://eccouncil.org ↗	Domain	eccouncil.org
Netblock Owner	Cloudflare, Inc.	Nameserver	henry.ns.cloudflare.com
Hosting company	Cloudflare	Domain registrar	pir.org
Hosting country	US ↗	Nameserver organisation	whois.cloudflare.com
IPv4 address	104.18.8.180 (VirusTotal ↗)	Organisation	REDACTED, REDACTED, REDACTED, US
IPv4 autonomous systems	AS13335 ↗	DNS admin	dns@cloudflare.com

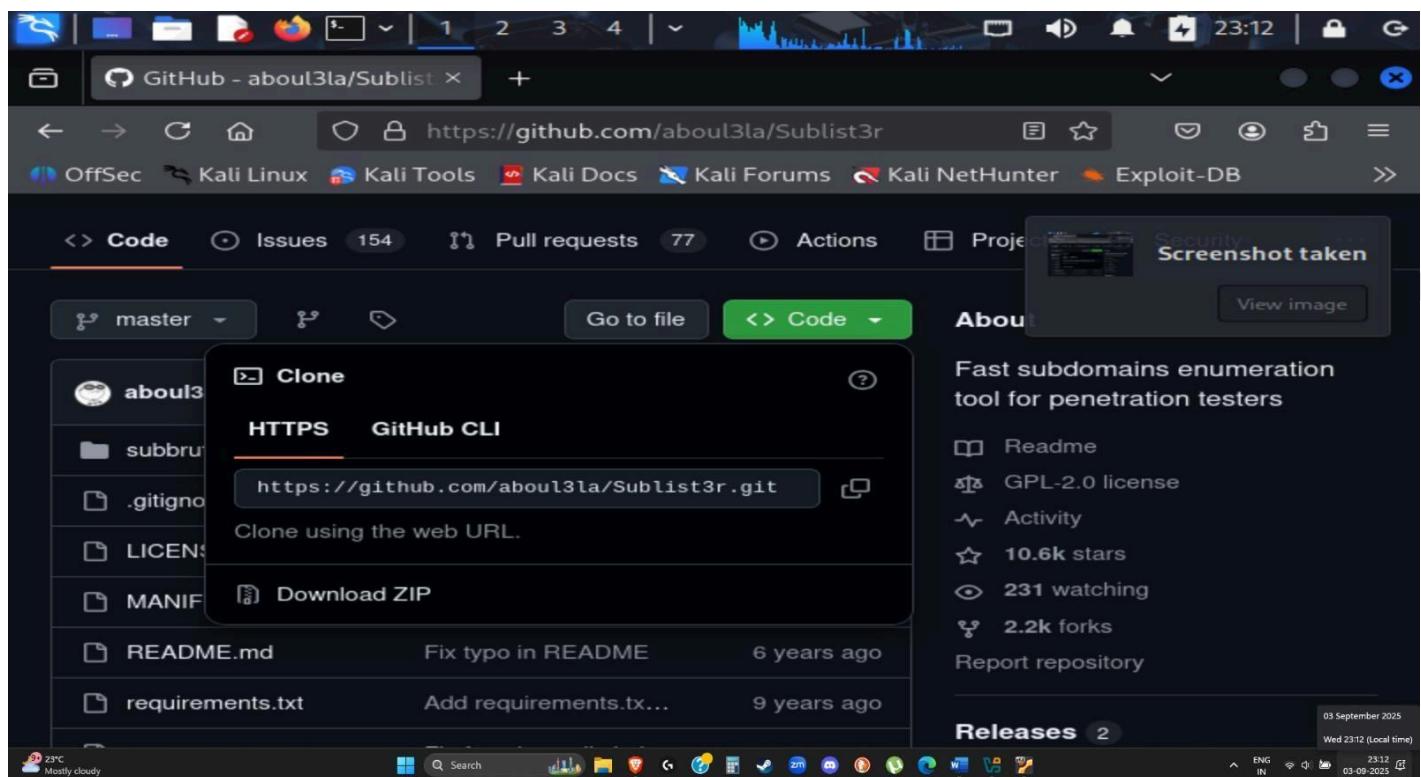
23°C Mostly cloudy Search 22:36 03-09-2025 ENG IN

## □ Extracting Company Domains and Sub-Domains using DNSdumpster tools:



## □ Extracting Company Domains and Sub-Domains using Sublist3r tool in Kali Linux:

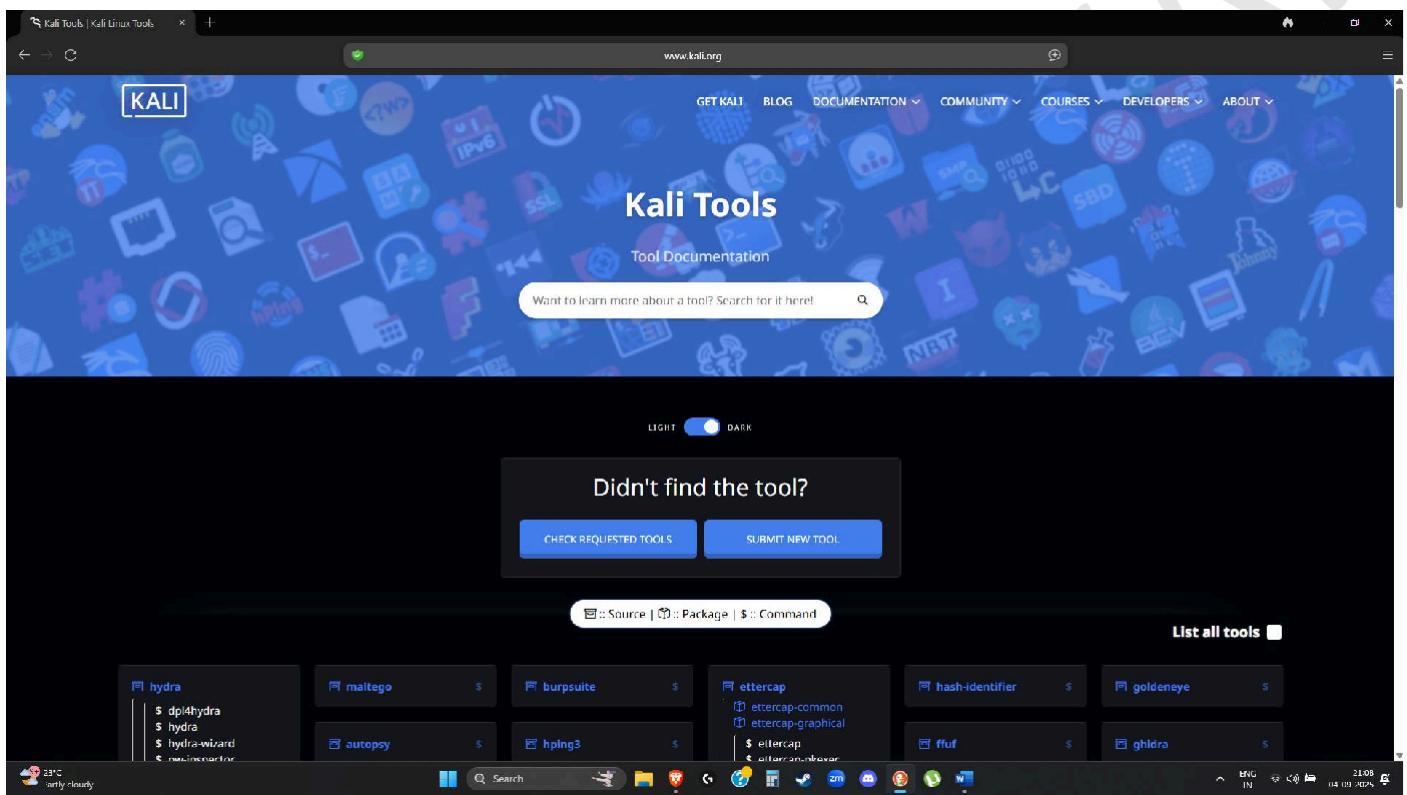




```
root@Mr: /home/MrRobot
File Actions Edit View Help
(MrRobot@Mr)-[~]
$ sudo su
[sudo] password for MrRobot:
(root@Mr)-[/home/MrRobot]
# sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la
Usage: python3 /usr/bin/sublist3r [Options] use -h for help
Error: the following arguments are required: -d/--domain
(root@Mr)-[/home/MrRobot]
# git clone https://github.com/aboul3la/Sublist3r.git
```

- Now understanding what is Sublist3r tool and how to use:

- Open Kali Tools on Google:

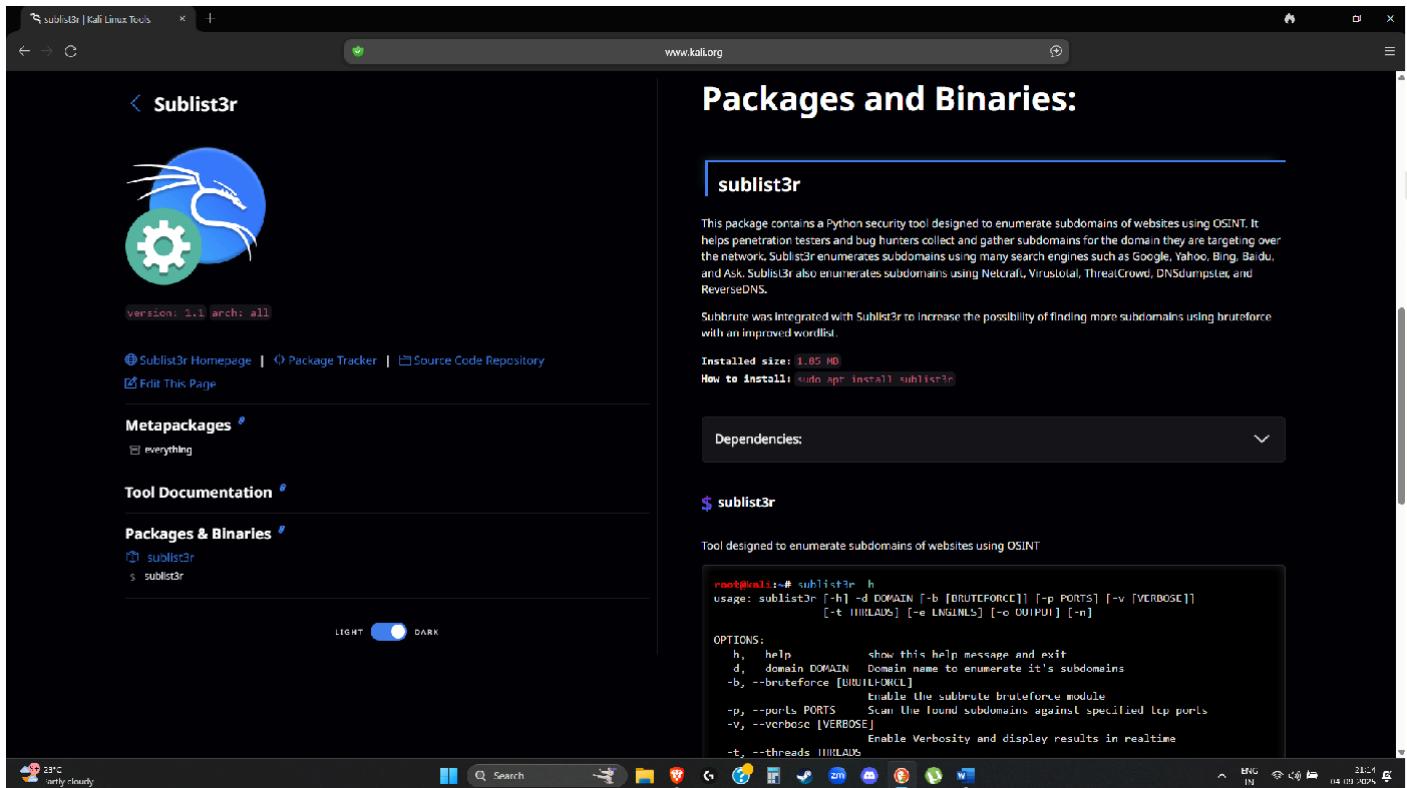


- Type **Sublist3r** and Press Enter :

The screenshot shows the Kali Tools website at [www.kali.org](http://www.kali.org). The main header features the KALI logo and navigation links for GET KALI, BLOG, DOCUMENTATION, COMMUNITY, COURSES, DEVELOPERS, and ABOUT. A search bar at the top contains the query "sublist3r". Below the search bar, a message says " Didn't find an answer to your question? Use Discord". A "LIGHT" to "DARK" toggle switch is present. A central box asks " Didn't find the tool? " with buttons for "CHECK REQUESTED TOOLS" and "SUBMIT NEW TOOL". At the bottom, there's a link to "List all tools" and a toolbar with icons for Source, Package, and Command. The main content area displays a grid of tool cards, with "sublist3r" highlighted in red. Other visible tools include hydra, maltego, burpsuite, ettercap, hash-identifier, goldeneye, ffuf, and ghidra.

The screenshot shows the "Tool Documentation" page for Sublist3r. The left sidebar includes links for Sublist3r Homepage, Package Tracker, Source Code Repository, Edit This Page, Metapackages (everything), Tool Documentation, and Packages & Binaries (sublist3r). The main content area has a title "Tool Documentation: sublist3r Usage Examples". It includes a note about searching for subdomains of kali.org using Bing with 3 threads. Below this is a terminal window showing the command "root@kali:~# sublist3r -d kali.org -t 3 -e bing" and its output, which lists 19 unique subdomains found for www.kali.org. The terminal also shows the credit " # Coded By Ahmed Abou-Lia - @aboulla". The bottom of the page features a "LIGHT" to "DARK" toggle switch and a standard Linux desktop taskbar.

- Type **Sublist3r** Package and Binaries:



## Foot-Printing Through Social Networking Sites for Hacking:

- Now understanding what is **Sublist3r** tool and how to use:

- Type **Sublist3r -d (any domain)**

[www.certifiedhacker.com](http://www.certifiedhacker.com):

```
Kali Linux [Running] - Oracle VM VirtualBox  
Session Actions Edit View Help  
[shinchan@kali:~] $ sudo su  
[sudo] password for shinchan:  
[root@kali:~/home/shinchan]  
# sublist3r -d www.certifiedhacker.com
```

**Sublist3r**  
# Coded By Ahmed Aboul-Ela - @abouela

```
[+] Enumerating subdomains now for www.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  
HTTPConnectionPool(host='searchdns.netcraft.com', port=443): Max retries exceeded with url: /?restriction=sit  
e+ends-with&host=example.com (Caused by ConnectTimeoutError(<urllib3.connection.HTTPSConnection object at 0x7f  
d661b6a120>, 'Connection to searchdns.netcraft.com timed out. (connect timeout=25)')  
Process NetcraftEnum-7:  
Traceback (most recent call last):  
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap  
    self.run()  
  ~~~~~^A  
  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 570, in enumerate  
    cookies = self.get_cookies(resp.headers)
```

25°C Mostly cloudy      06 September 2025 Sat 20:18 (local time)      20:18 06:03 02:25

