MODULE 2

Foot Printing & Reconnaissance

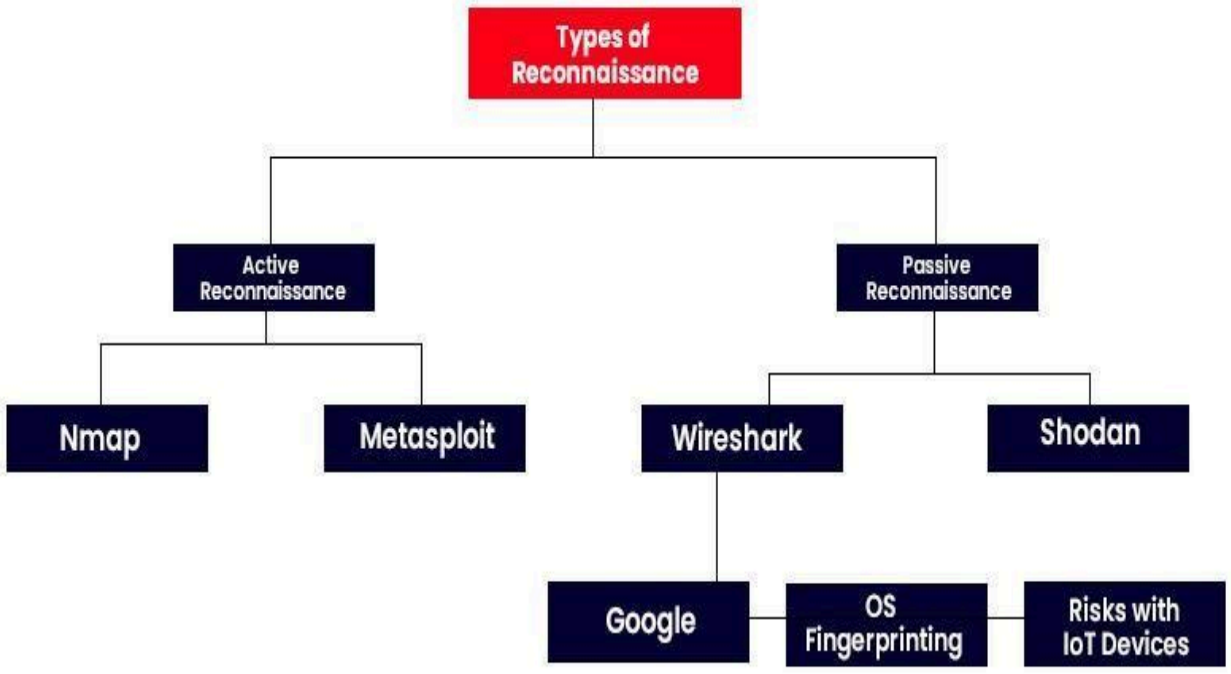
Name: Omkar Hundekari

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.

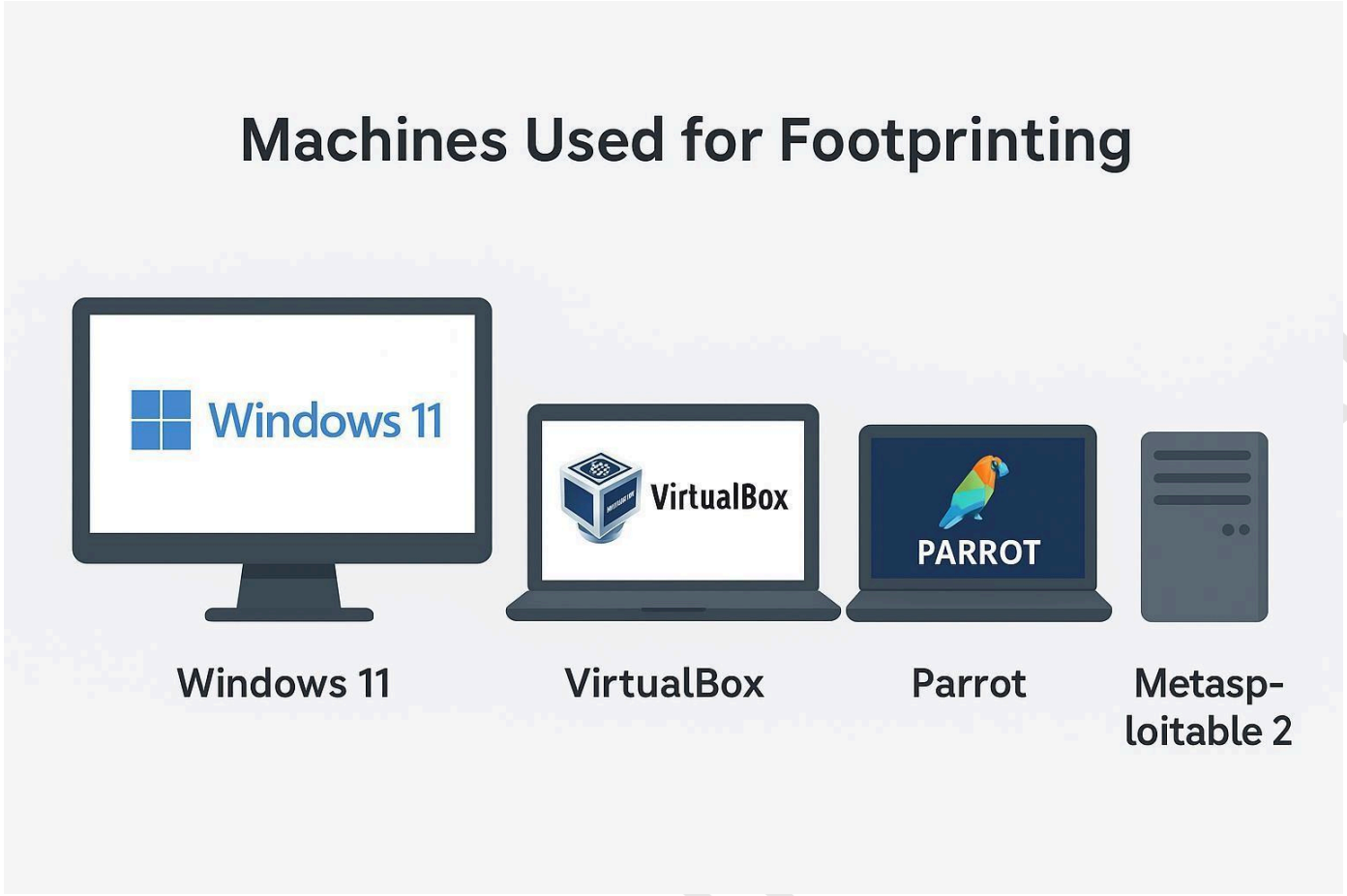
- Why is this Information important ?