```
Kali Linux [Running] - Oracle VM VirtualBox  
Session Actions Edit View Help  
[shinchan@kali:~] $ sudo su  
[sudo] password for shinchan:  
[root@kali:~/home/shinchan]  
# sublist3r -d www.certifiedhacker.com
```

**Sublist3r**  
# Coded By Ahmed Aboul-Ela - @abouela

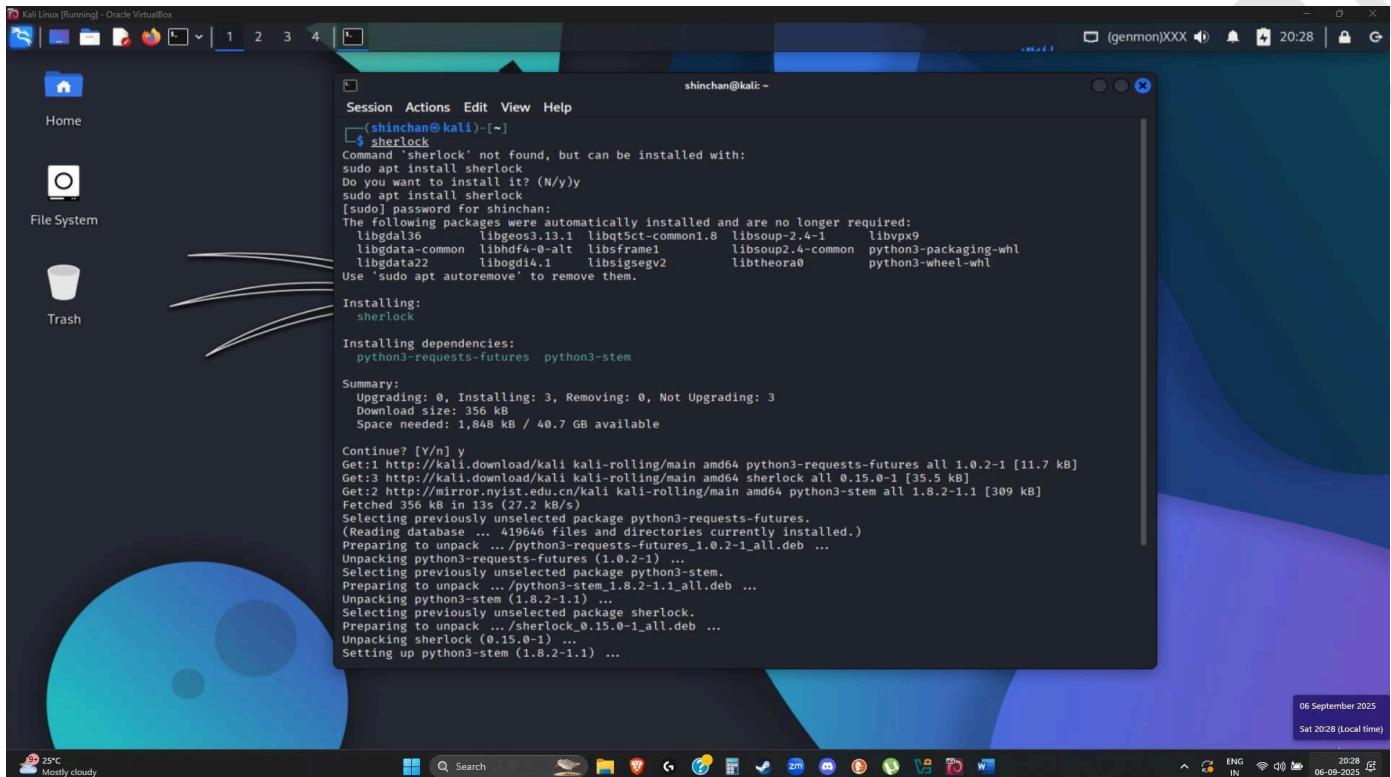
```
[+] Searching now in Baidu..  
[+] Searching now in Yahoo..  
[+] Searching now in Google..  
[+] Searching now in Bing..  
[+] Searching now in Ask..  
[+] Searching now in Netcraft..  
[+] Searching now in DNSdumpster..  
[+] Searching now in VirusTotal..  
[+] Searching now in ThreatCrowd..  
[+] Searching now in SSL Certificates..  
[+] Searching now in PassiveDNS..  
[!] Error: VirusTotal probably now is blocking our requests  
HTTPConnectionPool(host='searchdns.netcraft.com', port=443): Max retries exceeded with url: /?restriction=sit  
e+ends-with&host=example.com (Caused by ConnectTimeoutError(<urllib3.connection.HTTPSConnection object at 0x7f  
d661b6a120>, 'Connection to searchdns.netcraft.com timed out. (connect timeout=25)')  
Process NetcraftEnum-7:  
Traceback (most recent call last):  
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap  
    self.run()  
  ~~~~~^A  
  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 570, in enumerate  
    cookies = self.get_cookies(resp.headers)  
AttributeError: 'NoneType' object has no attribute 'headers'  
Process DNSdumpster-8:  
Traceback (most recent call last):  
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap  
    self.run()  
  ~~~~~^A  
  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_csrftoken(resp)  
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken  
    token = csrf_regex.findall(resp)[0]  
IndexError: list index out of range
```

25°C Mostly cloudy      06 September 2025 Sat 20:17 (local time)      20:17 06:09 02:25

## Now Gathering Information Through Social Media

### Sites using Sherlock:

- First Install **Sherlock** by typing ‘sherlock command’.



```
shinchan@kali: ~
$ sudo apt install sherlock
Command 'sherlock' not found, but can be installed with:
sudo apt install sherlock
Do you want to install it? (N/y)
sudo apt install sherlock
[sudo] password for shinchan:
The following packages were automatically installed and are no longer required:
  libgdal36  libgeos3.13.1  libqt5ct-common1.8  libsoup-2.4-1  libvpx9
  libgdata-common  libhdf4-0-alt  libisframe1  libqt5c2a  libqt5c2b  libqt5c2c
  libgdata22  libgd3.1.1  libsigsegv2  libtheora0  python3-packaging-whl
Use 'sudo apt autoremove' to remove them.

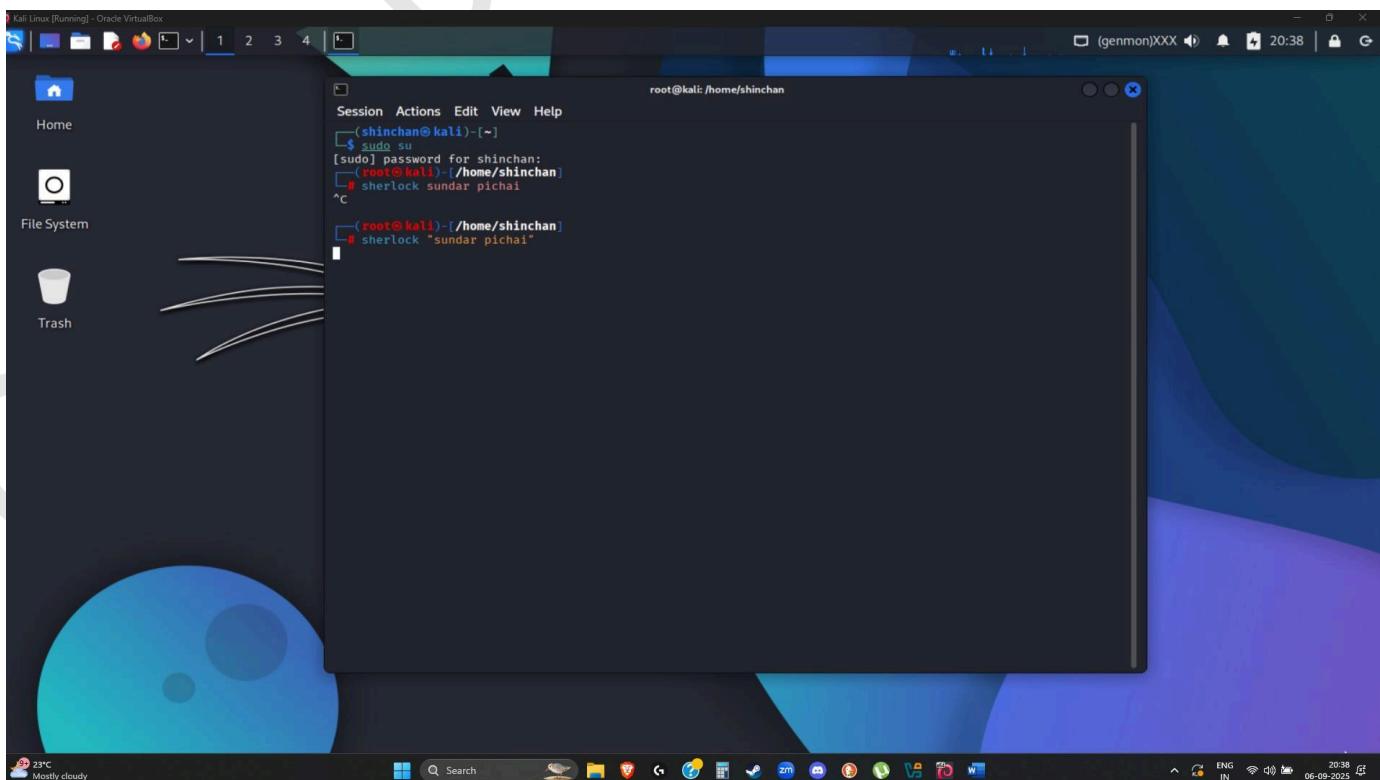
Installing:
  sherlock

Installing dependencies:
  python3-requests-futures  python3-stem

Summary:
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 3
  Download size: 356 kB
  Space needed: 1,848 kB / 40.7 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 python3-requests-futures all 1.0.2-1 [11.7 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 sherlock all 0.15.0-1 [35.5 kB]
Get:2 http://mirror.nyist.edu.cn/kali kali-rolling/main amd64 python3-stem all 1.8.2-1.1 [309 kB]
Fetched 356 kB in 13s (27.2 kB/s)
Selecting previously unselected package python3-requests-futures.
(Reading database ... 419646 files and directories currently installed.)
Preparing to unpack .../python3-requests-futures_1.0.2-1_all.deb ...
Unpacking python3-requests-futures (1.0.2-1) ...
Selecting previously unselected package python3-stem.
Preparing to unpack .../python3-stem_1.8.2-1.1_all.deb ...
Unpacking python3-stem (1.8.2-1.1) ...
Selecting previously unselected package sherlock.
Preparing to unpack .../sherlock_0.15.0-1_all.deb ...
Unpacking sherlock (0.15.0-1) ...
Setting up python3-stem (1.8.2-1.1) ...
```

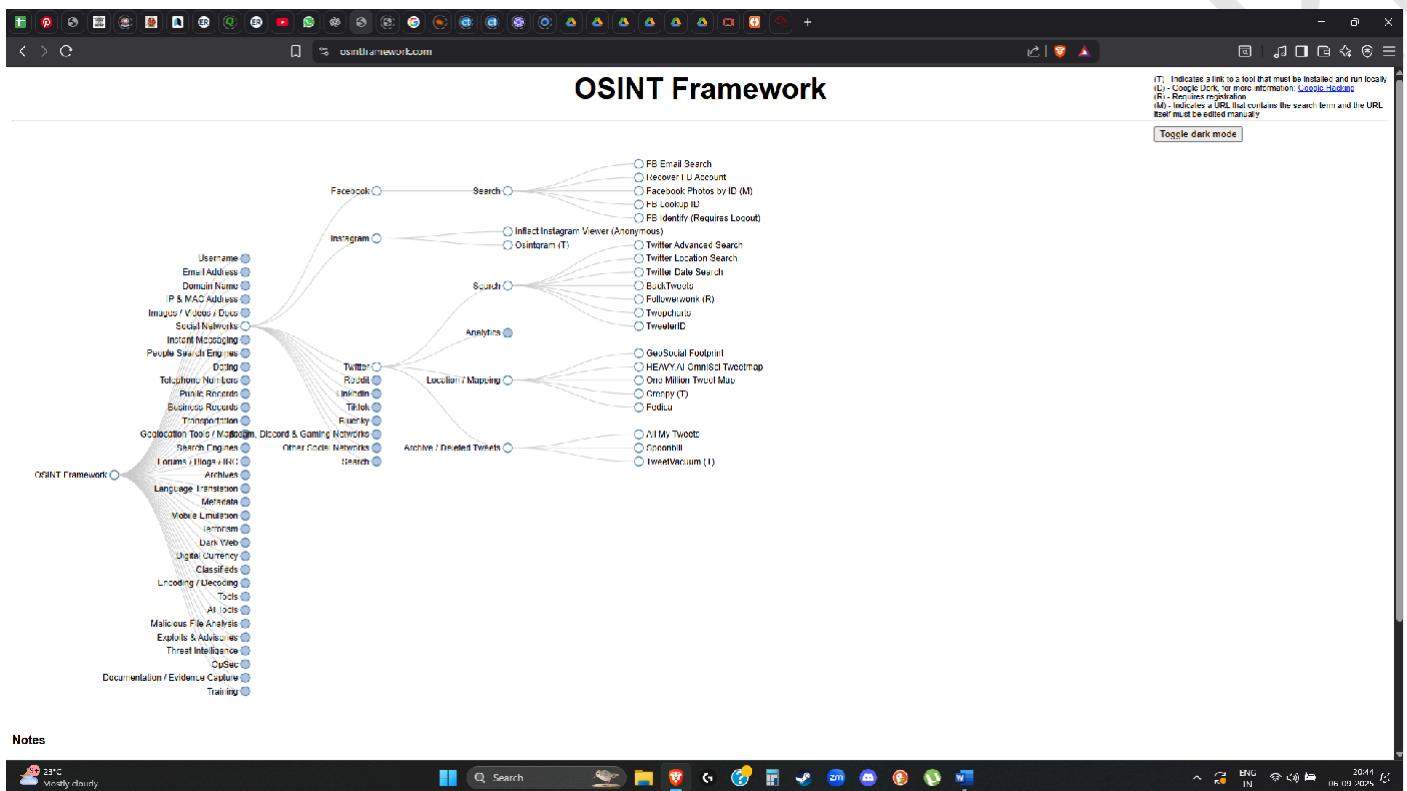
- Now use **Sherlock** to gather information, for example:



```
root@kali: /home/shinchan
$ sudo su
[sudo] password for shinchan:
[root@kali] -/home/shinchan
# sherlock sundar pichai
^C
[root@kali] -/home/shinchan
# sherlock "sundar pichai"
```

# Foot-Printing for Social Media Hacking using OSINT Framework:

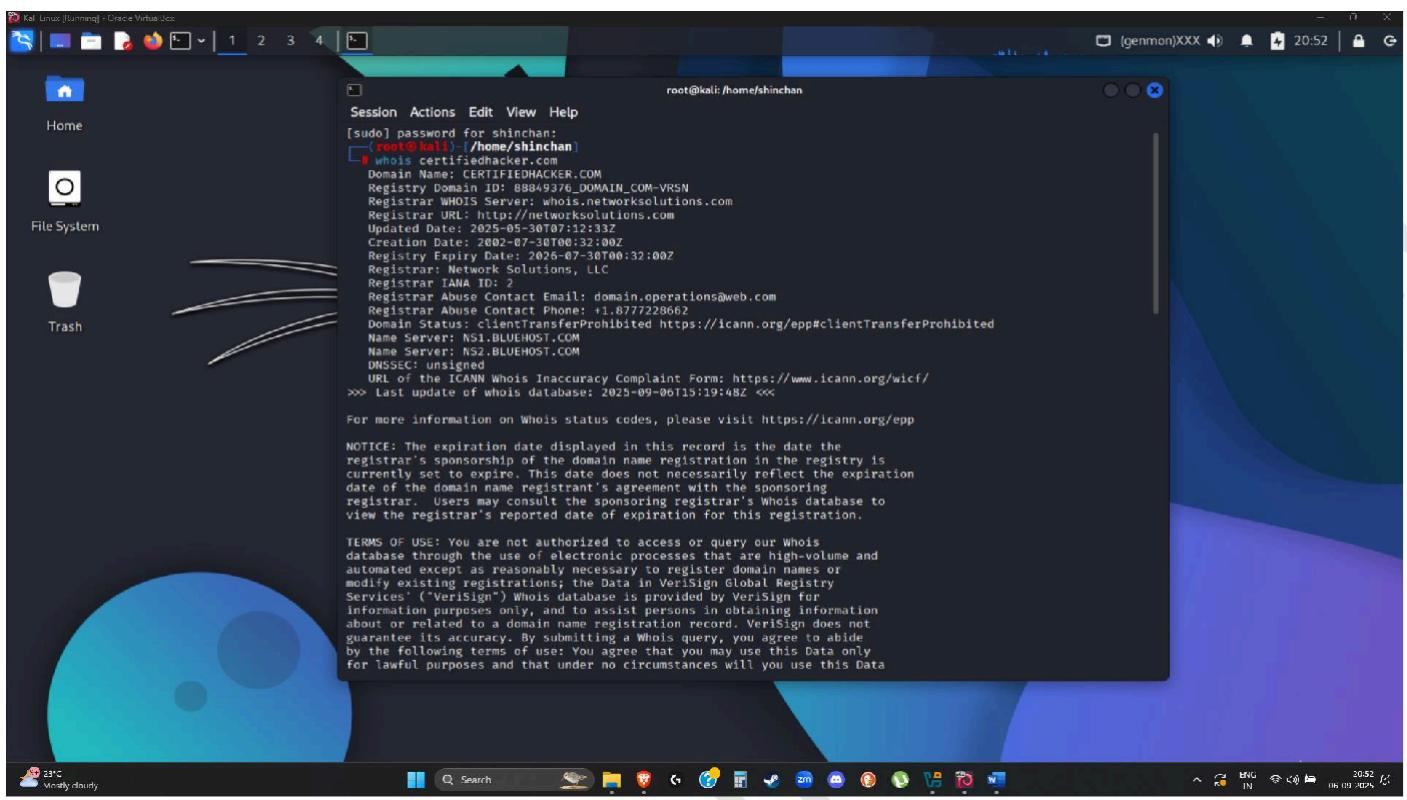
- Performed using OSINT Framework.



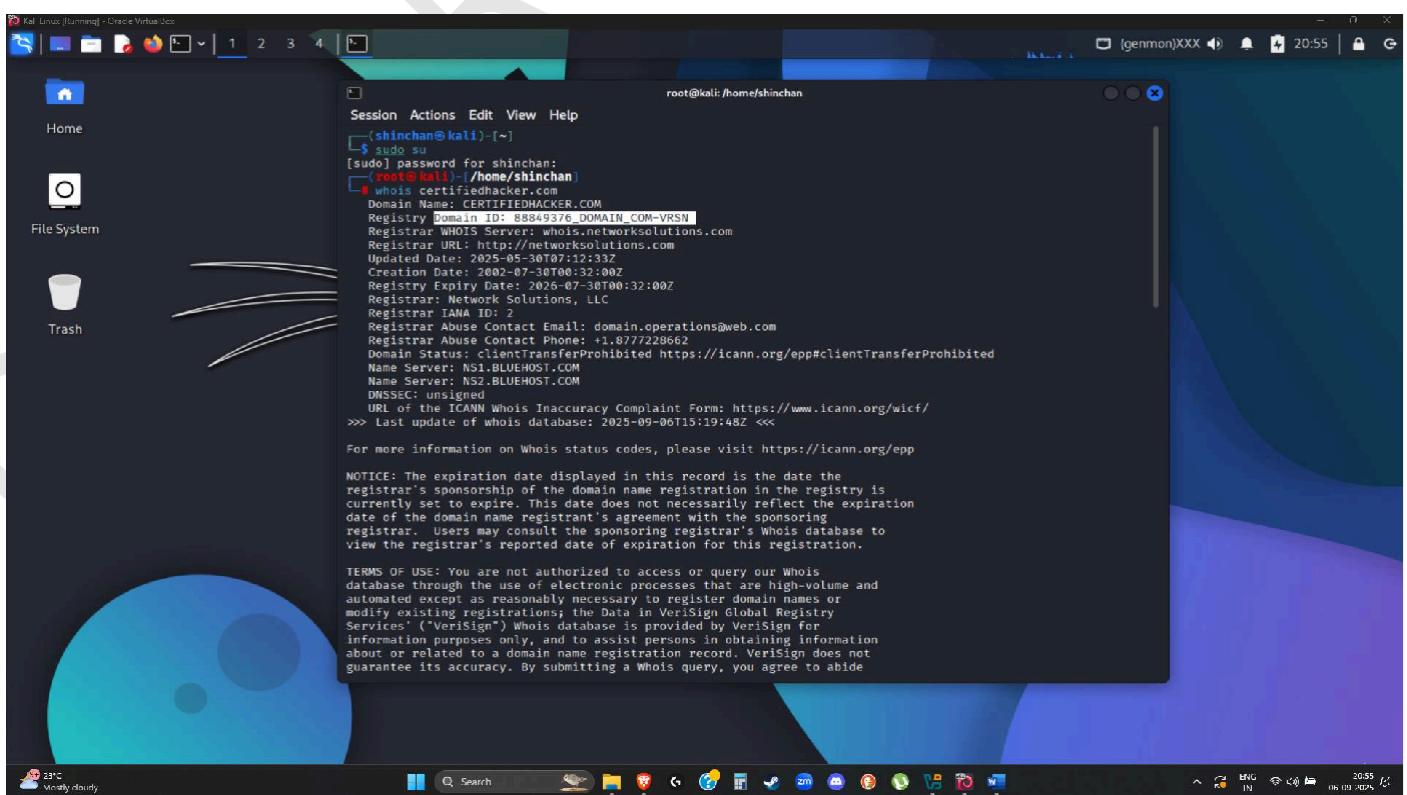
# Foot-Printing by performing Whois for Hacking:

- Performed to reveal available information on a Hostnames, ip addresses or Domains.
- Example next page:
- Like Domain name, Domain id

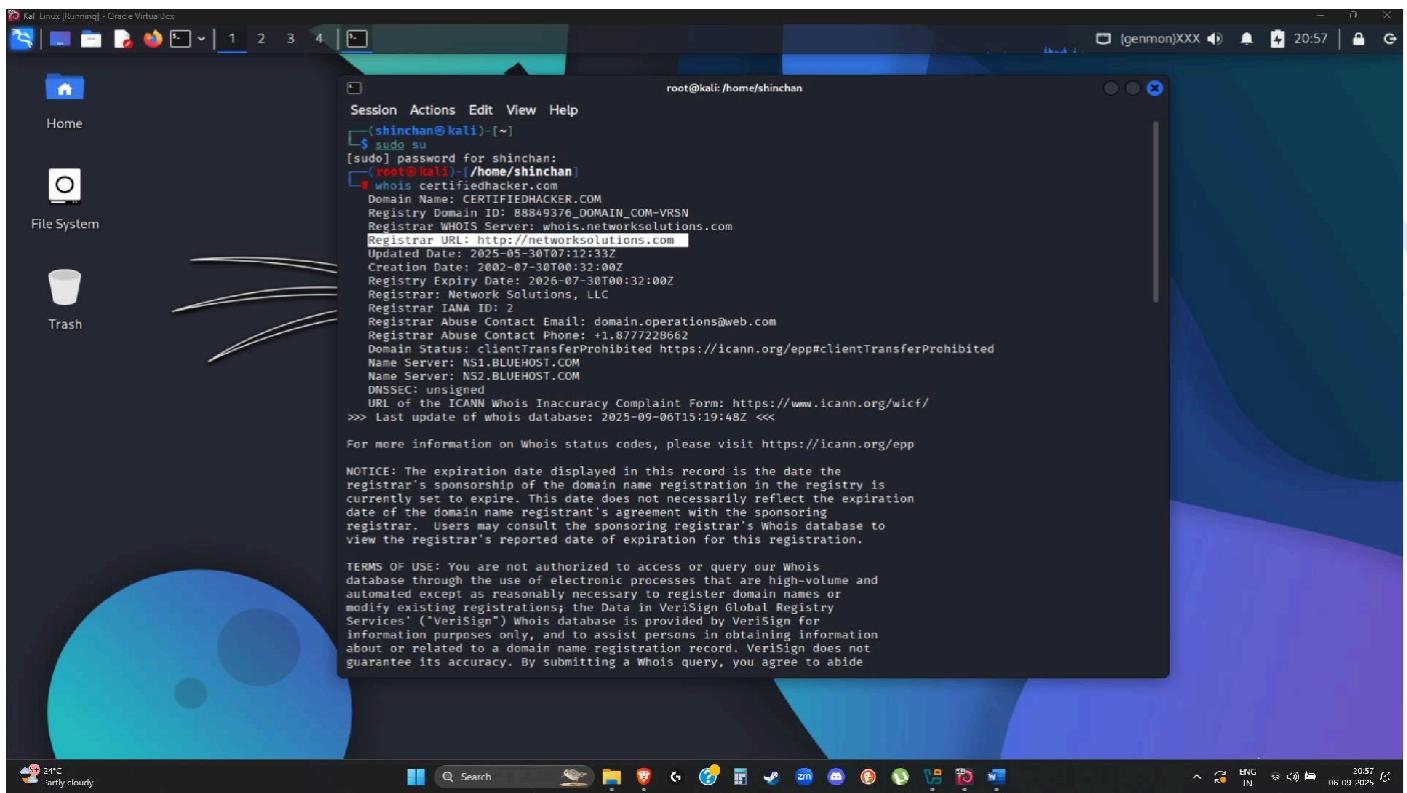
## □ Domain Name:



## □ Domain ID:



## Registrar URL:



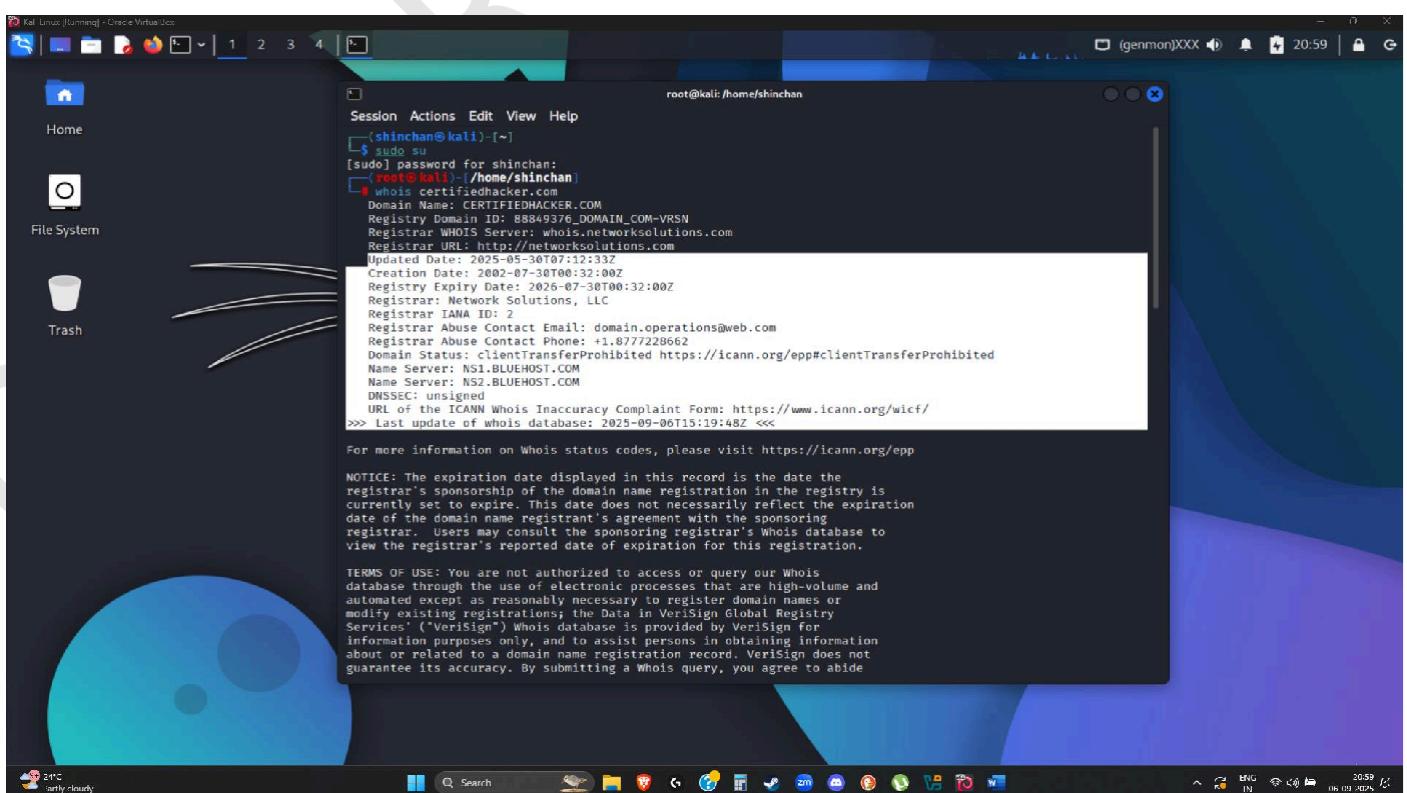
```
root@kali:~/home/shinchan
Session Actions Edit View Help
(shinchan㉿kali)-[~]
$ sudo su
[sudo] password for shinchan:
(shinchan㉿kali)-[~]
# whois certifiedhacker.com
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2025-05-30T07:12:33Z
Creation Date: 2002-07-30T00:32:00Z
Registry Expiry Date: 2026-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: domain.operations@web.com
Registrar Abuse Contact Phone: +1.8777228662
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: 2025-05-06T15:19:48Z <<<

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
```

## Everything you want regarding it:



```
root@kali:~/home/shinchan
Session Actions Edit View Help
(shinchan㉿kali)-[~]
$ sudo su
[sudo] password for shinchan:
(shinchan㉿kali)-[~]
# whois certifiedhacker.com
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2025-05-30T07:12:33Z
Creation Date: 2002-07-30T00:32:00Z
Registry Expiry Date: 2026-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: domain.operations@web.com
Registrar Abuse Contact Phone: +1.8777228662
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: 2025-05-06T15:19:48Z <<<

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
```

## □ You may use Whois Domain and search on Search Engines:

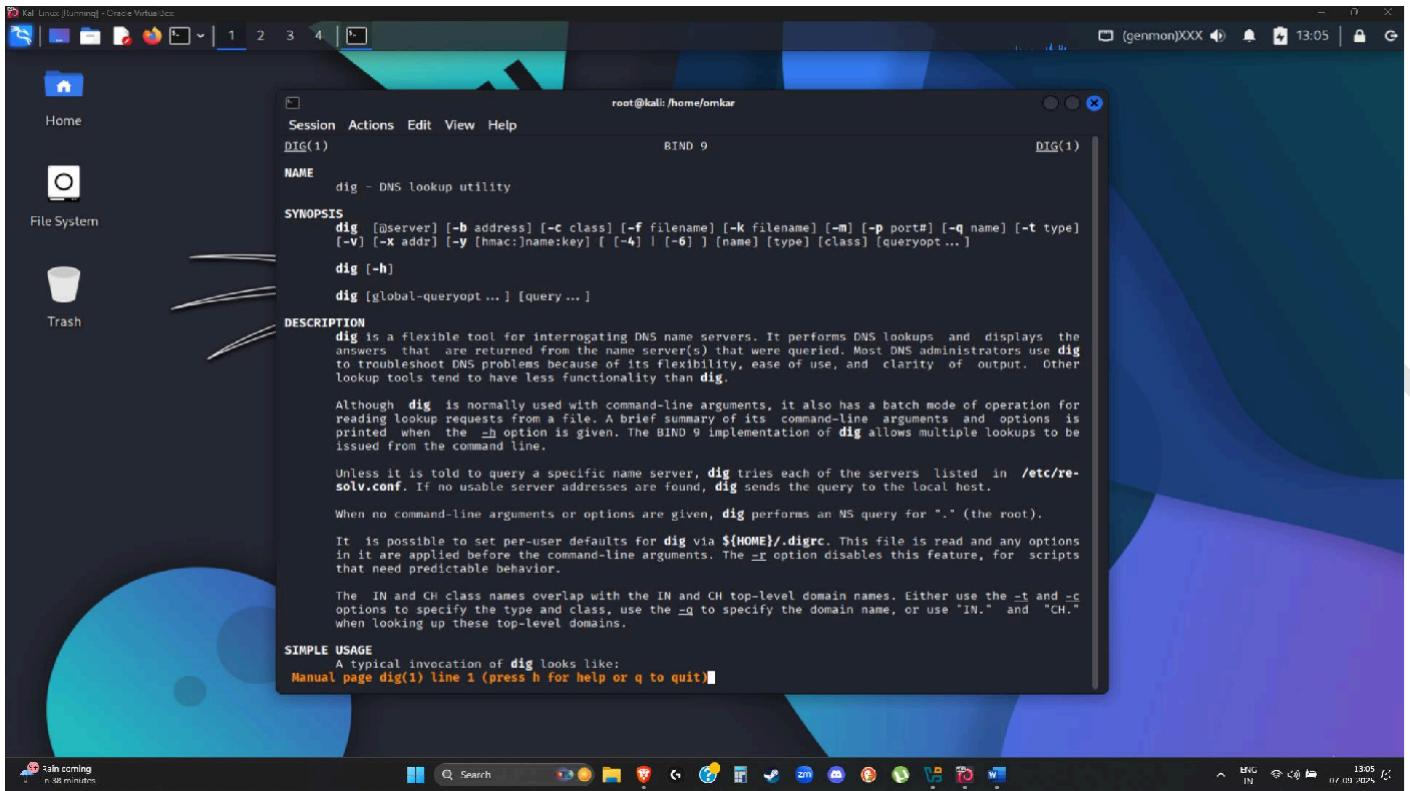
The screenshot shows a web browser window for shop.whois.com. The search bar at the top contains 'certifiedhacker.com'. Below the search bar, it says 'certifiedhacker.com' and 'Unavailable'. A button labeled 'Search again' is visible. Underneath, there's a section titled 'Other matching domains that are available' with a 'FILTER BY: PRICE EXACT MATCHES' dropdown. A list of domains is shown with their prices and discount percentages:

Domain	Length	Price	Discount	Action
certifiedhacker.in	1 year	\$14.88	50% off	Add to cart
certifiedhacker.space	1 year	\$29.99	\$1.18	Add to cart
certifiedhacker.top	1 year	\$4.99	\$1.08	Add to cart
certifiedhacker.me	1 year	\$2.28	50% off	Add to cart
certifiedhacker.site	1 year	\$3.28	50% off	Add to cart
certifiedhacker.online	1 year	\$5.28	50% off	Add to cart
certifiedhacker.life	1 year	\$2.48	\$3.60 off	Add to cart
certifiedhacker.fun	1 year	\$1.48	\$1.00 off	Add to cart

## Foot-Printing by performing DNS for Hacking:

DNS or Domain name System, reveals information about DNS zone data.

- Perform in Kali Linux- command man dig To understand DIG and its usage.



Kali Linux [Running] - Oracle VM VirtualBox

Session Actions Edit View Help

DIG(1) BIND 9 DIG(1)

**NAME**  
dig - DNS lookup utility

**SYNOPSIS**  
`dig [ @server ] [-b address] [-c class] [-f filename] [-k filename] [-m] [-p port#] [-q name] [-t type] [-v] [-x addr] [-y [hmac:]name:key] [ [-4] | [-6] ] [name] [type] [class] [queryopt ...]`

`dig [-h]`

`dig [global-queryopt ...] [query ...]`

**DESCRIPTION**  
`dig` is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use `dig` to troubleshoot DNS problems because of its flexibility, ease of use, and clarity of output. Other lookup tools tend to have less functionality than `dig`.

Although `dig` is normally used with command-line arguments, it also has a batch mode of operation for reading lookup requests from a file. A brief summary of its command-line arguments and options is printed when the `-h` option is given. The BIND 9 implementation of `dig` allows multiple lookups to be issued from the command line.

Unless it is told to query a specific name server, `dig` tries each of the servers listed in `/etc/resolv.conf`. If no usable server addresses are found, `dig` sends the query to the local host.

When no command-line arguments or options are given, `dig` performs an NS query for "." (the root).

It is possible to set per-user defaults for `dig` via `~/.digrc`. This file is read and any options in it are applied before the command-line arguments. The `-f` option disables this feature, for scripts that need predictable behavior.

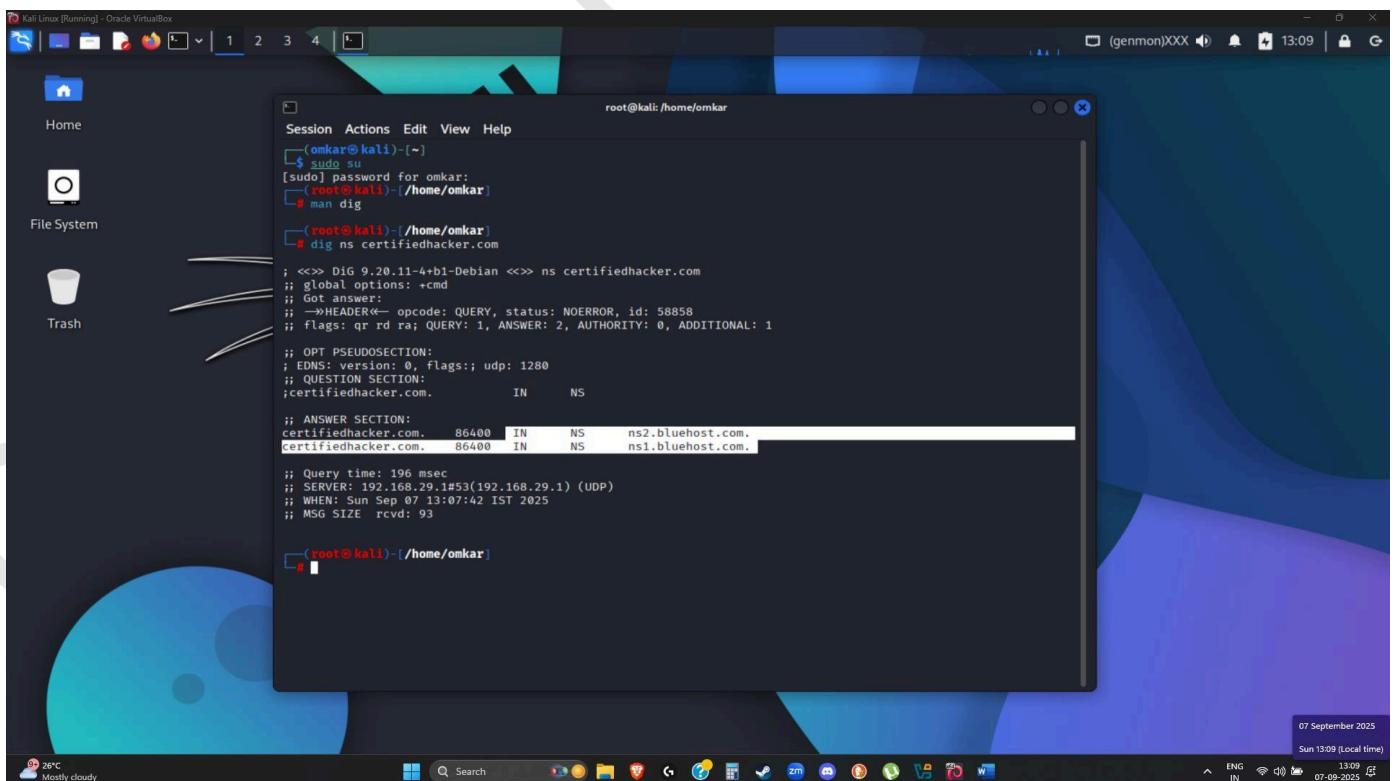
The IN and CH class names overlap with the IN and CH top-level domain names. Either use the `-t` and `-c` options to specify the type and class, use the `-q` to specify the domain name, or use "IN." and "CH." when looking up these top-level domains.

**SIMPLE USAGE**  
A typical invocation of `dig` looks like:  
`Manual page dig(1) line 1 (press h for help or q to quit)`

13:05 07/09/2023

- Perform in Kali Linux- command `dig ns certifiedhacker.com`

We found Name Server (NS) records of domain.



Kali Linux [Running] - Oracle VM VirtualBox

Session Actions Edit View Help

(omkar@kali)-[~]

\$ sudo su

[sudo] password for omkar:

(root@kali)-[/home/omkar]

# man dig

(root@kali)-[/home/omkar]

# dig ns certifiedhacker.com