- **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:



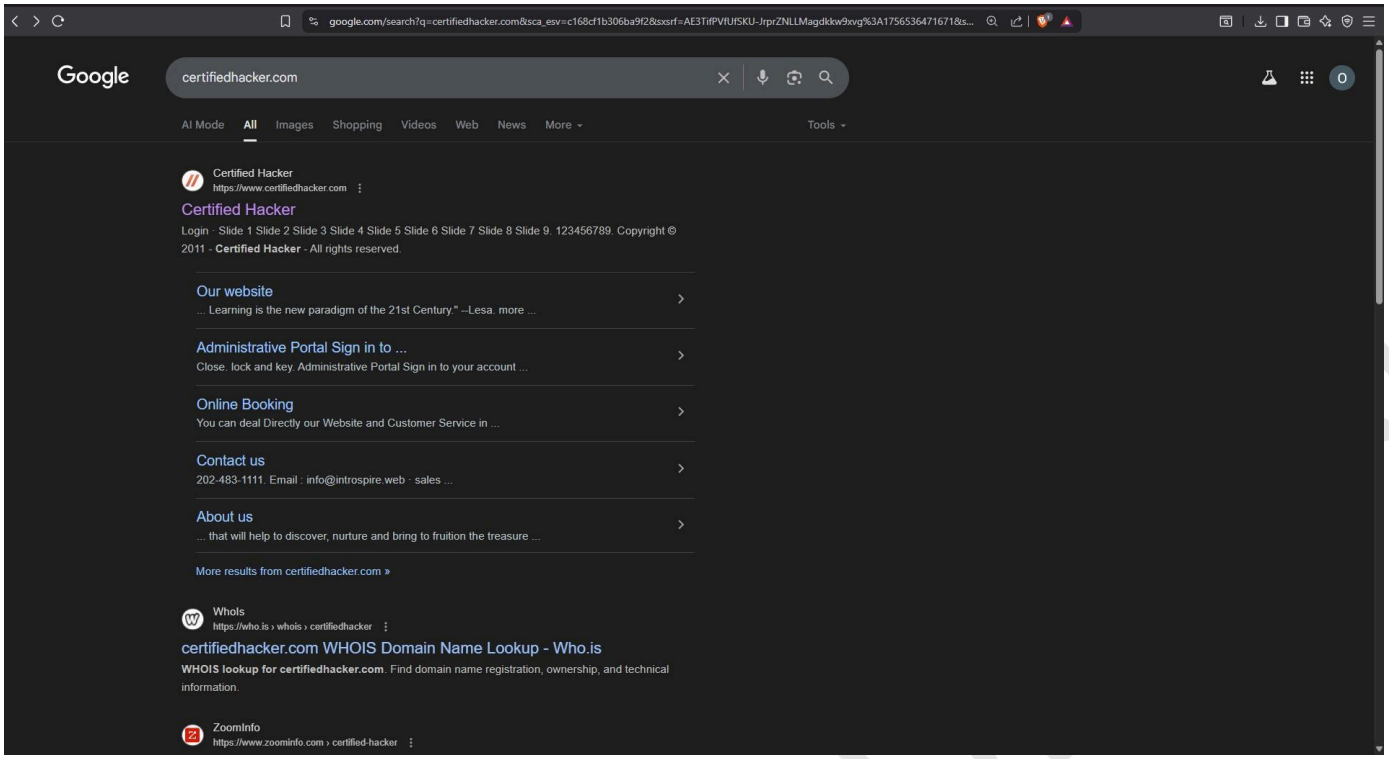
Search Engines in Foot-Printing:

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.

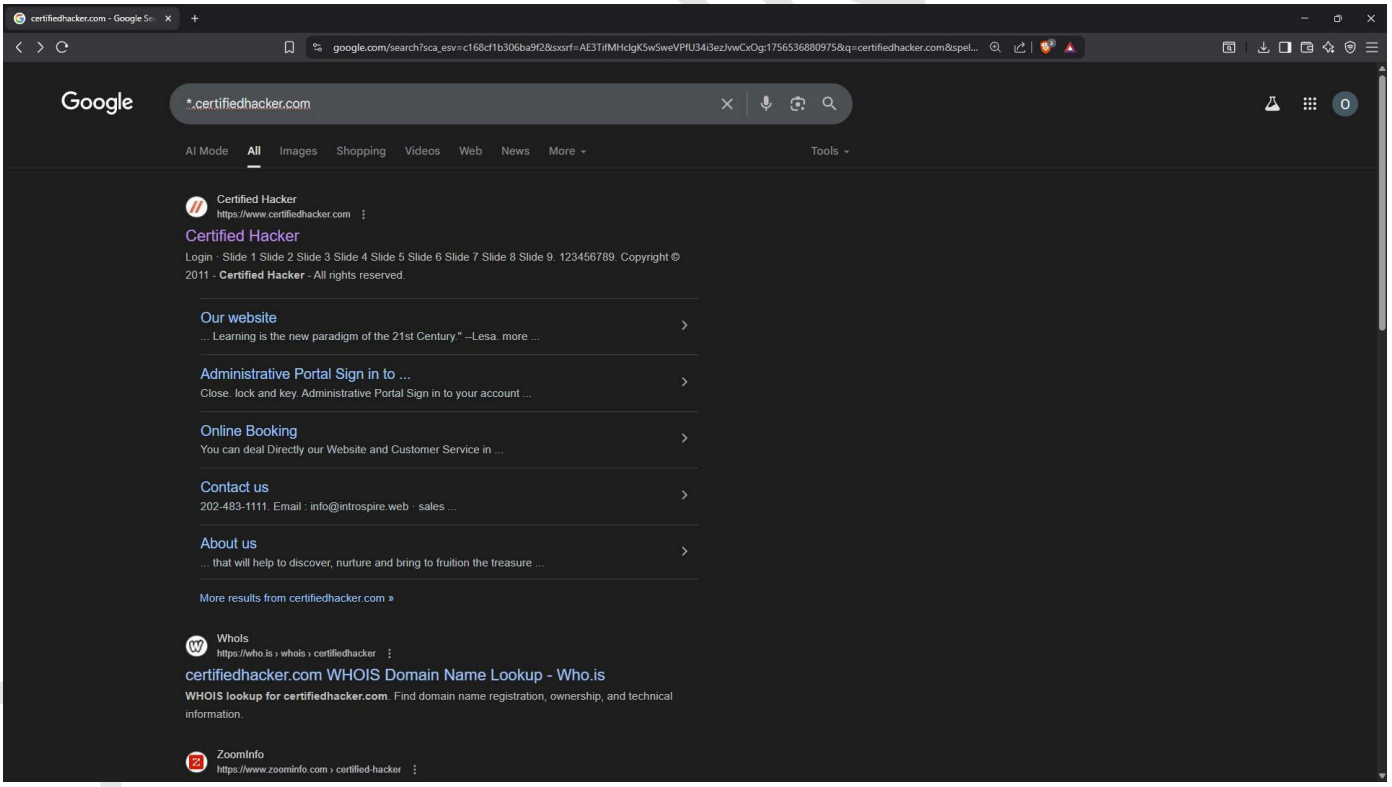
- Advanced Google Hacking Techniques:

- **Specific Domain:**
  a) Site:Certifiedhacker.com
  b) Site:*.certifiedhacker.com

a)



b)