```
; <>> DIG 9.20.11-4+b1-Debian <>> ns certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<- opcode: QUERY, status: NOERROR, id: 58858
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com.      IN      NS

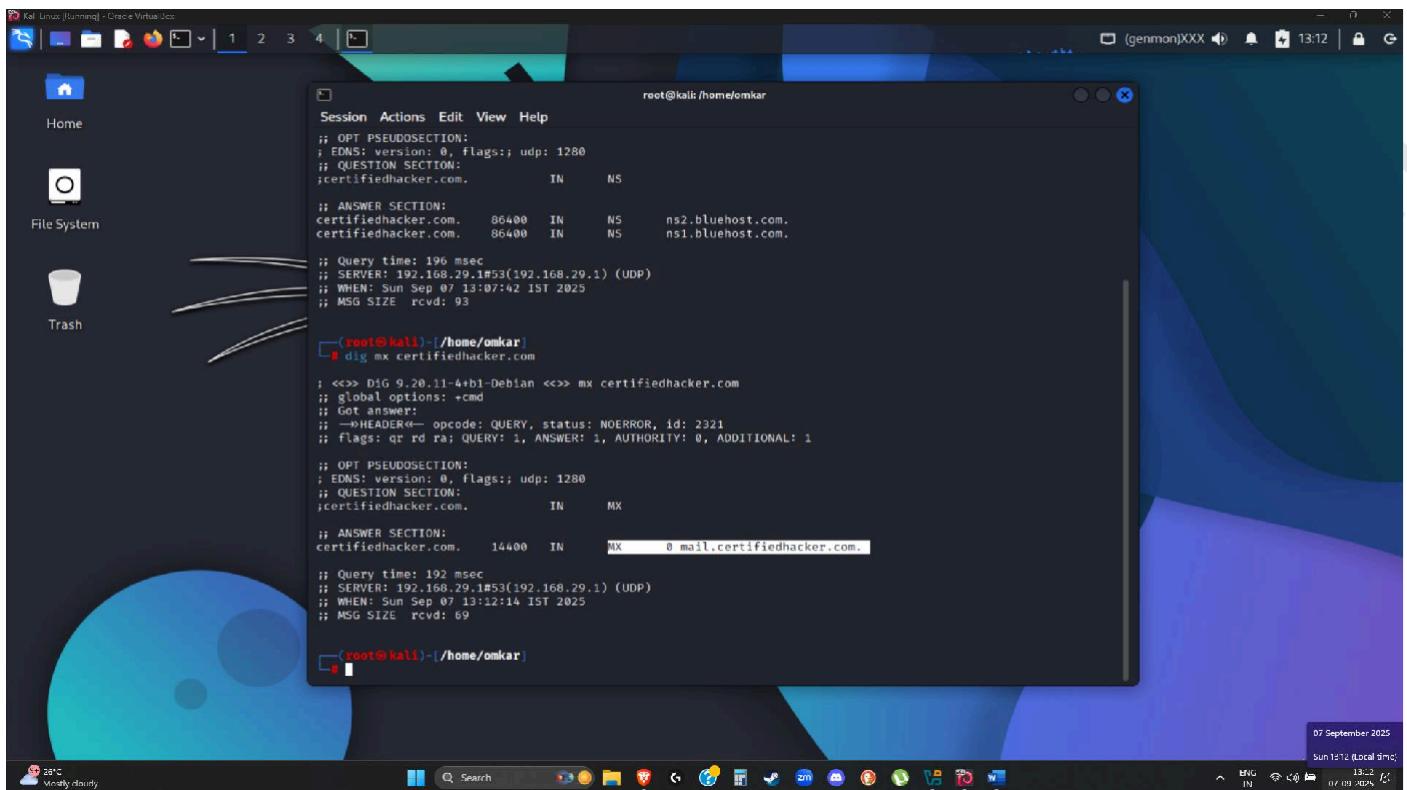
;; ANSWER SECTION:
certifiedhacker.com.  86400   IN      NS      ns2.bluehost.com.
certifiedhacker.com.  86400   IN      NS      ns1.bluehost.com.

;; Query time: 196 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Sun Sep 07 13:07:42 IST 2025
;; MSG SIZE  rcvd: 93
```

(root@kali)-[/home/omkar]

07 September 2025  
Sun 13:09 (Local time)  
26°C Mostly cloudy

- Perform in Kali Linux- command `dig mx certifiedhacker.com`  
To find mx (mail)record of domain



```
root@kali:~/home/omkar
Session Actions Edit View Help
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com.      IN      NS

;; ANSWER SECTION:
certifiedhacker.com.    86400   IN      NS      ns2.bluehost.com.
certifiedhacker.com.    86400   IN      NS      ns1.bluehost.com.

;; Query time: 196 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Sun Sep 07 13:07:42 IST 2025
;; MSG SIZE rcvd: 93

[root@kali]# dig mx certifiedhacker.com

; <>> DIG 9.20.11-4+b1-Debian <>> mx certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 2321
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

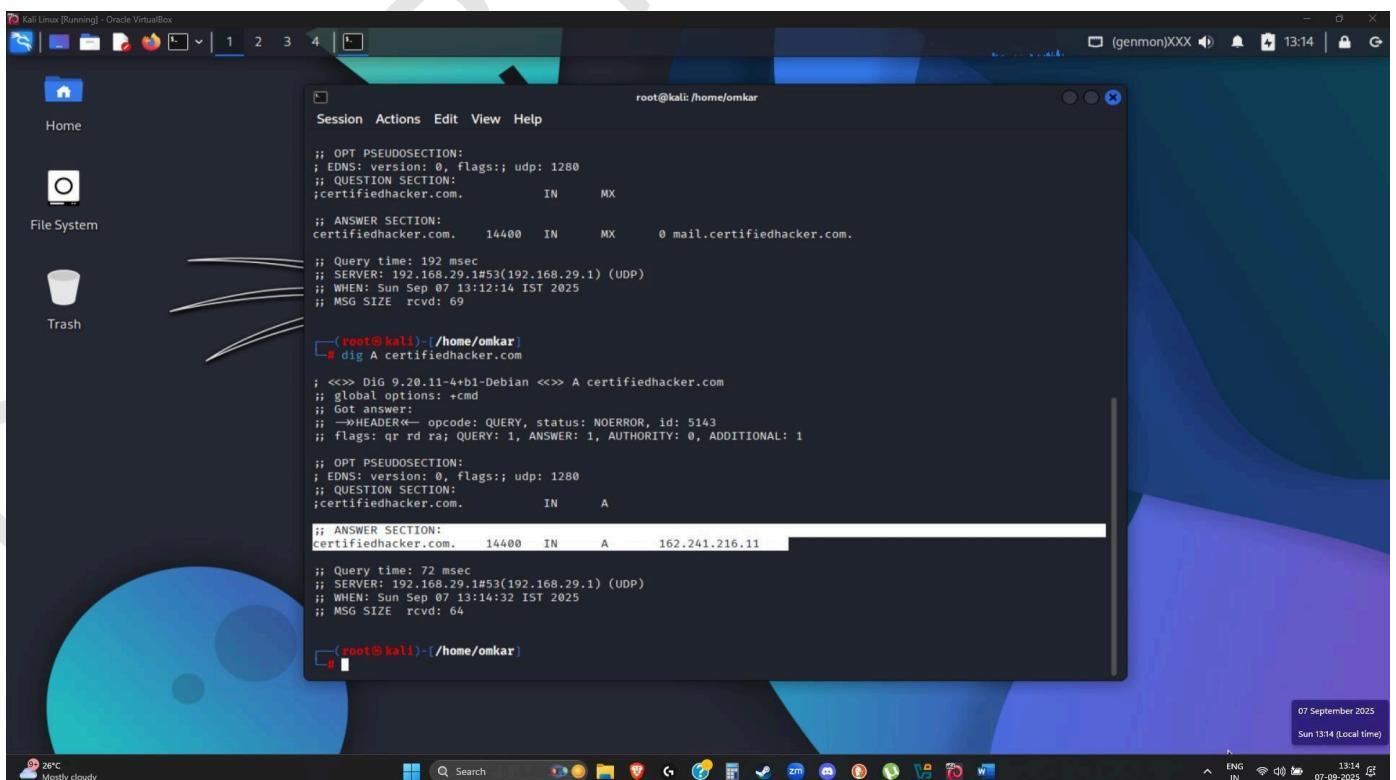
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com.      IN      MX

;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      MX      0 mail.certifiedhacker.com.

;; Query time: 192 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Sun Sep 07 13:12:14 IST 2025
;; MSG SIZE rcvd: 69

[root@kali]#
```

- Perform in Kali Linux- command `dig A certifiedhacker.com`  
To find A (means ip) record of domain



```
root@kali:~/home/omkar
Session Actions Edit View Help
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com.      IN      MX

;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      MX      0 mail.certifiedhacker.com.

;; Query time: 192 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Sun Sep 07 13:12:14 IST 2025
;; MSG SIZE rcvd: 69

[root@kali]# dig A certifiedhacker.com

; <>> DIG 9.20.11-4+b1-Debian <>> A certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 5143
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

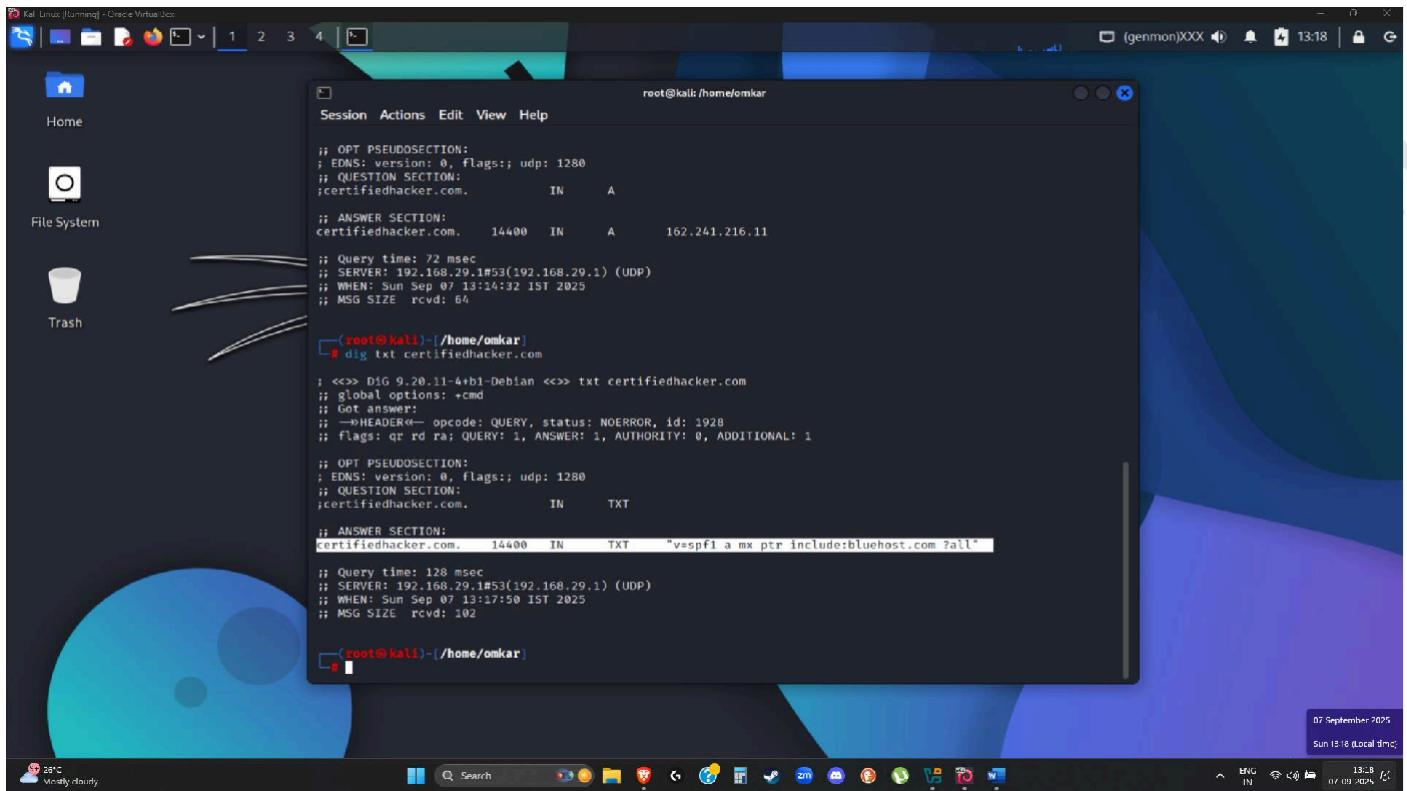
;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      A       162.241.216.11