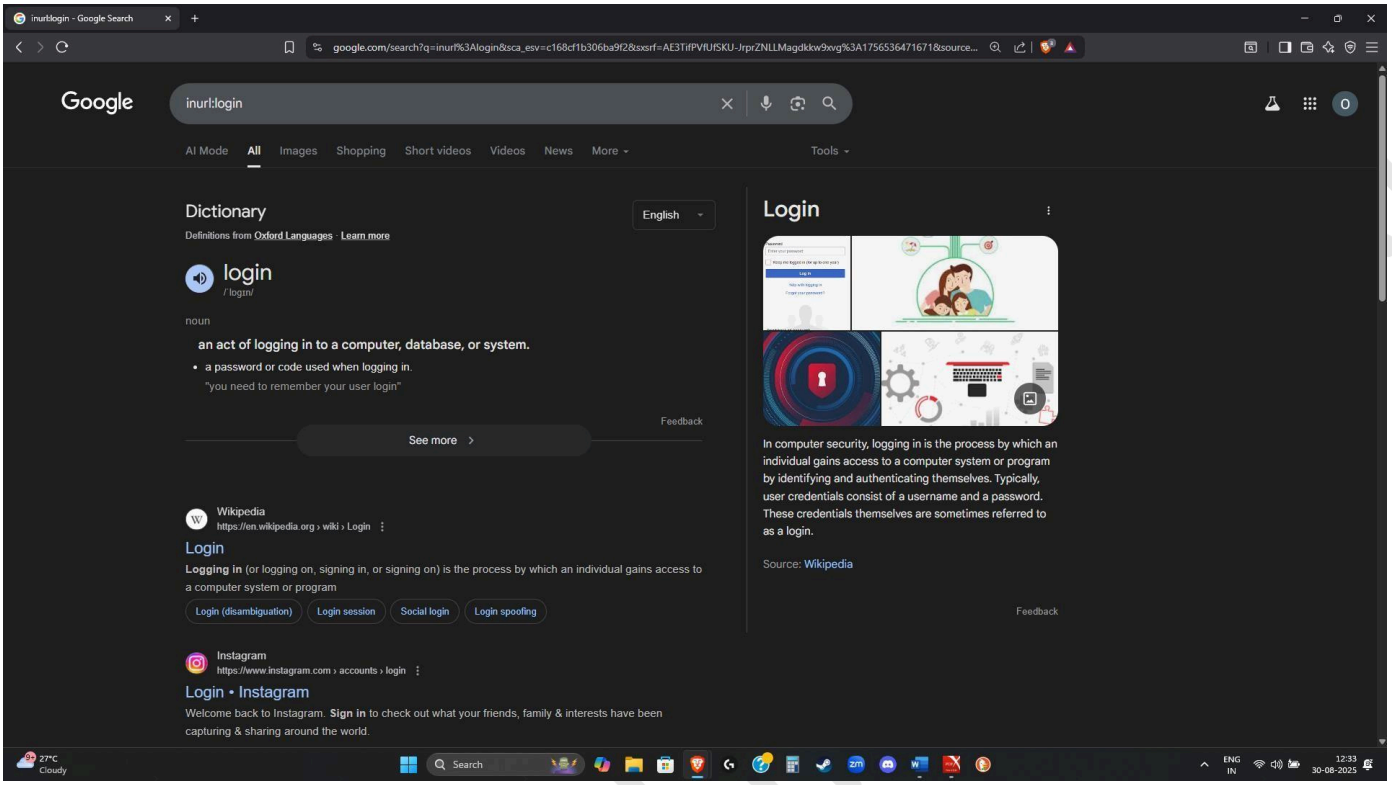
- **Find Keywords inside a URL:**

a) inurl:login

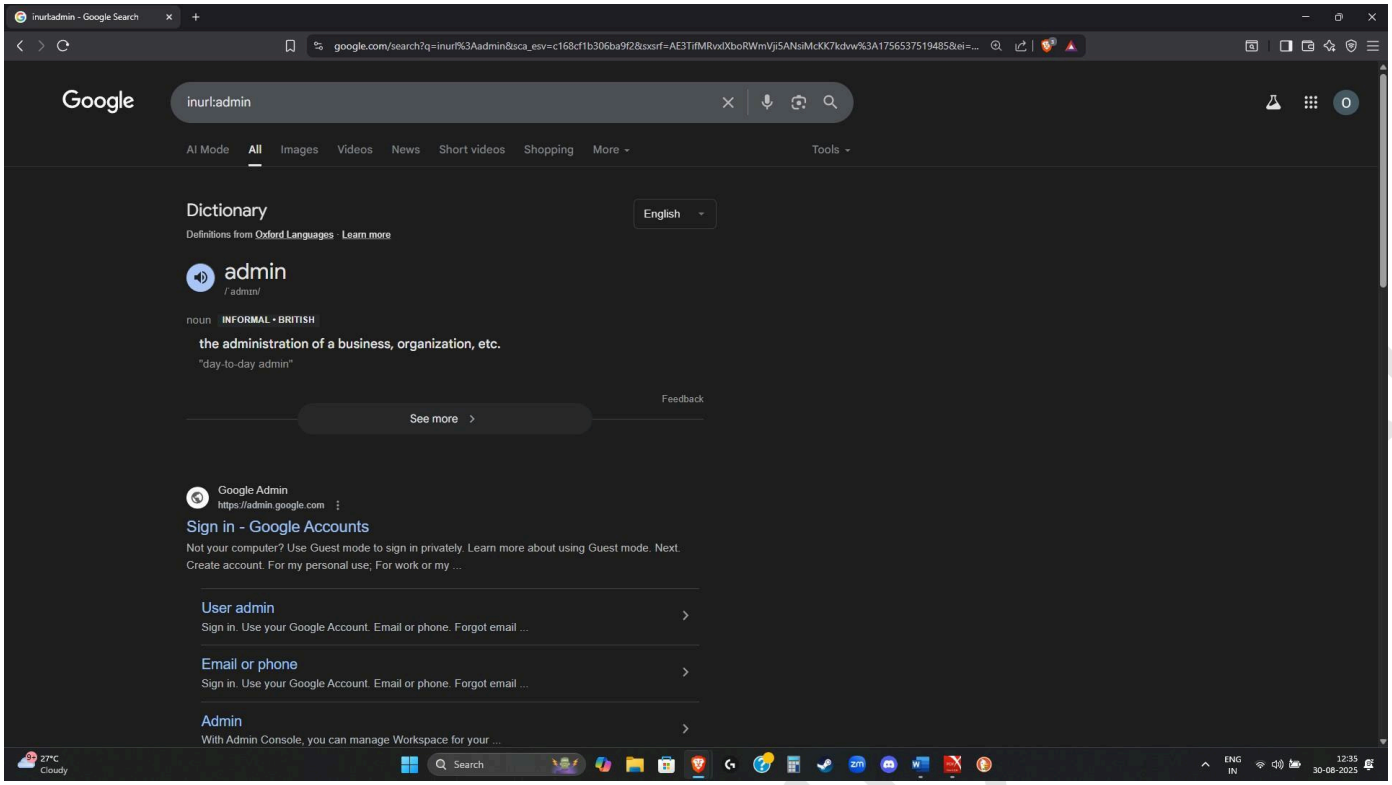
b) inurl:admin

c) inurl:dashboard

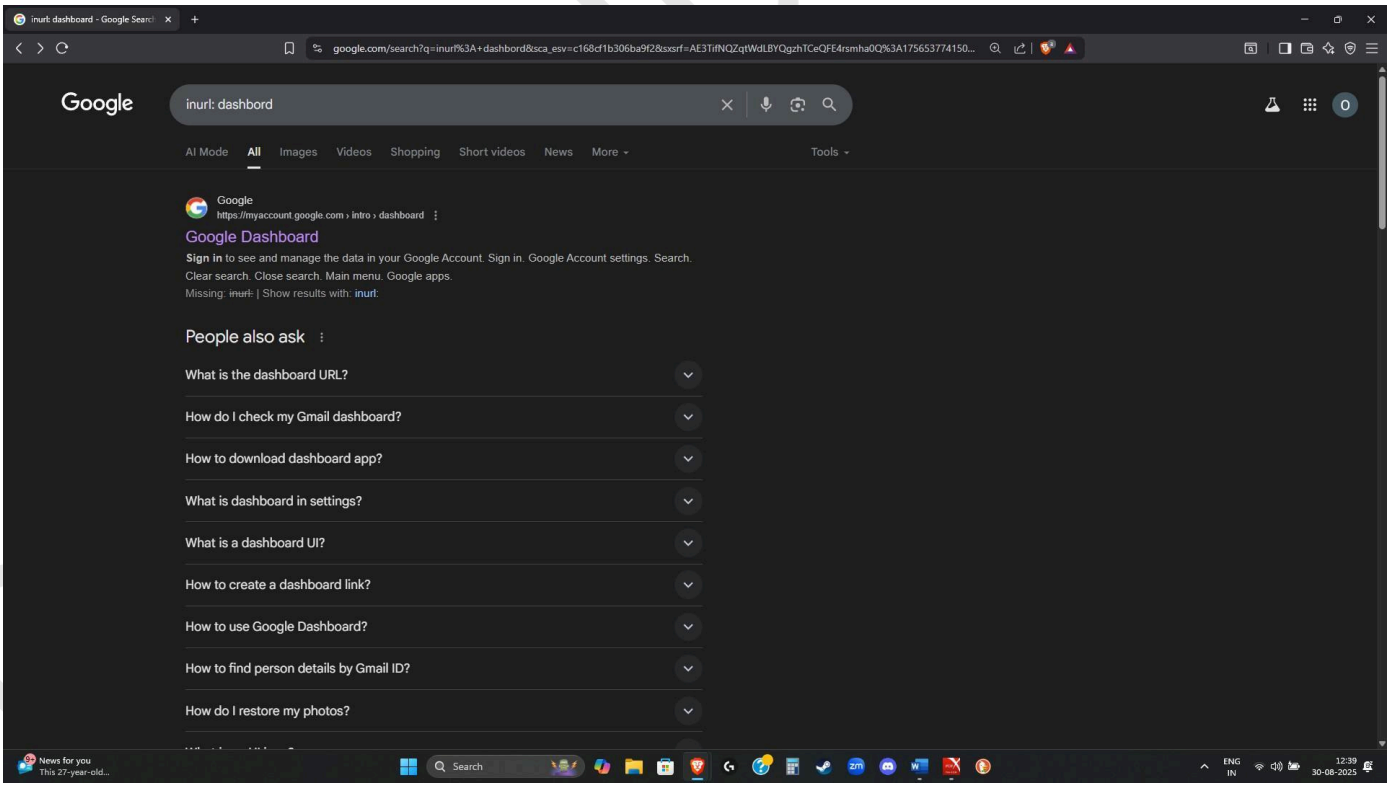
a)



b) Image next page



c)

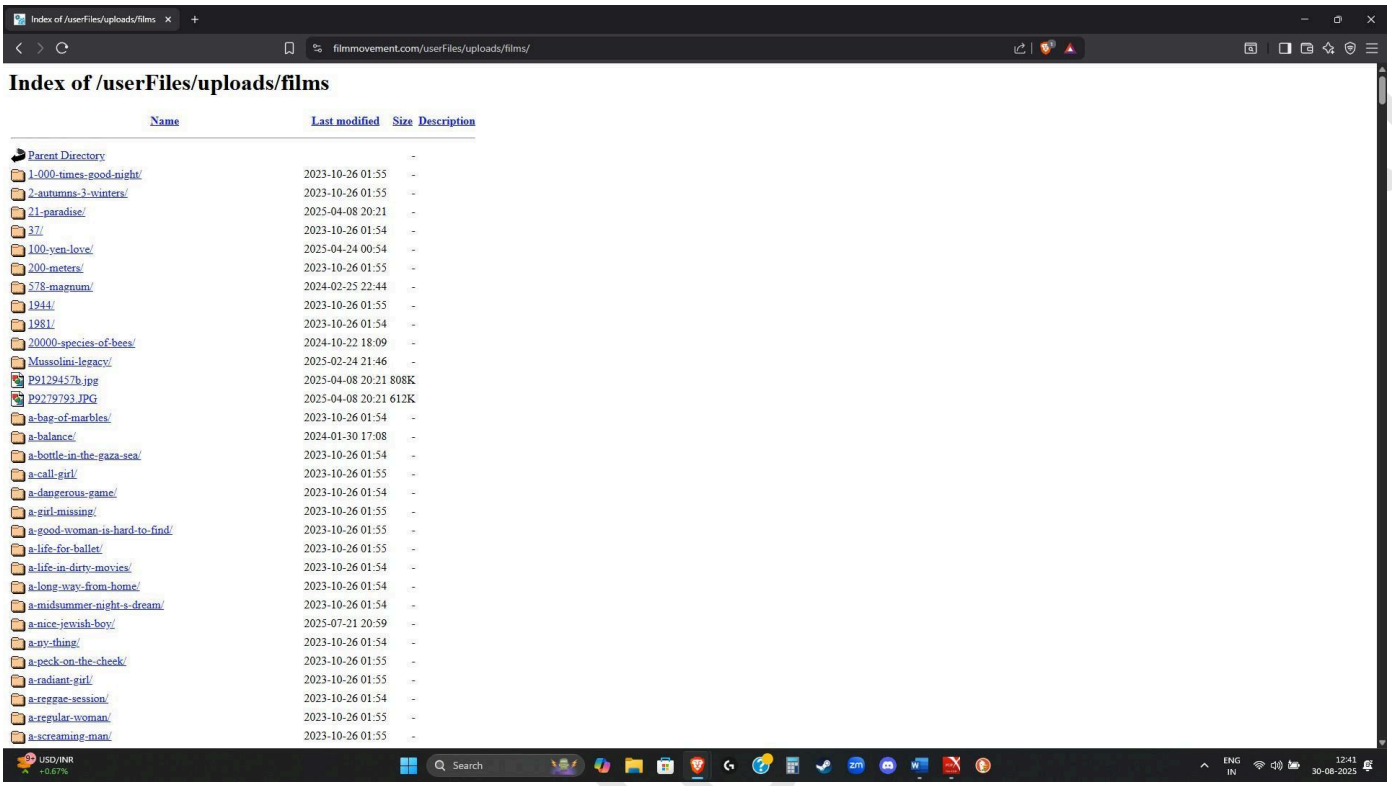


- **Search for Keywords in page titles:**

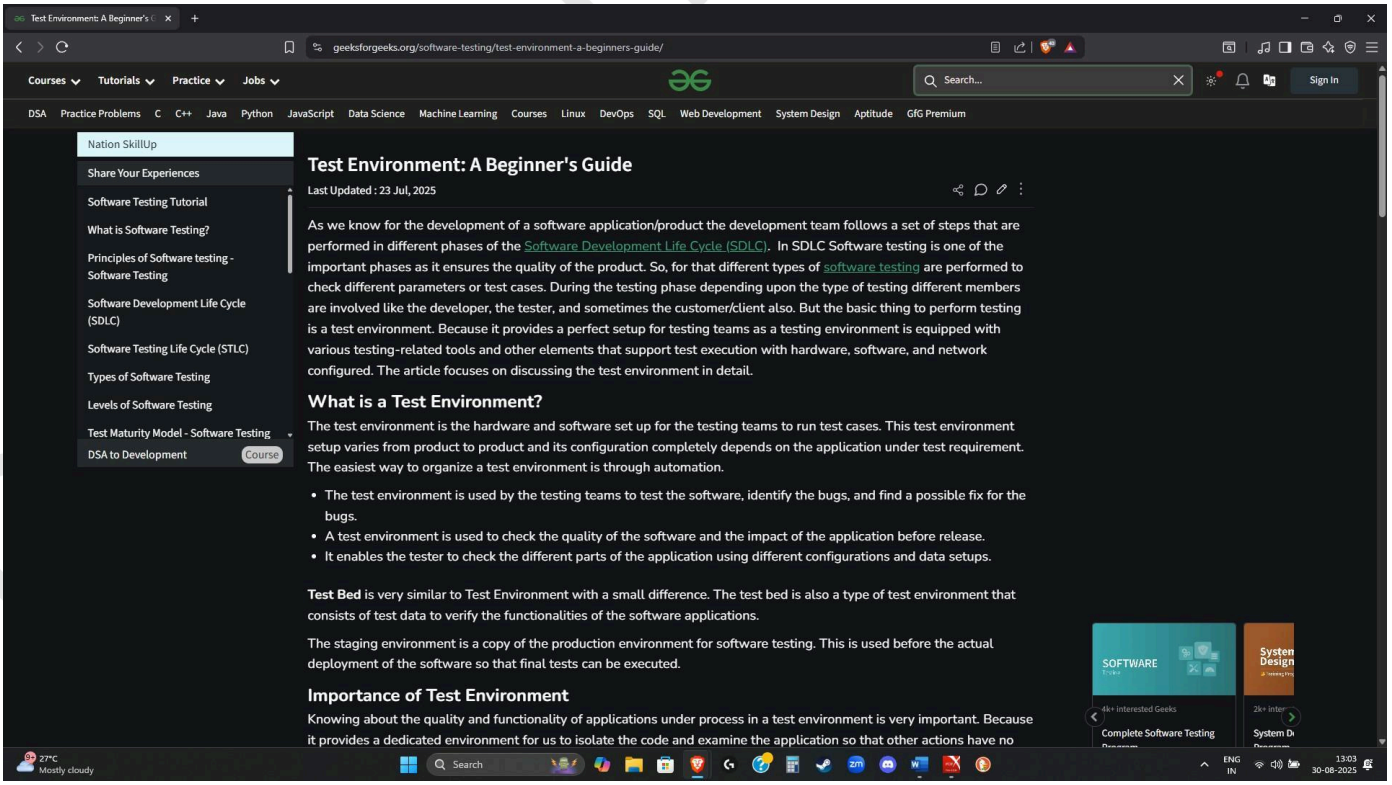
a) Intitle:“index of”

b) Intitle: “test environment”

a)