;; Query time: 72 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Sun Sep 07 13:14:32 IST 2025
;; MSG SIZE rcvd: 64

[root@kali]#
```

- Perform in Kali Linux- command `dig txt certifiedhacker.com`

To find TXT record of domain



```
root@kali:~/home/omkar
Session Actions Edit View Help

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com.      IN      A
;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      A      162.241.216.11
;; Query time: 72 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Sun Sep 07 13:14:32 IST 2025
;; MSG SIZE rcvd: 64

[root@kali]-(~/home/omkar)
# dig txt certifiedhacker.com

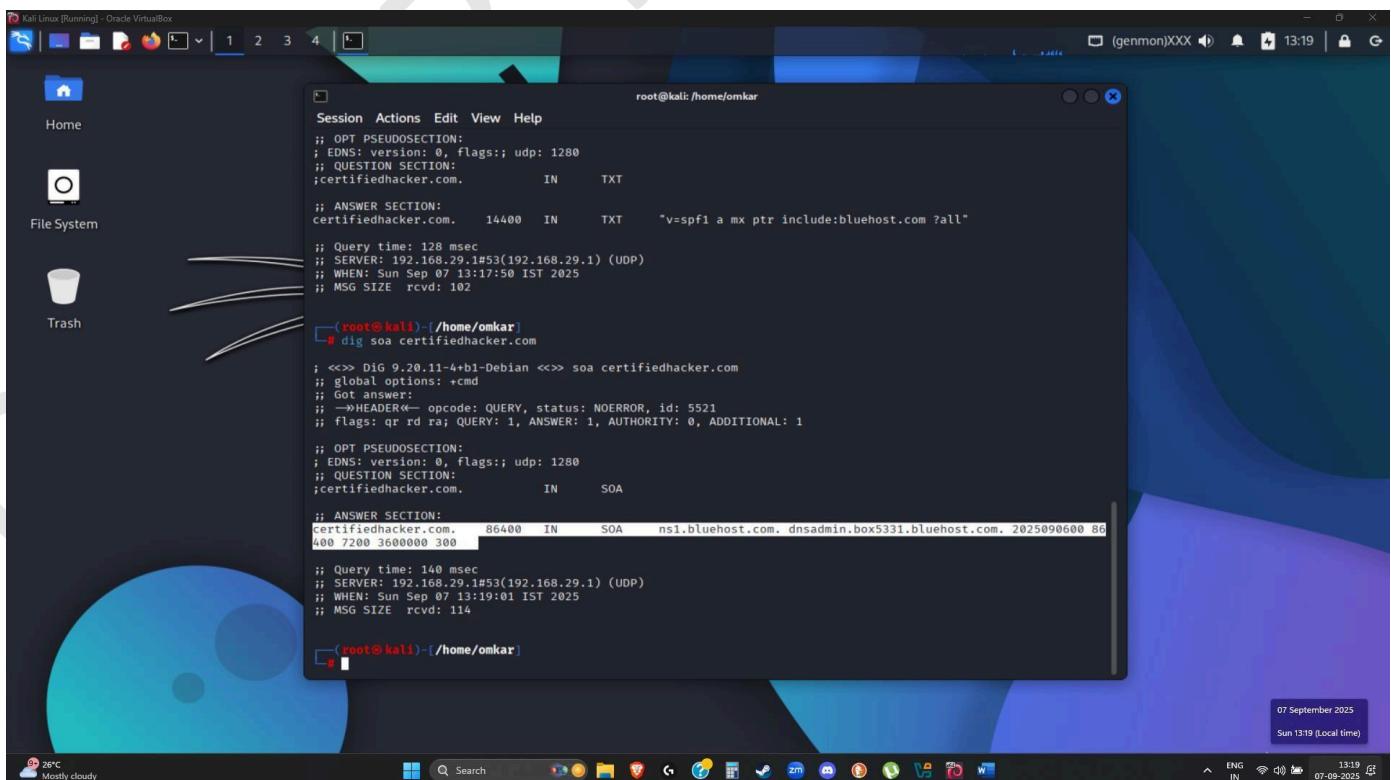
; <>> DIG 9.20.11-4+b1-Debian <>> txt certifiedhacker.com
; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 1928
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com.      IN      TXT
;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      TXT    "v=spf1 a mx ptr include:bluehost.com ?all"
;; Query time: 128 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Sun Sep 07 13:17:50 IST 2025
;; MSG SIZE rcvd: 102

[root@kali]-(~/home/omkar)
#
```

- Perform in Kali Linux- command `dig soa certifiedhacker.com`

To find SOA record of domain



```
root@kali:~/home/omkar
Session Actions Edit View Help

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com.      IN      TXT
;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      TXT    "v=spf1 a mx ptr include:bluehost.com ?all"
;; Query time: 128 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Sun Sep 07 13:17:50 IST 2025
;; MSG SIZE rcvd: 102

[root@kali]-(~/home/omkar)
# dig soa certifiedhacker.com

; <>> DIG 9.20.11-4+b1-Debian <>> soa certifiedhacker.com
; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 5521
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

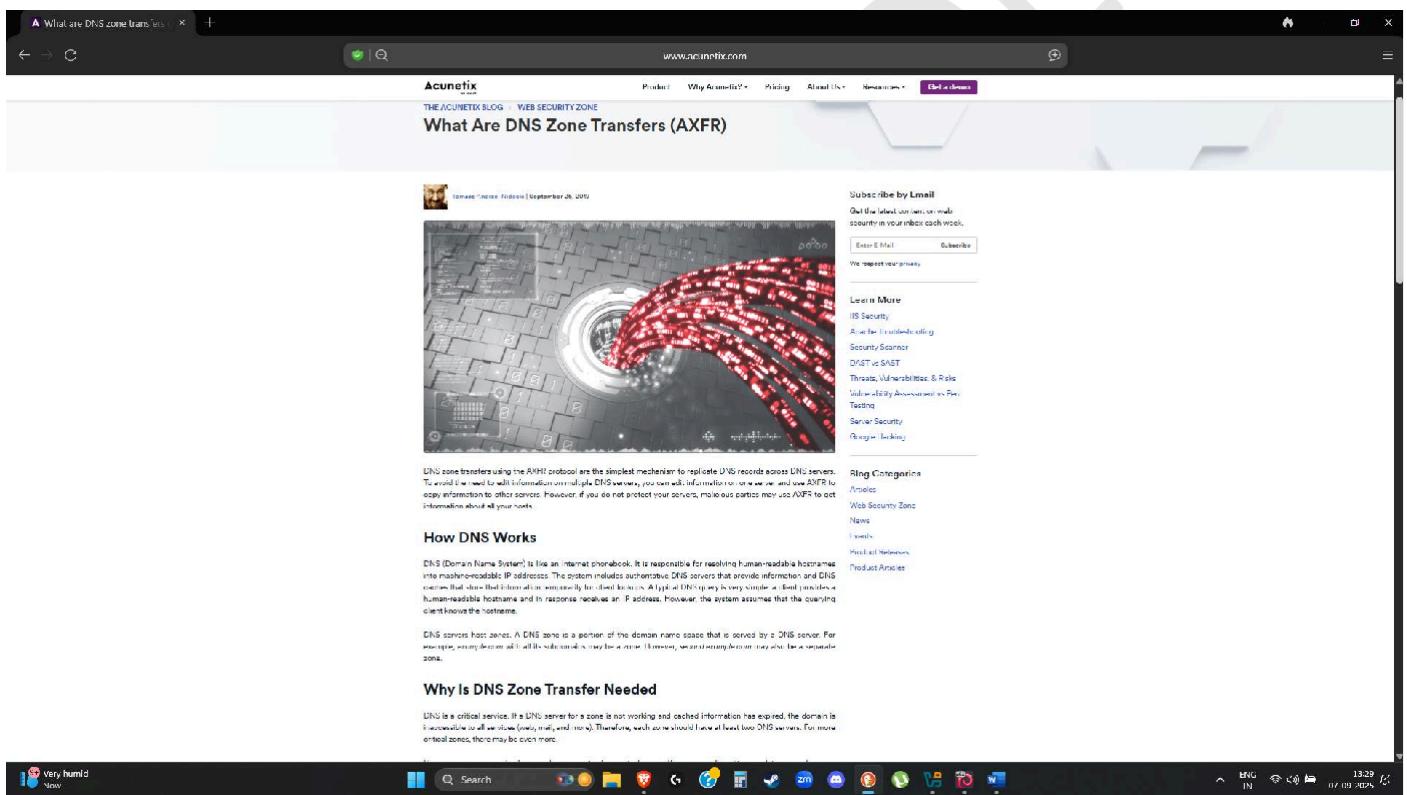
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;certifiedhacker.com.      IN      SOA
;; ANSWER SECTION:
certifiedhacker.com.    86400   IN      SOA    ns1.bluehost.com. dnsadmin.box5331.bluehost.com. 2025090600 86
400 7200 3600000 300
;; Query time: 140 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Sun Sep 07 13:19:01 IST 2025
;; MSG SIZE rcvd: 114

[root@kali]-(~/home/omkar)
#
```

## □ You may use DNS Zone and search on Search Engines to understand:

Performing it and creating its **Replica (Clone)**, so that the system which provides information and DNS caches that will store that information for client lookups.

Which shows how using AXFR, in creating a replica offering in no authentication and in order to prevent vulnerability from occurring, the DNS server should be configured to only allow zone transfer from trusted ip addresses.



- Now Perform in **Kali Linux**- command `dig @ns1.bluehost.com certifiedhacker.com axfr`

To perform zone transfer to domain, if its success then there's a clone and if Transfer failed, no need to create a Replica.

```

root@kali:~/home/omkar
certifiedhacker.com. 86400 IN SOA ns1.bluehost.com. dnsadmin.box5331.bluehost.com. 2025090600 86
400 7200 3600000 300

;; Query time: 140 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Sun Sep 07 13:19:01 IST 2025
;; MSG SIZE rcvd: 114

[root@kali:~/home/omkar] # dig @
[root@kali:~/home/omkar] # dig @ns1.bluehost.com certifiedhacker.com -AXFR
Invalid option: -AXFR
Usage: dig [@global-server] [domain] [q-type] [q-class] {q-opt}
      {global-d-opt} host {@local-server} {local-d-opt}
      [ host {@local-server} {local-d-opt} [ ... ]]

Use "dig -h" (or "dig -h | more") for complete list of options
[root@kali:~/home/omkar] # dig @ns1.bluehost.com certifiedhacker.com -axfr
Invalid option: -axfr
Usage: dig [@global-server] [domain] [q-type] [q-class] {q-opt}
      {global-d-opt} host {@local-server} {local-d-opt}
      [ host {@local-server} {local-d-opt} [ ... ]]

Use "dig -h" (or "dig -h | more") for complete list of options
[root@kali:~/home/omkar] # dig @ns1.bluehost.com certifiedhacker.com axfr
; <>> DIG 9.20.11-4+deb1-Debian <>> @ns1.bluehost.com certifiedhacker.com axfr
; (1 server found)
; global options: +cmd
; Transfer failed.