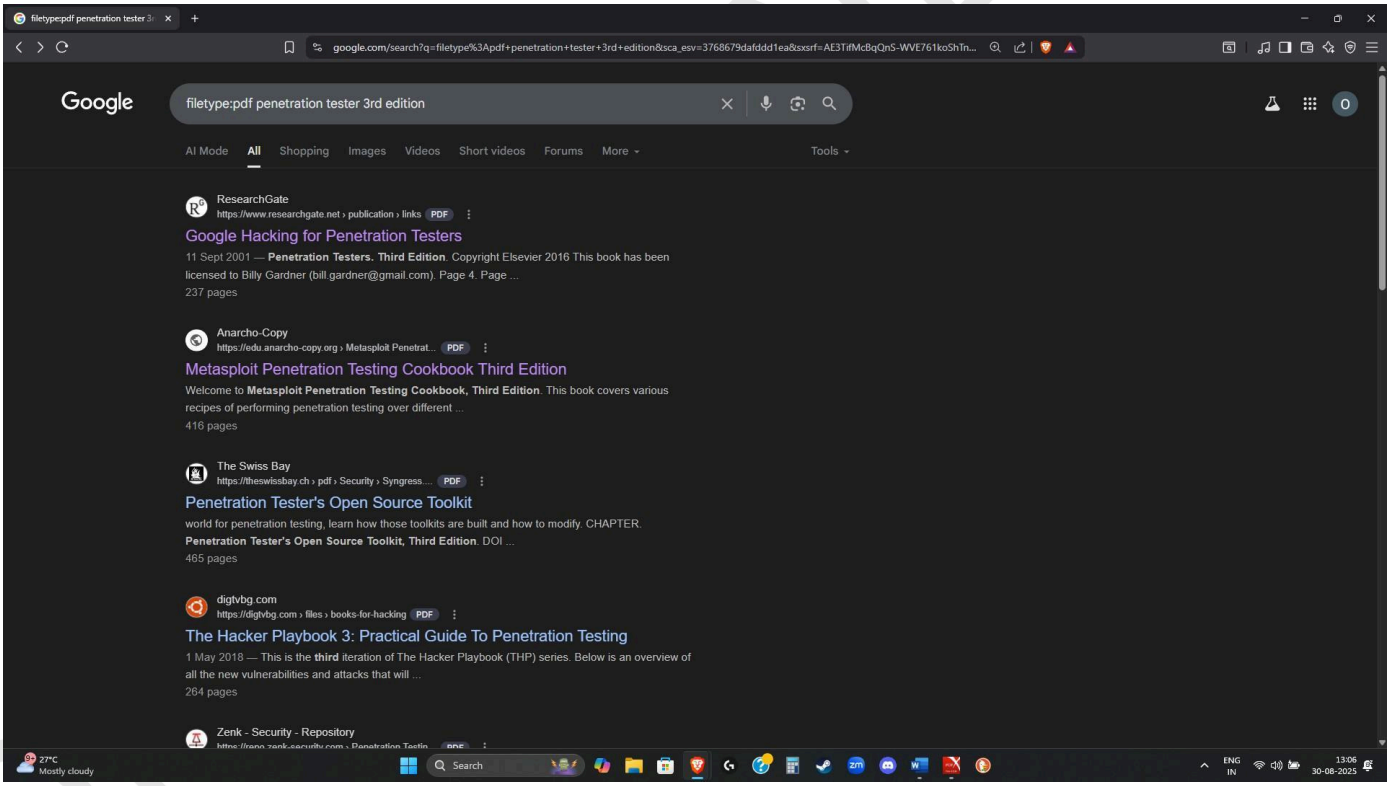
b)image on next page



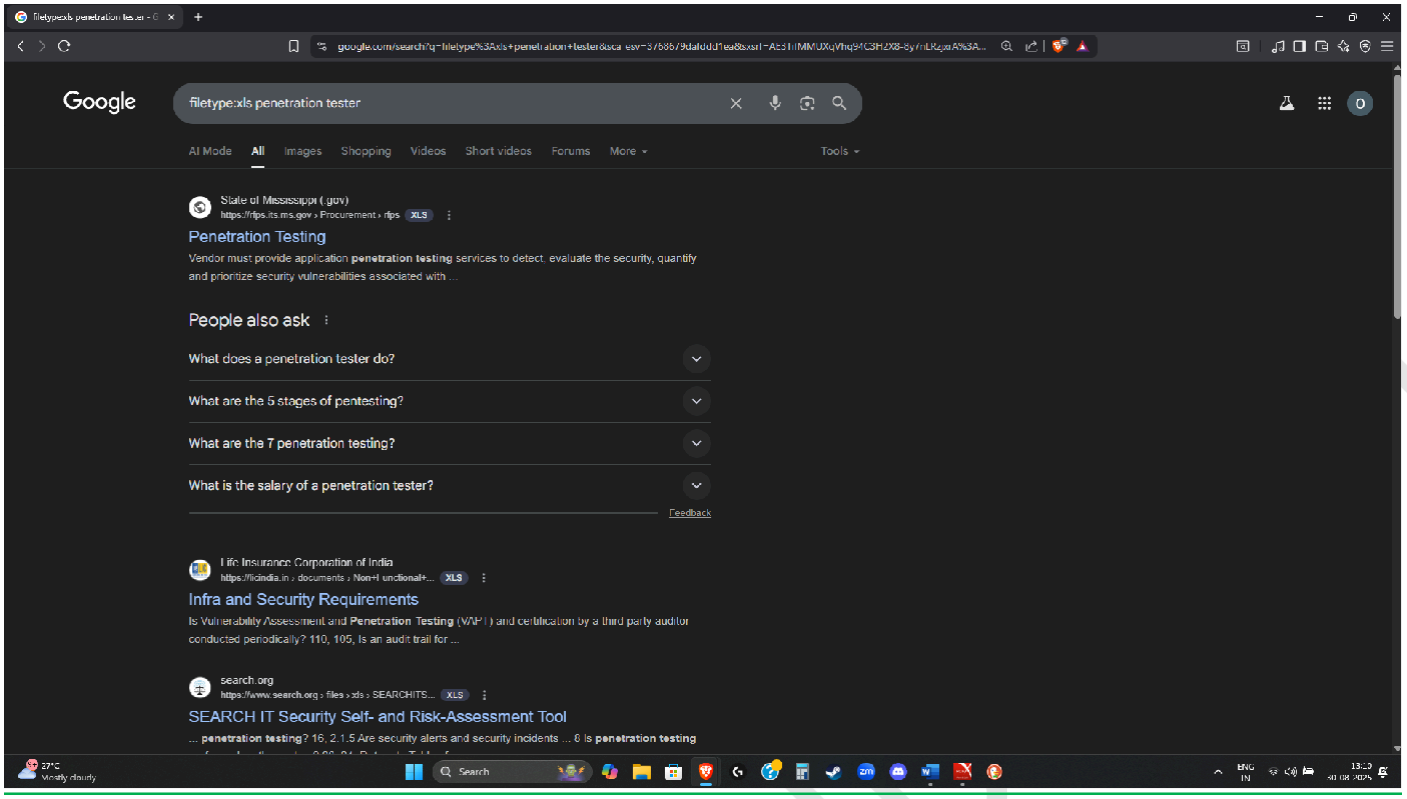
- **Find the files with specific extension:**