[root@kali:~/home/omkar] #

```

## □ You may use Kloth DNS and search on Search

### Engines to understand:

You may search records of TXT, SOA, AFXR, etc. in Kloth.net

KLOTH.NET - NSLOOKUP - DNS

www.kloth.net

NSLOOKUP: look up and find IP addresses in the DNS

Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.

This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or other internet abuse.

This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots.

NSLOOKUP

Domain:  ... the name of the machine to look up.

Server:  ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query: A (IPv4 address)

Look it up

The DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup manual (man page).

Basic usage: nslookup [domain] [server] [options]

To resolve an IP address to a host name, use ANY (any type).

Like the PTR record, CNAME (canonical name) is used to map one host name to another.

You can't tell if a host has a PTR record.

If you prefer to use the standard nslookup command, use nslookup [domain] [server] [options].

Link to www: nslookup [domain] [server] [options]

Recommended: nslookup [domain] [server] [options]

You are coming from a DNS reverse zone. If you prefer to use the standard nslookup command, use nslookup [domain] [server] [options].

Current date: 07-09-07 08:16:44. This is the 250th day of this year.

Document URL: <http://www.kloth.net/services/nslookup>

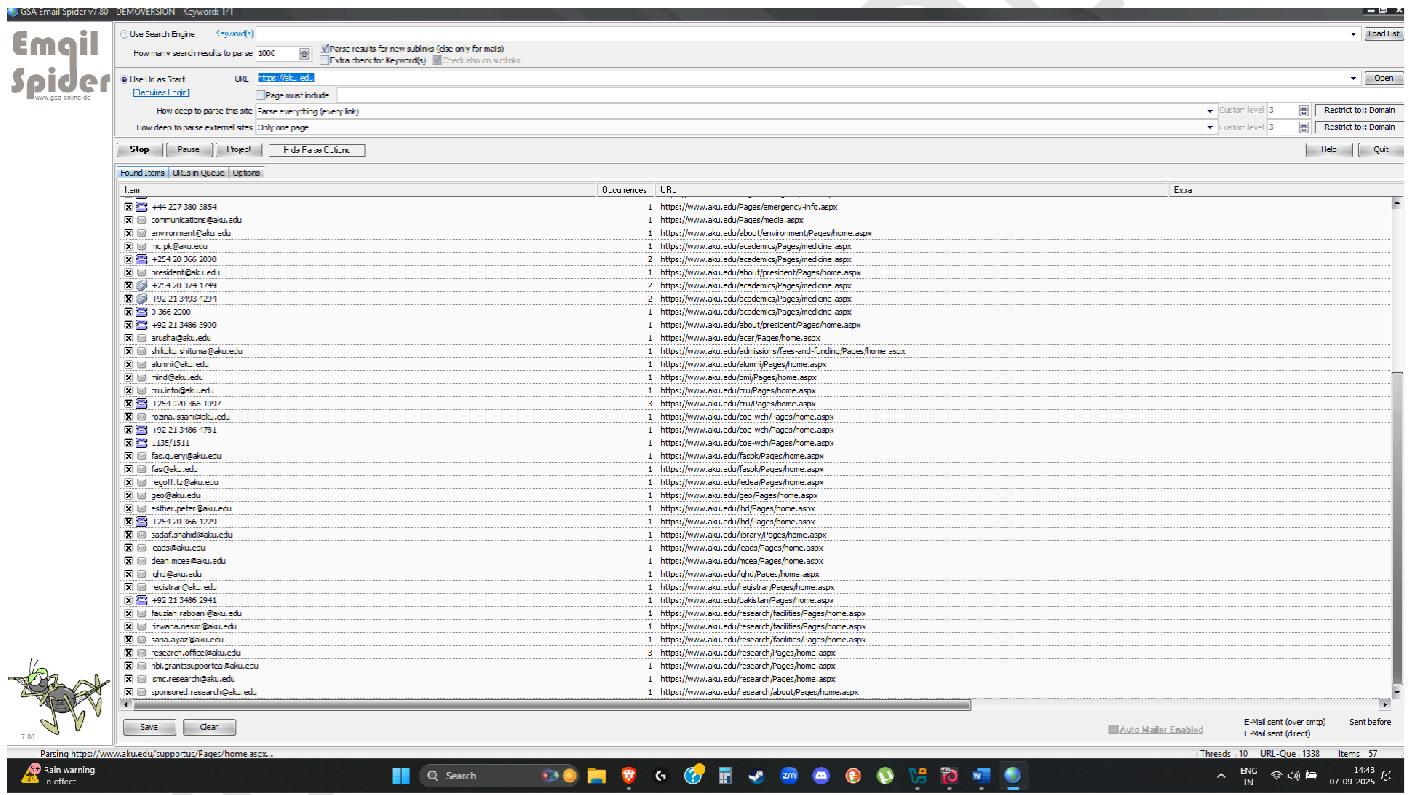
Copyright © 1999-2025 LessInventive 2025.09.07.08:16:44. Your visit 2025-09-07 08:16:44. Page created in 20.061 sec.

[Go to the top of this page] [... to the index page]



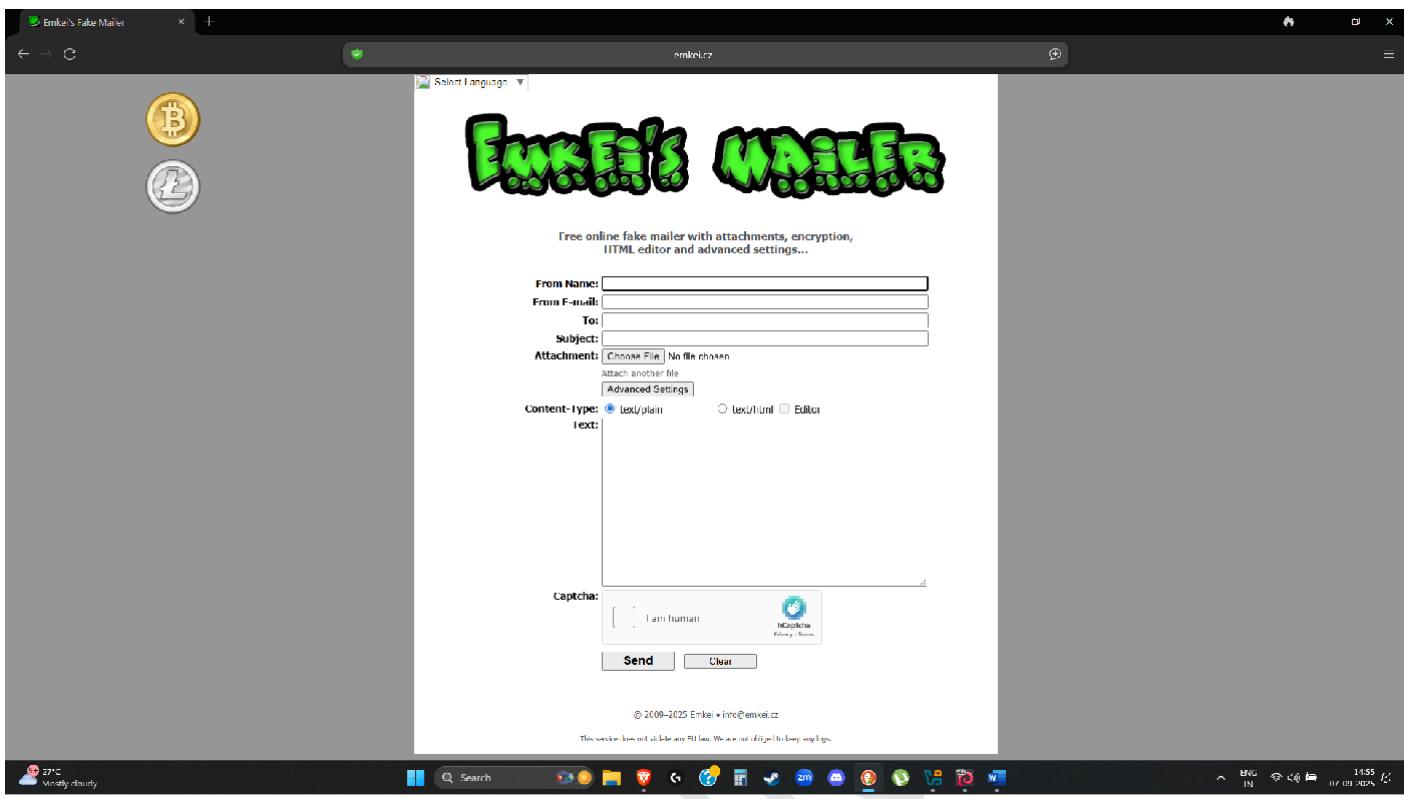
# Performing E-mail Foot-Printing for Hacking:

- Before Performing E-mail Foot-Printing Download **GSA Email Spider**.
- Type URL and next
- Now its Exploring E-mails, this is called (Spidering).



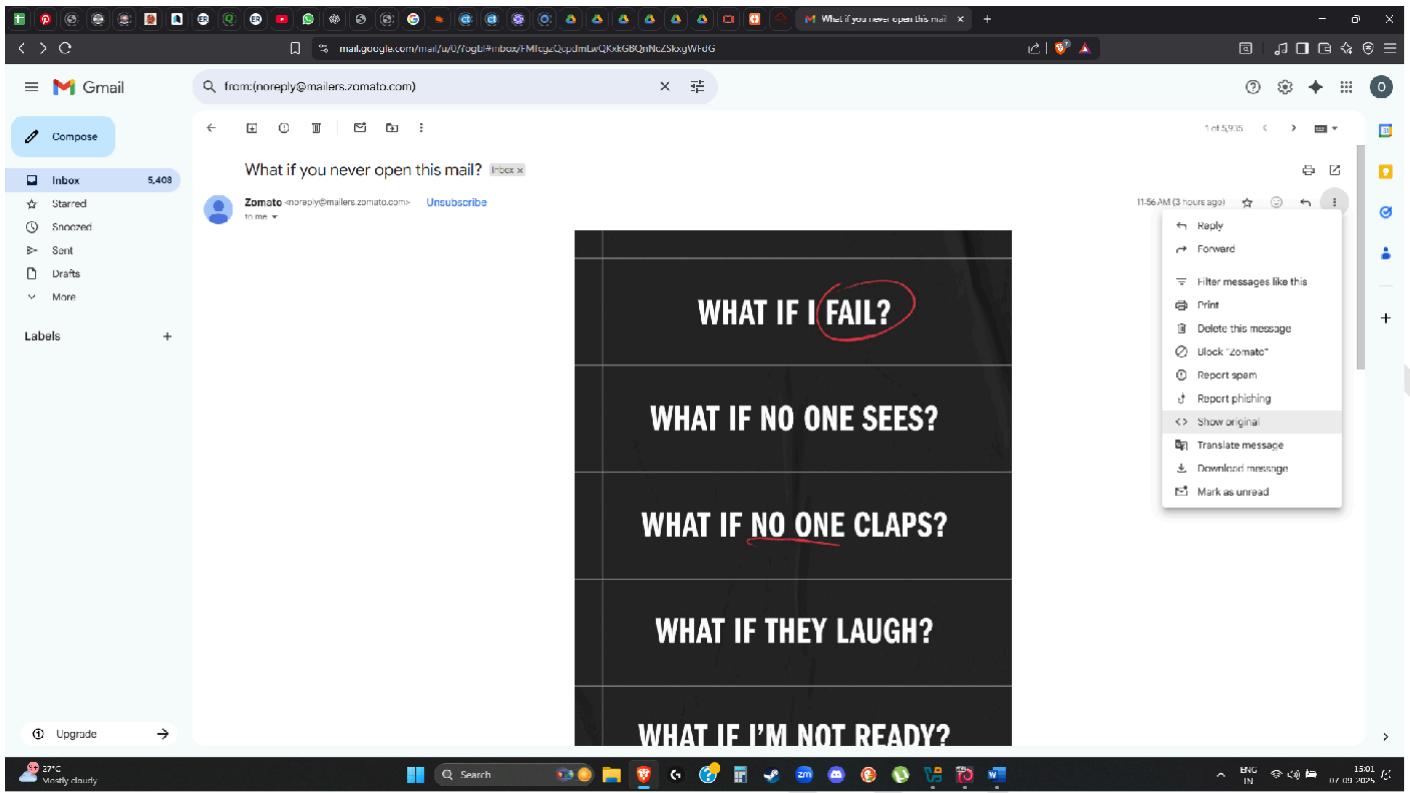
□ Now how fake E-mails are done through where, So to understand:

- Fake Email's are done through using Emkei's Mailer.



## □ Now how to know fake E-mails, So to avoid it:

- Example we will use **Gmail's account**.
- Open Gmail.
- Select mail, which you want to check.
- Now open it.
- Click on 3 Dots option and select **Show Original**.
- If its True, it will show “PASS”, for Fake it will show “SOFTFAIL”
- And it will also show E-mailed from Real Domain or Fake Domain.



- And now after gathering all information copy the information and use [mxtoolbox](#).
- In ‘[Analyze Header](#)’ paste the copied information.
- It will arrange it for you to understand it easily.

**ABOUT EMAIL HEADERS**

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop counts, anti-spam results and more. If you need help getting copies of your email headers, just read this tutorial.

- Perform Network Trace Routing in Windows

**Network Foot-Printing** is the process of gathering information of target organization.

- Example- **Ip address, Host name, Domain, Sub-Domains.**

- In this we can also check from our **network**, to whom we are **Targeting**.
- Also we can check between our **Network** and our **Target**, How many **Hops** and **Routers** are connected.

- Perform Network Trace Routing in Windows and Linux Machine:

- In Windows.
- Example- Open Command Prompt.
- Type **tracert** (any Domain) **certifiedhacker.com**.
- It will Trace route, showing **System Gateway** and till last how many **hops** and **ip's** are connected to **certifiedhacker**.

The screenshot shows a Windows Command Prompt window titled "Command Prompt - traceroute". The window displays the output of the "traceroute" command, which traces the route to the domain "certifiedhacker.com". The output shows 6 hops, with the final destination being "certifiedhacker.com [162.241.216.11]". The hops are listed as follows:

Hop	Time	Time	Time	Host
1	1 ms	1 ms	2 ms	reliance.reliance [192.168.29.1]
2	3 ms	2 ms	2 ms	10.66.248.1
3	3 ms	3 ms	3 ms	172.31.3.64
4	66 ms	63 ms	46 ms	192.168.92.244
5	2 ms	2 ms	2 ms	172.26.106.117
6	4 ms	4 ms	3 ms	

- In Kali Linux.
- Example- Open Terminal.
- Type **traceroute** (any Domain) **certifiedhacker.com**.
- It will Trace route, showing **System Gateway** and till last how many **hops** and **ip's** are connected to certifiedhacker.

```

Session Actions Edit View Help
[sudo] password for omkar:
[root@kali:~/home/omkar]
# traceroute certifethacker.com
traceroute to certifethacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1  Reliance_reliance (192.168.29.1) 7.511 ms 7.599 ms
 2  10.66.248.1 (10.66.248.1) 9.175 ms 8.161 ms 8.168 ms
 3  172.31.3.60 (172.31.3.60) 8.136 ms 8.145 ms 8.133 ms
 4  192.168.92.242 (192.168.92.242) 8.012 ms 192.168.92.240 (192.168.92.240) 7.931 ms 192.168.92.244 (192.168.92.244) 8.941 ms
 5  172.26.106.117 (172.26.106.117) 7.853 ms 7.865 ms 7.836 ms
 6  172.26.106.99 (172.26.106.99) 8.539 ms 3.350 ms 172.26.106.98 (172.26.106.98) 3.613 ms
 7  192.168.92.166 (192.168.92.166) 3.869 ms 192.168.92.164 (192.168.92.164) 7.357 ms 192.168.92.166 (192.168.92.166) 8.916 ms
 8  * * *
 9  * * *
10  103.198.140.176 (103.198.140.176) 13.069 ms 12.978 ms 12.887 ms
11  103.198.140.56 (103.198.140.56) 197.060 ms 103.198.140.54 (103.198.140.54) 109.515 ms 103.198.140.211 (103.198.140.211) 120.547 ms
12  * * *
13  130.117.14.54 (130.117.14.54) 147.049 ms mei-b5-link.ip.twelve99.net (62.115.11.140) 160.489 ms 160.475 ms
14  prs-bb1-link.ip.twelve99.net (62.115.124.54) 160.464 ms prs-bb2-link.ip.twelve99.net (62.115.124.56) 165.684 ms 173.962 ms
15  adm-bb1-link.ip.twelve99.net (62.115.134.96) 272.549 ms ffm-bb1-link.ip.twelve99.net (62.115.123.12) 274.034 ms ldn-bb1-link.ip.twelve99.net (62.115.135.24) 165.552 ms
16  ewr-bb2-link.ip.twelve99.net (62.115.139.246) 239.816 ms 256.311 ms nyk-bb5-link.ip.twelve99.net (62.115.139.244) 236.996 ms
17  chi-bb2-link.ip.twelve99.net (62.115.132.135) 241.813 ms nyk-b17-link.ip.twelve99.net (62.115.137.19) 247.228 ms chi-bb1-link.ip.twelve99.net (62.115.139.33) 240.098 ms
18  * kanc-bb2-link.ip.twelve99.net (62.115.136.103) 236.762 ms 236.872 ms
19  * * *
20  chi-b23-link.ip.twelve99.net (62.115.126.159) 248.126 ms salt-b4-link.ip.twelve99.net (62.115.132.207) 244.836 ms 245.456 ms
21  salt-bs5-link.ip.twelve99.net (62.115.136.107) 258.898 ms 252.193 ms chi-bb1-link.ip.twelve99.net (62.115.140.108) 240.108 ms 244.15 ms
22  chi-b23-link.ip.twelve99.net (62.115.126.159) 263.579 ms dcm-bb1-link.ip.twelve99.net (62.115.115.76) 253.746 ms nowroldigital-lc-380138.ip.twelve99-cust.net (80.239.167.103) 245.718 ms
23  69.195.64.105.unifiedlayer.com (69.195.64.105) 242.800 ms chi-bb1-link.ip.twelve99.net (62.115.140.108) 259.181 ms 69.195.64.105.unifiedlayer.com (69.195.64.105) 243.099 ms
24  po97.prv-leafia.net.unifiedlayer.com (162.144.248.123) 242.166 ms salt-b4-link.ip.twelve99.net (62.115.13)

```

## Tool to find how many Systems are there in Network:

- Tool is Angry IP Scanner:

IP	Ping	Fingerprint	Ports [?]
192.168.1.1	[Up]	[n/a]	
192.168.1.2	[Up]	[n/a]	
192.168.1.3	[Up]	[n/a]	
192.168.1.4	[Up]	[n/a]	
192.168.1.5	[Up]	[n/a]	
192.168.1.6	[Up]	[n/a]	
192.168.1.7	[Up]	[n/a]	
192.168.1.8	[Up]	[n/a]	
192.168.1.9	[Up]	[n/a]	
192.168.1.10	[Up]	[n/a]	
192.168.1.11	[Up]	[n/a]	
192.168.1.12	[Up]	[n/a]	
192.168.1.13	[Up]	[n/a]	
192.168.1.14	[Up]	[n/a]	
192.168.1.15	[Up]	[n/a]	
192.168.1.16	[Up]	[n/a]	
192.168.1.17	[Up]	[n/a]	
192.168.1.18	[Up]	[n/a]	
192.168.1.19	[Up]	[n/a]	
192.168.1.20	[Up]	[n/a]	
192.168.1.21	[Up]	[n/a]	
192.168.1.22	[Up]	[n/a]	
192.168.1.23	[Up]	[n/a]	
192.168.1.24	[Up]	[n/a]	
192.168.1.25	[Up]	[n/a]	
192.168.1.26	[Up]	[n/a]	
192.168.1.27	[Up]	[n/a]	
192.168.1.28	[Up]	[n/a]	
192.168.1.29	[Up]	[n/a]	
192.168.1.30	[Up]	[n/a]	
192.168.1.31	[Up]	[n/a]	
192.168.1.32	[Up]	[n/a]	
192.168.1.33	[Up]	[n/a]	
192.168.1.34	[Up]	[n/a]	
192.168.1.35	[Up]	[n/a]	
192.168.1.36	[Up]	[n/a]	
192.168.1.37	[Up]	[n/a]	
192.168.1.38	[Up]	[n/a]	
192.168.1.39	[Up]	[n/a]	
192.168.1.40	[Up]	[n/a]	
192.168.1.41	[Up]	[n/a]	
192.168.1.42	[Up]	[n/a]	
192.168.1.43	[Up]	[n/a]	
192.168.1.44	[Up]	[n/a]	
192.168.1.45	[Up]	[n/a]	
192.168.1.46	[Up]	[n/a]	

# Performing Reconnaissance Kali Linux:

- This **recon-ng** Tool in **Kali Linux** is used to gather information.
- It will show **no content**.
- Type next command **help**.
- And at last type command- **marketplace install all**.
- **It will start installing**.
- After installing, to check everything installed, command-**modules search**
- Now you can create your own **Workspaces**, command-**workspaces create CEHv13**.
- At last to check how many Workspace, command-**workspaces list**

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: /home/omkar'. The terminal content shows the following session:

```
Session Actions Edit View Help
[ omkar@kali ) - [ ~ ]
$ sudo su
[sudo] password for omkar:
[ root@kali ) - [ /home/omkar ]
# recon-ng
[*] Version check disabled.

Sponsored by ...
      ^   ^   ^
     / \ / \ \
    //  BLACK HILLS  \
   www.blackhillsinfosec.com

PRACTISEC
www.practise.com

[recon-ng] v5.1.2, Tim Tomes (@lanmaster53)

[*] No modules enabled/installed.

[recon-ng][default] > help

Commands (type [help?] <topic>):
back           Exits the current context
dashboard      Displays a summary of activity
db             Interfaces with the workspace's database
exit           Exits the framework
help           Displays this menu
index          Creates a module index (dev only)
keys           Manages third party resource credentials
marketplace    Interfaces with the module marketplace
modules        Interfaces with installed modules
options        Manages the current context options
pdb            Starts a Python Debugger session (dev only)
```

The desktop interface includes a file manager sidebar on the left and a taskbar at the bottom with various application icons.

Kali Linux [Running] - Oracle VM VirtualBox

root@kali: /home/omkar

```
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]  
[*] No modules enabled/installed.  
[recon-ng][default] > help  
Commands (type [help?] <topic>):  
back           Exits the current context  
dashboard      Displays a summary of activity  
db             Interfaces with the workspace's database  
exit           Exits the framework  
help           Displays this menu  
index          Creates a module index (dev only)  
keys           Manages third party resource credentials  
marketplace    Interfaces with the module marketplace  
modules        Interfaces with installed modules  
options        Manages the current context options  
pdb            Starts a Python Debugger session (dev only)  
script         Records and executes command scripts  
shell          Executes shell commands  
show           Shows various framework items  
snapshots      Manages workspace snapshots  
spool          Spools output to a file  
workspaces     Manages workspaces  
[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: recon/companies-contacts/bing_linkedin_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/viewsdns_reverse_whois  
[*] Module installed: recon/companies-domains/whoxy_dns  
[*] Module installed: recon/companies-multi/censys_org  
[*] Module installed: recon/companies-multi/censys_tls_subjects
```

07 September 2023  
Sun 005 (local time)

OMKAR H

```
Kali Linux [Running] - Oracle VM VirtualBox  
File Home File System Trash  
Session Actions Edit View Help  
[!] 'censysio_id' key not set. censysio module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_secret' key not set. censysio module will likely fail at runtime. See 'keys add'.  
[!] 'google_api' key not set. reverse_geocode module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_id' key not set. censys_email_to_domains module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_secret' key not set. censys_email_to_domains module will likely fail at runtime. See 'keys add'.  
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.  
[!] Module "recon/companies-domains/censys_subdomains" disabled. Dependency required: 'me' 'censysCertificates' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/_init_.py').  
[!] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.  
[!] 'shodan_api' key not set. shodan_ip module will likely fail at runtime. See 'keys add'.  
[!] 'virusTotal_api' key not set. virusTotal module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_id' key not set. censys_netblock module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_secret' key not set. censys_netblock module will likely fail at runtime. See 'keys add'.  
[!] 'shodan_api' key not set. shodan_net module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_id' key not set. censys_netblock_company module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_secret' key not set. censys_netblock_company module will likely fail at runtime. See 'keys add'.  
[!] 'shodan_anil' key not set. pushin module will likely fail at runtime. See 'keys add'.  
[recon-ng][default] > modules search  
Discovery  
discovery/info_disclosure/cache_snoop  
discovery/info_disclosure/interesting_files  
Exploitation  
exploitation/injection/command_injector  
exploitation/injection/xpath_bruter  
Import  
import/csv_file  
import/list  
root@kali:/home/omkar  
17 September 2023  
Sun 19:07 (Local Time)  
85°C Windy cloudy  
Search ENG IN ☰ 19:07 01/09/2023
```

```
Kali Linux [Running] - Oracle VM VirtualBox  
File Home File System Trash  
Session Actions Edit View Help  
reporting/proxifier  
reporting/pushpin  
reporting/xlsx  
reporting/xml  
[recon-ng][default] > workspaces  
Manages workspaces  
Usage: workspaces <create|list|load|remove> [...]  
[recon-ng][default] > workspaces create CEHV13  
[!] 'names_api' key not set. names_org module will likely fail at runtime. See 'keys add'.  
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_id' key not set. censys_org module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_id' key not set. censys_ore module will likely fail at runtime. See 'keys add'.  
[!] 'shodan_api' key not set. shodan_ore module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_id' key not set. censys_threats module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_secret' key not set. censys_threats module will likely fail at runtime. See 'keys add'.  
[!] 'http_api' key not set. http_parts module will likely fail at runtime. See 'keys add'.  
[!] 'http_api' key not set. http_breach module will likely fail at runtime. See 'keys add'.  
[!] 'whoxy_api' key not set. whoxy_whois module will likely fail at runtime. See 'keys add'.  
[!] 'whoxy_api' key not set. whoxy_whois module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_id' key not set. censys_companies module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_secret' key not set. censys_companies module will likely fail at runtime. See 'keys add'.  
[!] 'namechk_api' key not set. namechk module will likely fail at runtime. See 'keys add'.  
[!] 'twitter_api' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.  
[!] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.  
[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.  
[!] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.  
[!] 'shodan_api' key not set. shodan module will likely fail at runtime. See 'keys add'.  
[!] 'twitter_api' key not set. twitter module will likely fail at runtime. See 'keys add'.  
[!] 'twitter_secret' key not set. twitter module will likely fail at runtime. See 'keys add'.  
[!] 'google_api' key not set. youtube module will likely fail at runtime. See 'keys add'.  
[!] 'flickr_api' key not set. flickr module will likely fail at runtime. See 'keys add'.  
[!] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_id' key not set. censys_domain module will likely fail at runtime. See 'keys add'.  
[!] 'censysio_secret' key not set. censys_domain module will likely fail at runtime. See 'keys add'.  
[!] 'bing_api' key not set. bing_domain_api module will likely fail at runtime. See 'keys add'.  
[!] 'builtwith_api' key not set. builtwith module will likely fail at runtime. See 'keys add'.  
[!] 'shodan_api' key not set. shodan_hostname module will likely fail at runtime. See 'keys add'.  
[!] 'spysse_api' key not set. spysse_subdomains module will likely fail at runtime. See 'keys add'.  
[!] 'bing_api' key not set. bing_linkedin_contacts module will likely fail at runtime. See 'keys add'.  
[!] 'github_api' key not set. github_users module will likely fail at runtime. See 'keys add'.  
[!] Module "recon/domains-contacts/metacrawler" disabled. Dependency required: "PyPDF3".  
/root/recon-hg/modules/recon/domains-contacts/wikileaker.py:49: SyntaxWarning: Invalid escape sequence '\\"'.  
emails = re.findall("email:\\\\xa0([a-zA-Z0-9_.-]+@[a-zA-Z0-9_.-]+)"),
```

```
Session Actions Edit View Help
m = re.search('\.\{3\} (?<title>.+?) at ', snippet)
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_email_address module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_email_address module will likely fail at runtime. See 'keys add'.
/recon-ng/modules/recon/contacts-contacts/mangle.py:35: SyntaxWarning: invalid escape sequence '\s'
    sub_pattern = '[s]'

[!] 'github_api' key not set. github_dorks module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_commits module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_ip module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_ip module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_ip module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_hostname module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_hostname module will likely fail at runtime. See 'keys add'.
[!] 'virustotal_api' key not set. virustotal module will likely fail at runtime. See 'keys add'.
[!] 'ipstack_api' key not set. ipstack module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_query module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_query module will likely fail at runtime. See 'keys add'.
[!] 'ipinfo_api' key not set. ipinfo module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. reverse_geocode module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_email_to_domains module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_email_to_domains module will likely fail at runtime. See 'keys add'.
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
Module 'recon/companies-domains/censys_subdomains' disabled. Dependency required: 'me' 'CensysCertificates' from 'censys.search' (/usr/lib/python/search/_init_.py)

[!] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_ip module will likely fail at runtime. See 'keys add'.
[!] 'virustotal_api' key not set. virustotal module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_netblock module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_net module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_netblock_company module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_netblock_company module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.

[recon-ng][CEHv13] >
```

Workspaces	Modified
CEHv13	2025-09-07 18:59:05
default	2025-09-07 15:53:52

```
Session Actions Edit View Help
[recon-ng][CEHv13] > workspaces list
+-----+-----+
| Workspaces | Modified |
+-----+-----+
| CEHv13 | 2025-09-07 18:59:05 |
| default | 2025-09-07 15:53:52 |
+-----+-----+
[recon-ng][CEHv13] >
```

- Now you can change your workspace from created to default and default to created by command- workspaces load default or workspaces load CEHv13.

```
[recon-ng][CEHv13] > recon-ng
[!] Invalid workspace name.
[recon-ng][CEHv13] > workspaces load Def
[*] Invalid workspace name.
[recon-ng][CEHv13] > workspaces load def
[*] Invalid workspace name.
[recon-ng][CEHv13] > workspaces load default
[*] hashes.org key not set. hashes.org module will likely fail at runtime. See 'keys add'.
[*] github.org key not set. github.miner module will likely fail at runtime. See 'keys add'.
[*] 'censysio_id' key not set. censys_org module will likely fail at runtime. See 'keys add'.
[*] 'censysio_secret' key not set. censys_org module will likely fail at runtime. See 'keys add'.
[*] 'shodan_api' key not set. shodan.org module will likely fail at runtime. See 'keys add'.
[*] 'censysio_id' key not set. censys_tls_subjects module will likely fail at runtime. See 'keys add'.
[*] 'censysio_secret' key not set. censys_tls_subjects module will likely fail at runtime. See 'keys add'.
[*] 'http_api' key not set. http_paste module will likely fail at runtime. See 'keys add'.
[*] 'http_api' key not set. http_breach module will likely fail at runtime. See 'keys add'.
[*] 'whoxy_api' key not set. whoxy_whois module will likely fail at runtime. See 'keys add'.
[*] 'censysio_id' key not set. censys_companies module will likely fail at runtime. See 'keys add'.
[*] 'censysio_secret' key not set. censys_companies module will likely fail at runtime. See 'keys add'.
[*] 'namechk_api' key not set. namechk module will likely fail at runtime. See 'keys add'.
[*] 'twitter_api' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[*] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[*] 'twitter_id' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[*] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[*] 'shodan_api' key not set. shodan module will likely fail at runtime. See 'keys add'.
[*] 'twitter_api' key not set. twitter module will likely fail at runtime. See 'keys add'.
[*] 'twitter_secret' key not set. twitter module will likely fail at runtime. See 'keys add'.
[*] 'google_api' key not set. youtube module will likely fail at runtime. See 'keys add'.
[*] 'flickr_api' key not set. flickr module will likely fail at runtime. See 'keys add'.
[*] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.
[*] 'censysio_id' key not set. censys_domain module will likely fail at runtime. See 'keys add'.
[*] 'censysio_secret' key not set. censys_domain module will likely fail at runtime. See 'keys add'.
[*] 'bing_api' key not set. bing_domain_api module will likely fail at runtime. See 'keys add'.
[*] 'builtwith_api' key not set. builtwith module will likely fail at runtime. See 'keys add'.
[*] 'shodan_api' key not set. shodan_hostname module will likely fail at runtime. See 'keys add'.
[*] 'spysy_api' key not set. spsy_subdomains module will likely fail at runtime. See 'keys add'.
[*] 'bing_api' key not set. bing_linkedin_contacts module will likely fail at runtime. See 'keys add'.
[*] 'github_api' key not set. github_users module will likely fail at runtime. See 'keys add'.
[*] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: 'PyPDF3'.
/recon/.recon/ng/modules/recon/domains-contacts/wikileaker.py:49: SyntaxWarning: invalid escape sequence '\.'
```

07 September 2025  
Sun 19:18 (Local time)  
ENG IN 19:18 07-09-2025

- Now performing Reconnaissance, command- db insert domains
- Now type text (domain)- certifiedhacker.com
- New command- show domain
- So we can see certifiedhacker.com domain is created.