    a) **filetype:pdf penetration tester 3rd edition**
    b) filetype:xls

    a) Image on next page



b)

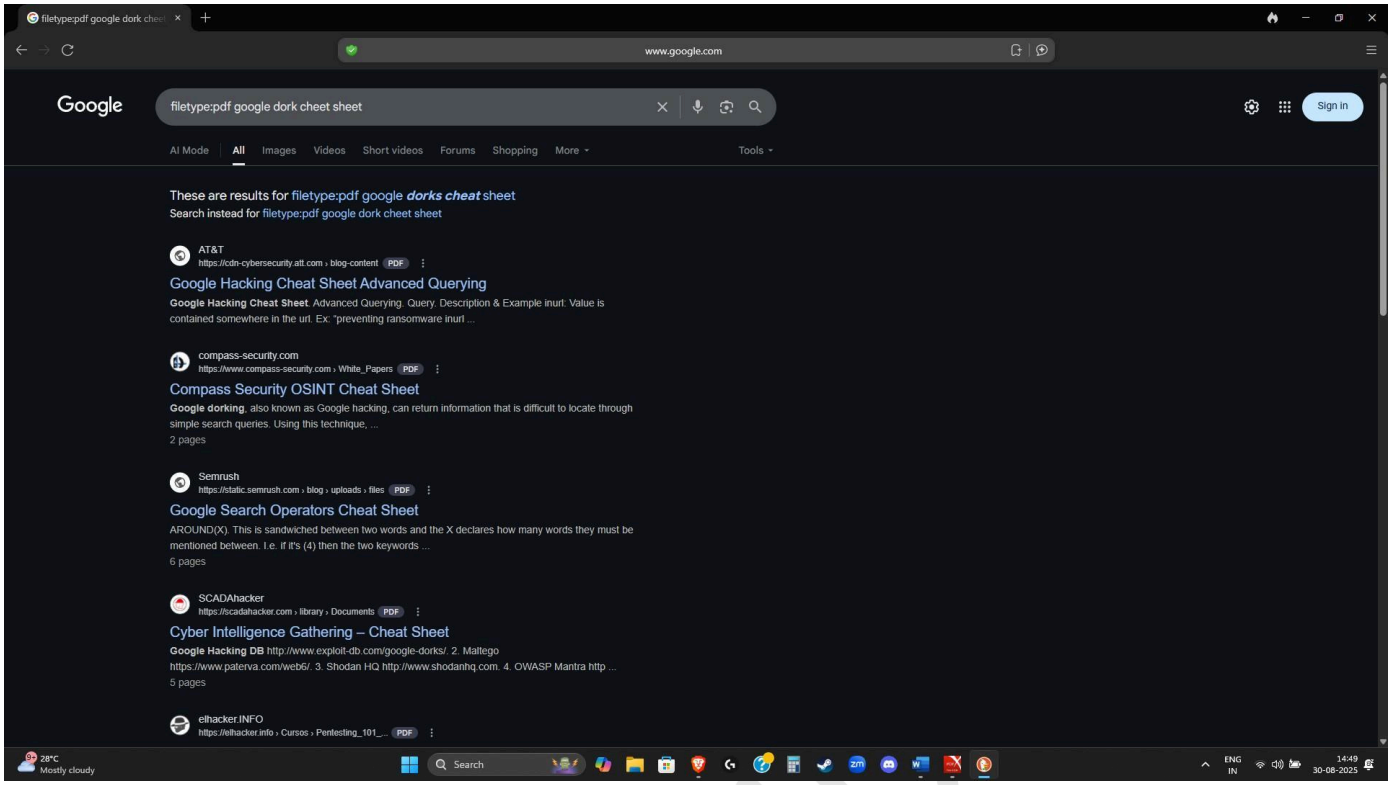


- Google Hacking Database:

- **Examples of Google Dorks from GHDB**

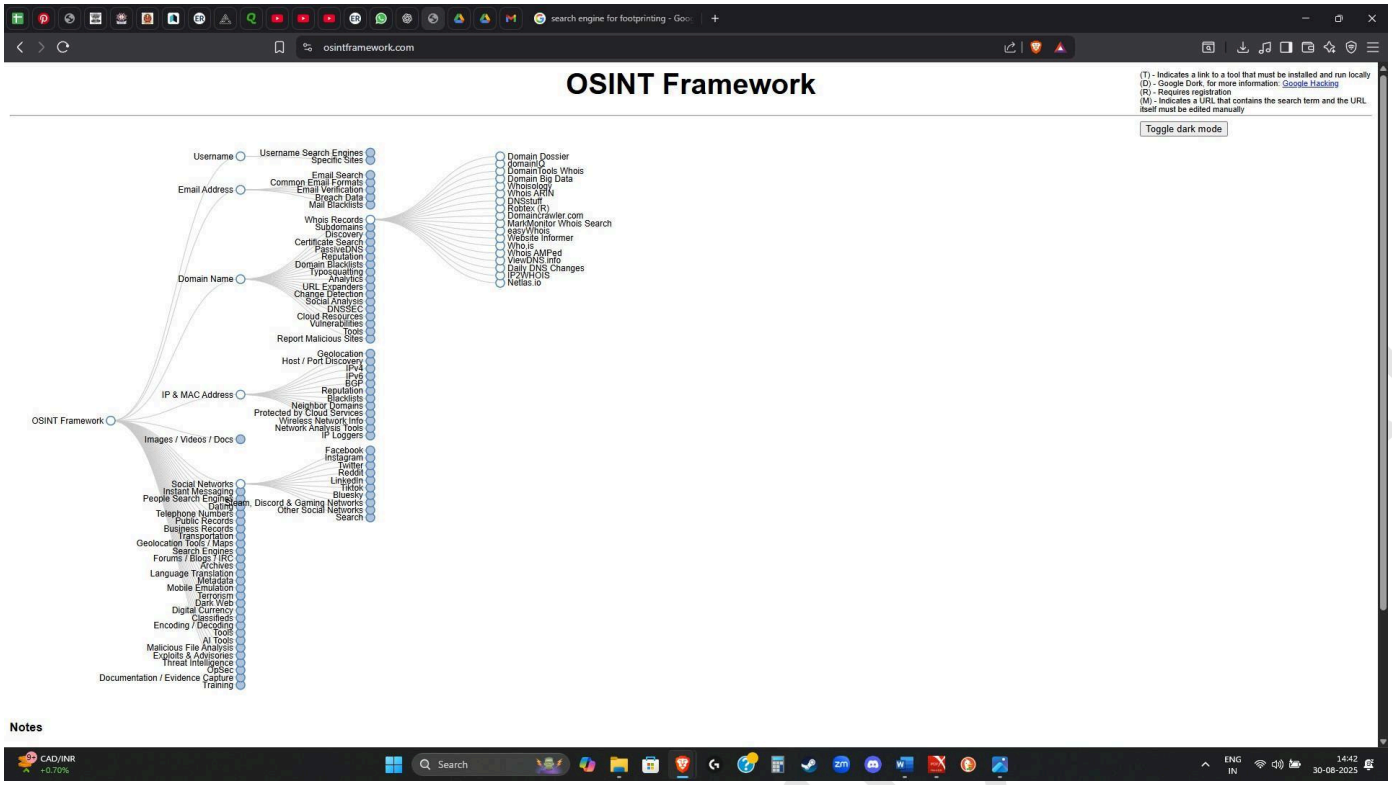
Here are some typical classes of GHDB queries:

- **Login Admin Portals**
  inurl:admin login
  inurl:login.php Cybrvault+1
- **Exposed Database Dumps or Credentials**
  filetype:sql intext:"INSERT INTO"
  intext:"password" filetype:txt Cybrvault+1
- **Directory Listings and Open Folders**
  intitle:"index of" "parent directory" Cybrvault+1Onion Linux
- **Sensitive Documents & PDFs**
  filetype:pdf intext:"confidential"
  filetype:docx intext:"restricted" Cybrvault+1Intellipaat
- **Security Cameras & Devices**
  inurl:"view/view.shtml"
  inurl:/view.shtml intext:admin CybrvaultIntellipaatOnion Linux
- **Server Configs / Error Messages**
  filetype:log
  intext:"DB_PASSWORD" filetype:env (common in exposed config files) WebAshaIntellipaat