```

Session Actions Edit View Help
[!] 'github_api' key not set, github_dorks module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set, github_commits module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' Key not set, censys_ip module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set, censys_ip module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set, bing_ip module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set, censys_hostname module will likely fail at runtime. See 'keys add'.
[!] 'virusotal_api' key not set, virusotal module will likely fail at runtime. See 'keys add'.
[!] 'ipstack_anl' Key not set, ipstack module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' Key not set, censys_query module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set, censys_query module will likely fail at runtime. See 'keys add'.
[!] 'ipinfodn_api' key not set, ipinfodn module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set, fullcontact module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' Key not set, censysio module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set, censysio module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set, reverse_geocode module will likely fail at runtime. See 'keys add'.
[!] 'ipstack_api' key not set, geocode module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' Key not set, censys_email_to_domains module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set, censys_email_to_domains module will likely fail at runtime. See 'keys add'.
[!] 'whoxy_api' key not set, whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-domains/censys_subdomains' disabled. Dependency required: 'me 'CensysCertificates' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/_init_.py').
[!] 'binaryedge_api' key not set, binaryedge module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set, shodan_ip module will likely fail at runtime. See 'keys add'.
[!] 'virusotal_api' key not set, virusotal module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' Key not set, censys_netblock module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set, censys_netblock module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' Key not set, shodan_net module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' Key not set, censys_netblock_company module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set, censys_netblock_company module will likely fail at runtime. See 'keys add'.
[*] 1 rows returned
[recon-ng][CEHv13] > show domains

```

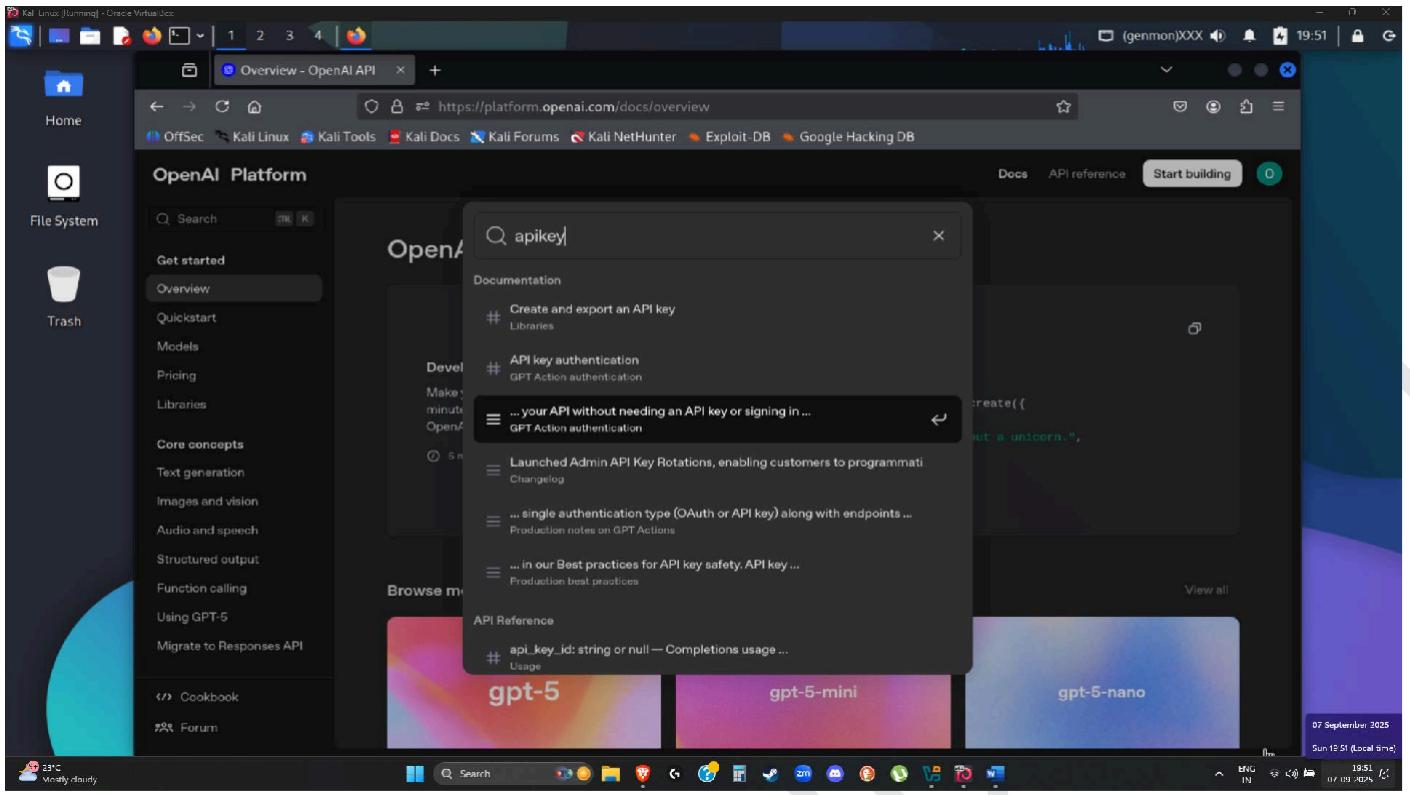
rowid	domain	notes	module
1	certifiedhacker.com	show domain	user_defined

[\*] 1 rows returned  
[recon-ng][CEHv13] >

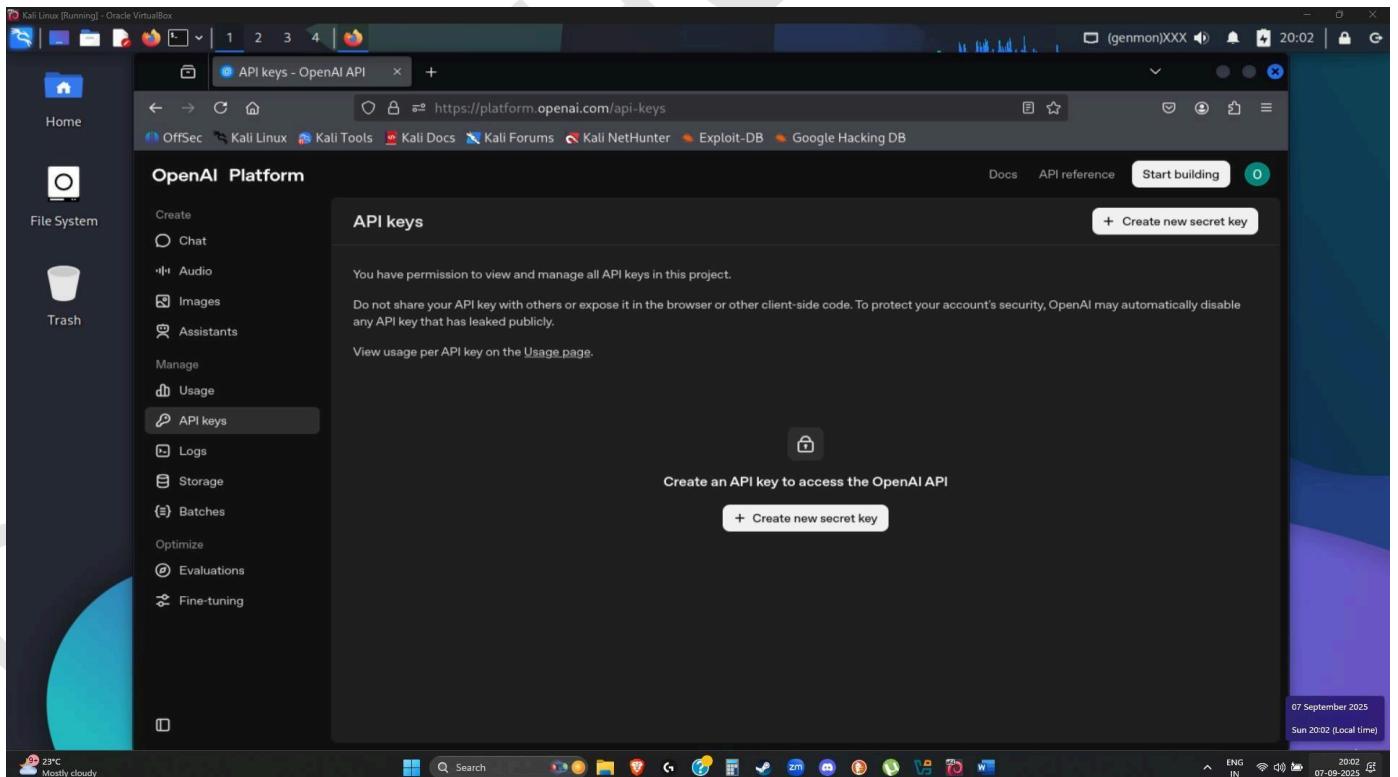
- So we can see, there are so many modules we can use to gather information.

## Performing Foot-Printing using AI:

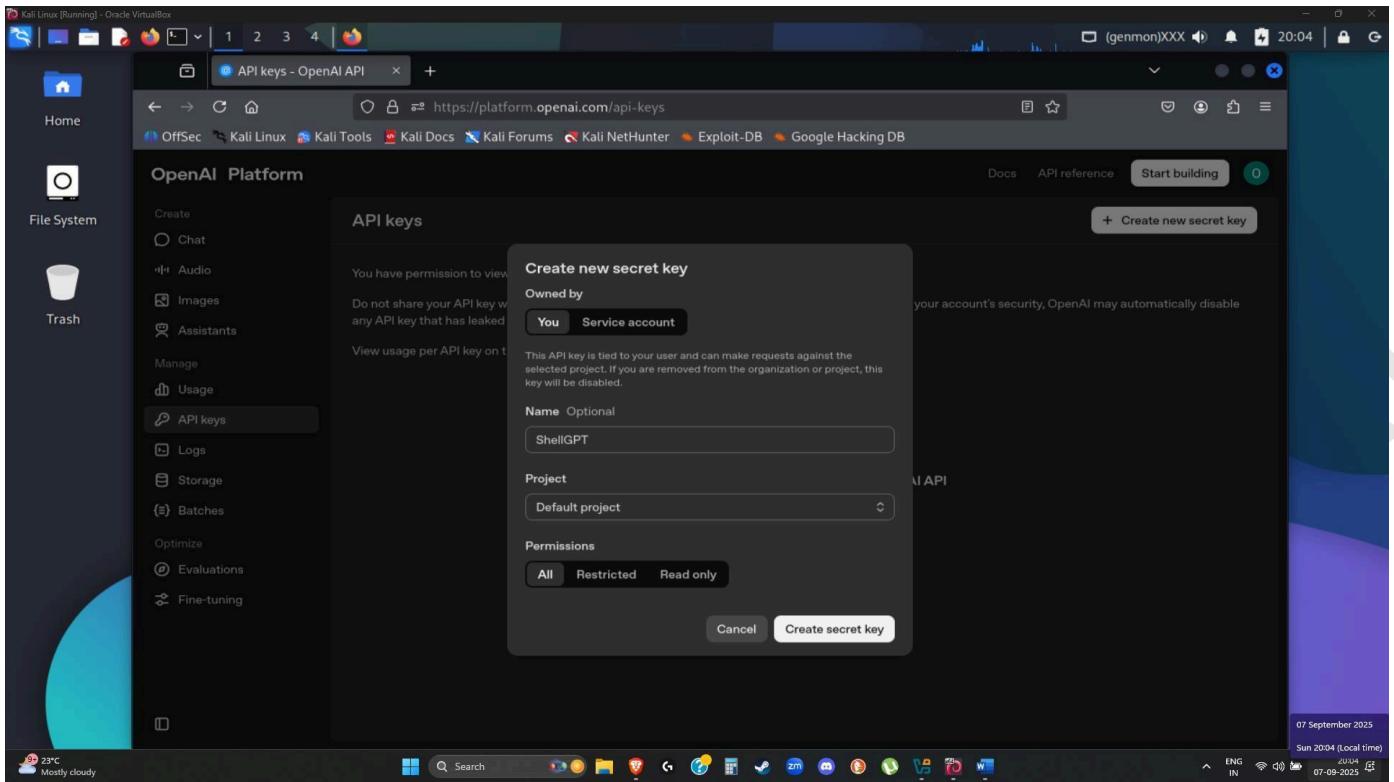
- First open Google in Kali Linux
- Search Platform openai
- Login in **openai** and perform
- Search **apikey**



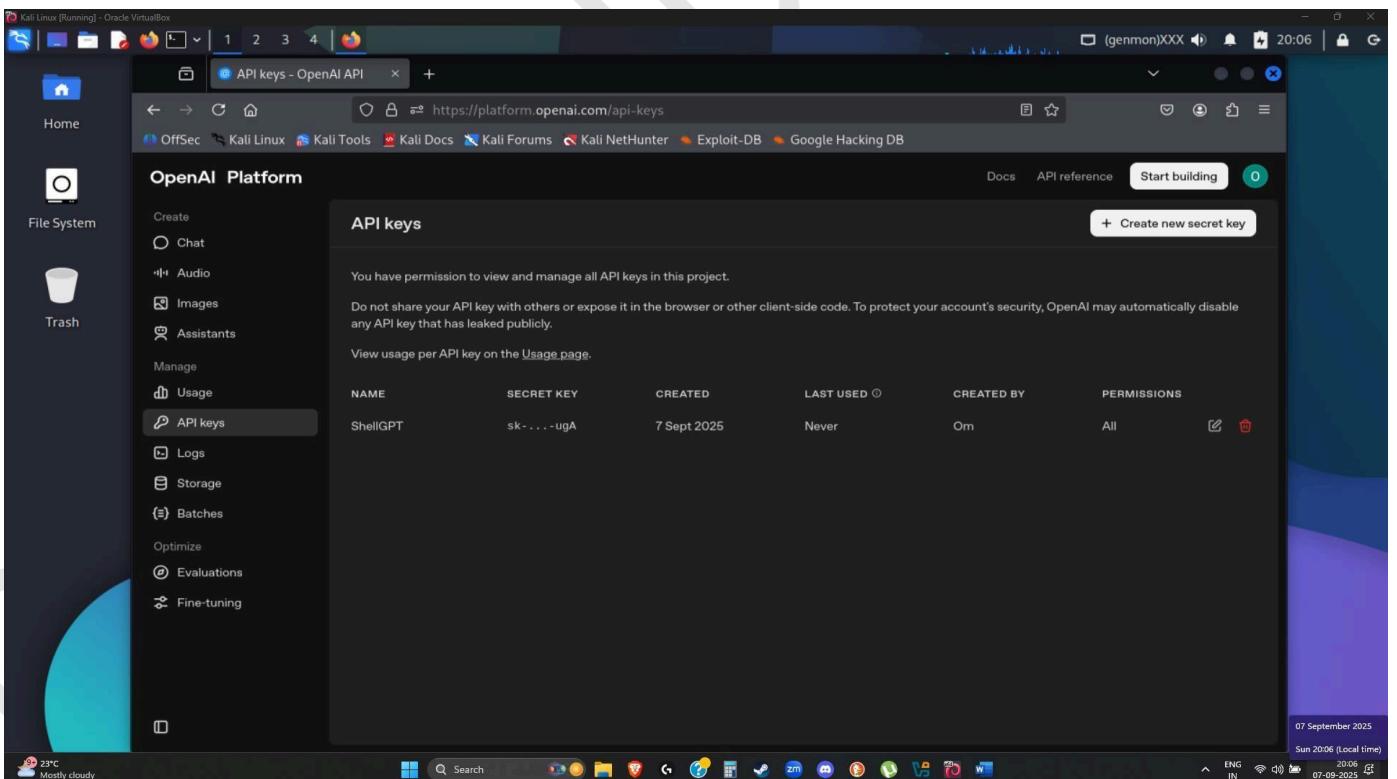
## ● First create API secret Key.



## ● Created API secret Key.

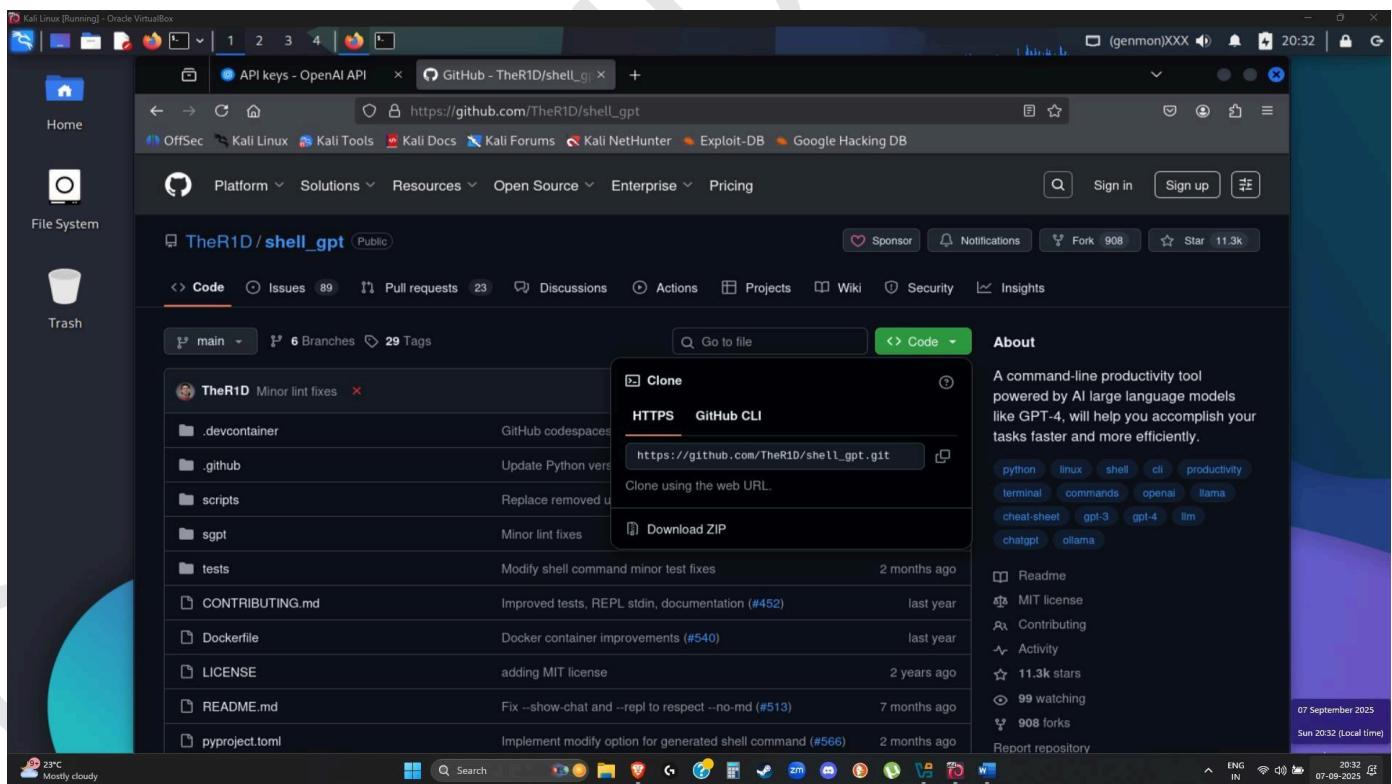


- Generated and Saved API key



- In Kali Linux run Terminal

- Run command **sgpt**
- It will show not installed
- Install using **Github**
- Open Google.com
- Type Shell- gpt github
- Open code and copy
- Paste in Terminal by command- **git clone (paste)**
- Now Run command **Shell\_gpt**



```
root@kali: /home/omkar/shell_gpt
Session Actions Edit View Help
(omkar@kali)-[~]
$ sudo su
[sudo] password for omkar:
[root@kali]-[/home/omkar]
# shell-gpt
shell-gpt: command not found
[root@kali]-[/home/omkar]
# apt install shell-gpt
Error: Unable to locate package shell-gpt
[root@kali]-[/home/omkar]
# sgpt
Command 'sgpt' not found, did you mean:
  command 'gpt' from deb gpt
  command 'cgpt' from deb cgpt
Try: apt install <deb name>
[root@kali]-[/home/omkar]
# git clone https://github.com/TheR1D/shell_gpt.git
Cloning into 'shell_gpt'...
remote: Enumerating objects: 868, done.
remote: Counting objects: 100% (34/34), done.
remote: Compressing objects: 100% (28/28), done.
remote: Total 868 (delta 23), reused 6 (delta 6), pack-reused 834 (from 3)
Receiving objects: 100% (868/868), 262.20 KiB | 446.00 KiB/s, done.
Resolving deltas: 100% (527/527), done.
[root@kali]-[/home/omkar]
# shell_gpt
[root@kali]-[/home/omkar/shell_gpt]
#
```

- Now check sgpt is there, command ls Enter
- We can see it says sgpt
- Next Run command ls sgpt

```
root@kali: /home/omkar/shell_gpt
Session Actions Edit View Help
(omkar@kali)-[~]
$ sudo su
[sudo] password for omkar:
[root@kali]-[/home/omkar]
# shell-gpt
shell-gpt: command not found
[root@kali]-[/home/omkar]
# apt install shell-gpt
Error: Unable to locate package shell-gpt
[root@kali]-[/home/omkar]
# sgpt
Command 'sgpt' not found, did you mean:
  command 'gpt' from deb gpt
  command 'cgpt' from deb cgpt
Try: apt install <deb name>
[root@kali]-[/home/omkar]
# git clone https://github.com/TheR1D/shell_gpt.git
Cloning into 'shell_gpt'...
remote: Enumerating objects: 868, done.
remote: Counting objects: 100% (34/34), done.
remote: Compressing objects: 100% (28/28), done.
remote: Total 868 (delta 23), reused 6 (delta 6), pack-reused 834 (from 3)
Receiving objects: 100% (868/868), 262.20 KiB | 446.00 KiB/s, done.
Resolving deltas: 100% (527/527), done.
[root@kali]-[/home/omkar]
# shell_gpt
[root@kali]-[/home/omkar/shell_gpt]
# ls
CONTRIBUTING.md Dockerfile LICENSE pyproject.toml README.md scripts sgpt tests
[root@kali]-[/home/omkar/shell_gpt]
# ls sgpt
app.py config.py handlers integration.py __main__.py role.py __version__.py
cache.py function.py __init__.py __l1m_functions printer.py utils.py
[root@kali]-[/home/omkar/shell_gpt]
#
```

- Now we use command in shell-gpt.

bash sgpt.sh "scan 192.168.1.10 for open ports and services"

- For open ports and services.

nmap -sV 192.168.1.10

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal session is root@kali:/home/omkar. The user has run the command 'bash sgpt.sh "scan 192.168.1.10 for open ports and services"'. The output shows that the file 'sgpt.sh' does not exist. Then, the user runs 'nmap -sV 192.168.1.10', which starts Nmap 7.95 and scans the host at 2025-09-07 20:50 IST. A note indicates the host seems down. The scan completes in 3.23 seconds with 1 IP address scanned. The desktop interface includes a file manager sidebar with Home, File System, and Trash options, and a system tray at the bottom showing weather (23°C, mostly cloudy), date (07 September 2025), and time (20:53).

## Conclusion:

*In this lab, I used tools like WHOIS, nslookup, theHarvester, and Google dorks (via ShellGPT) to gather domain, IP, subdomain, and email information. The results show how attackers can map a target before exploitation. To defend, organizations should use WHOIS privacy, secure DNS, limit public exposure of sensitive data, and monitor for information leaks.*