- **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



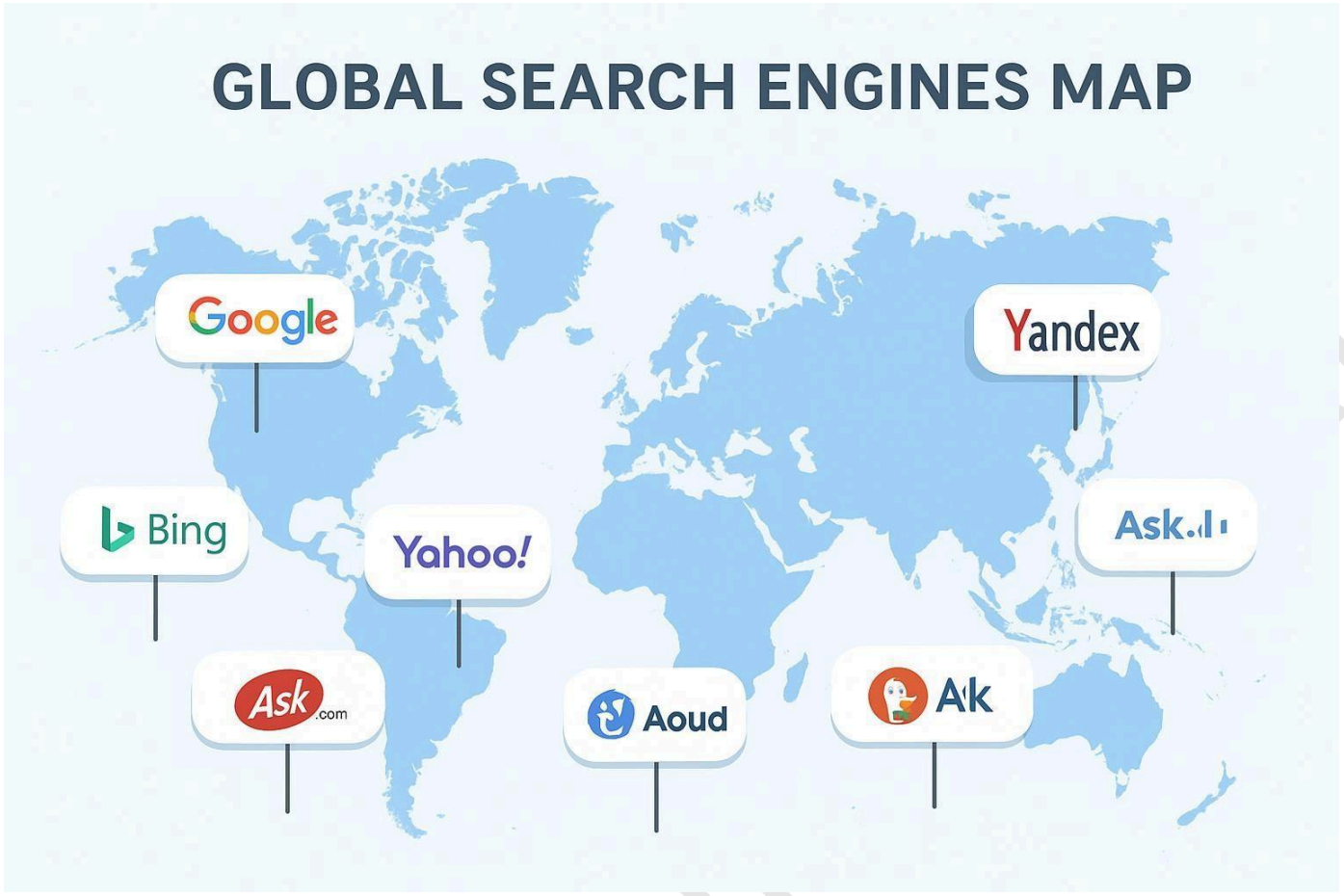
▪ Summary Table

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

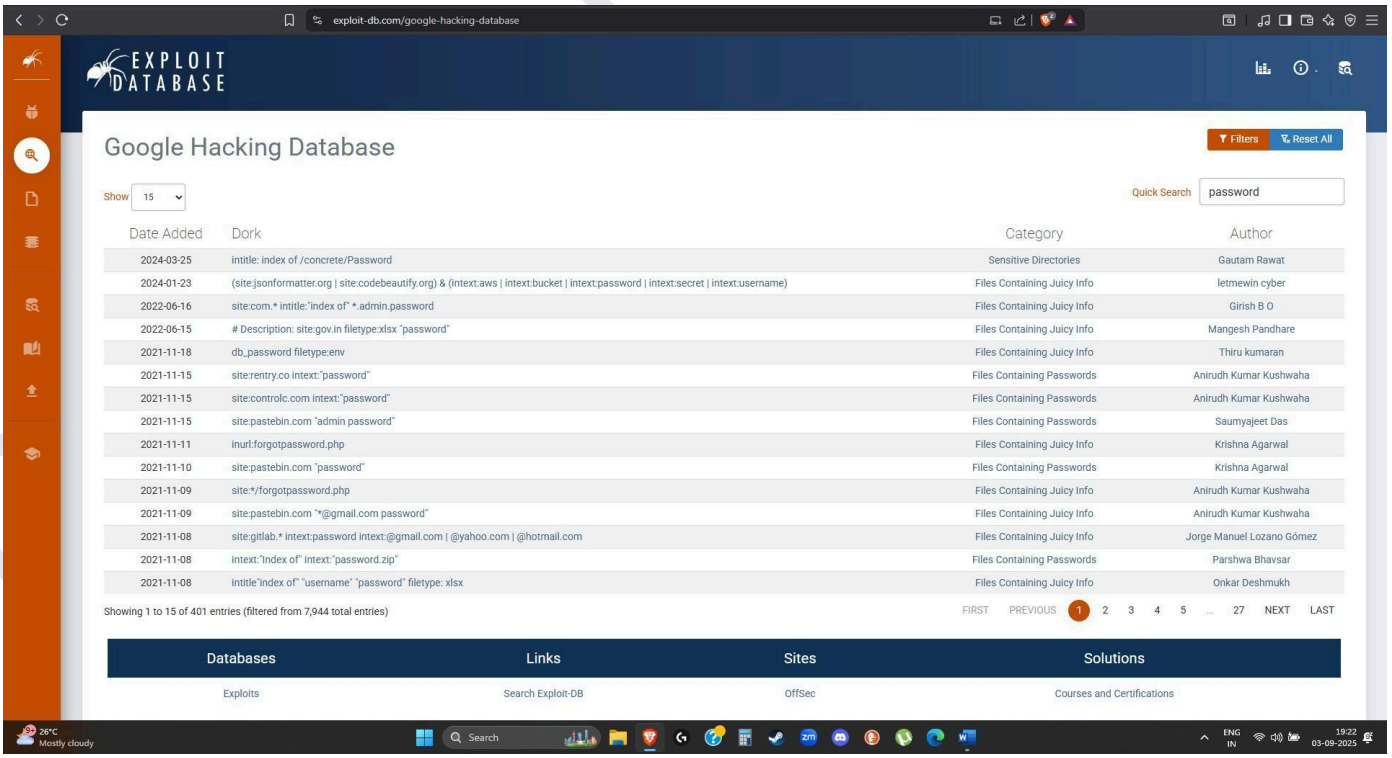
Legal considerations	Only use with authorization—misuse may violate laws like CFAA and GDPR

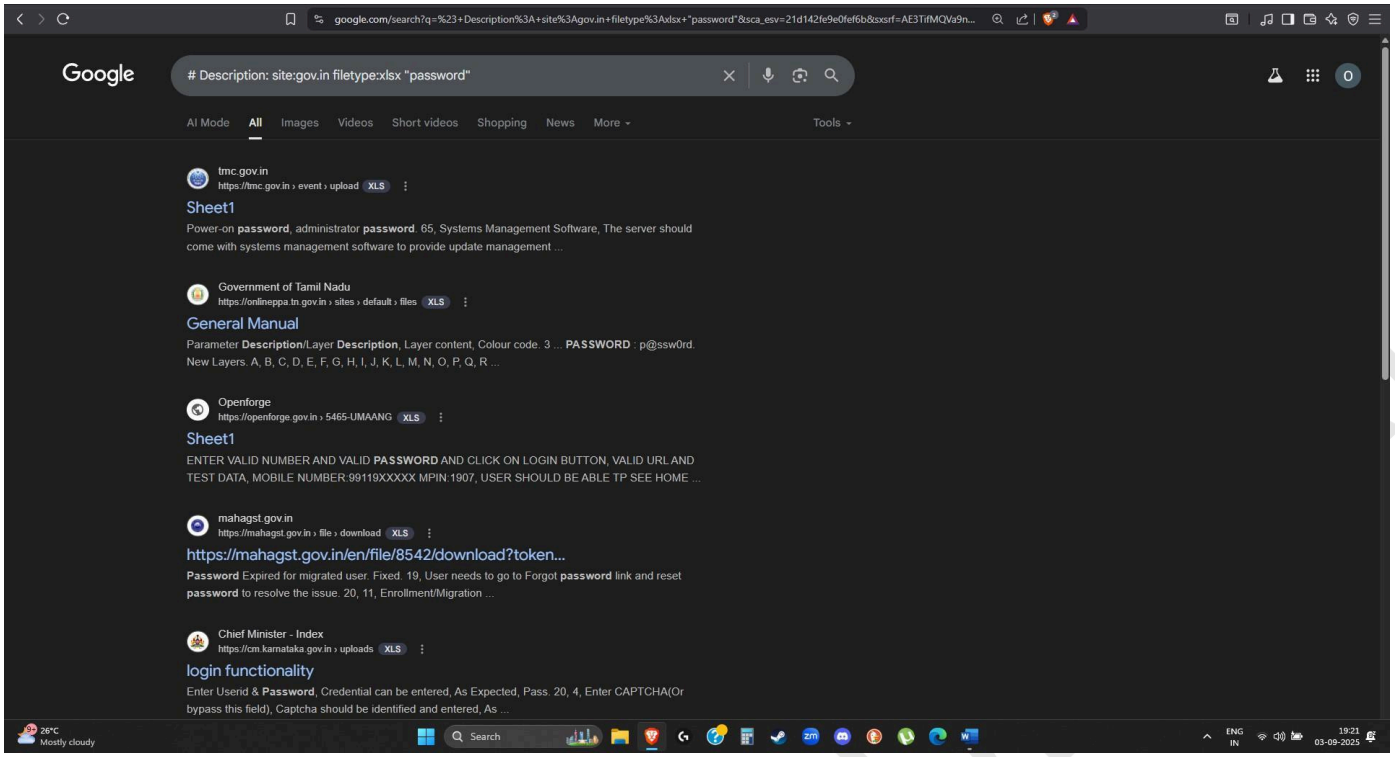
- **Examples of Major Search Engines:**

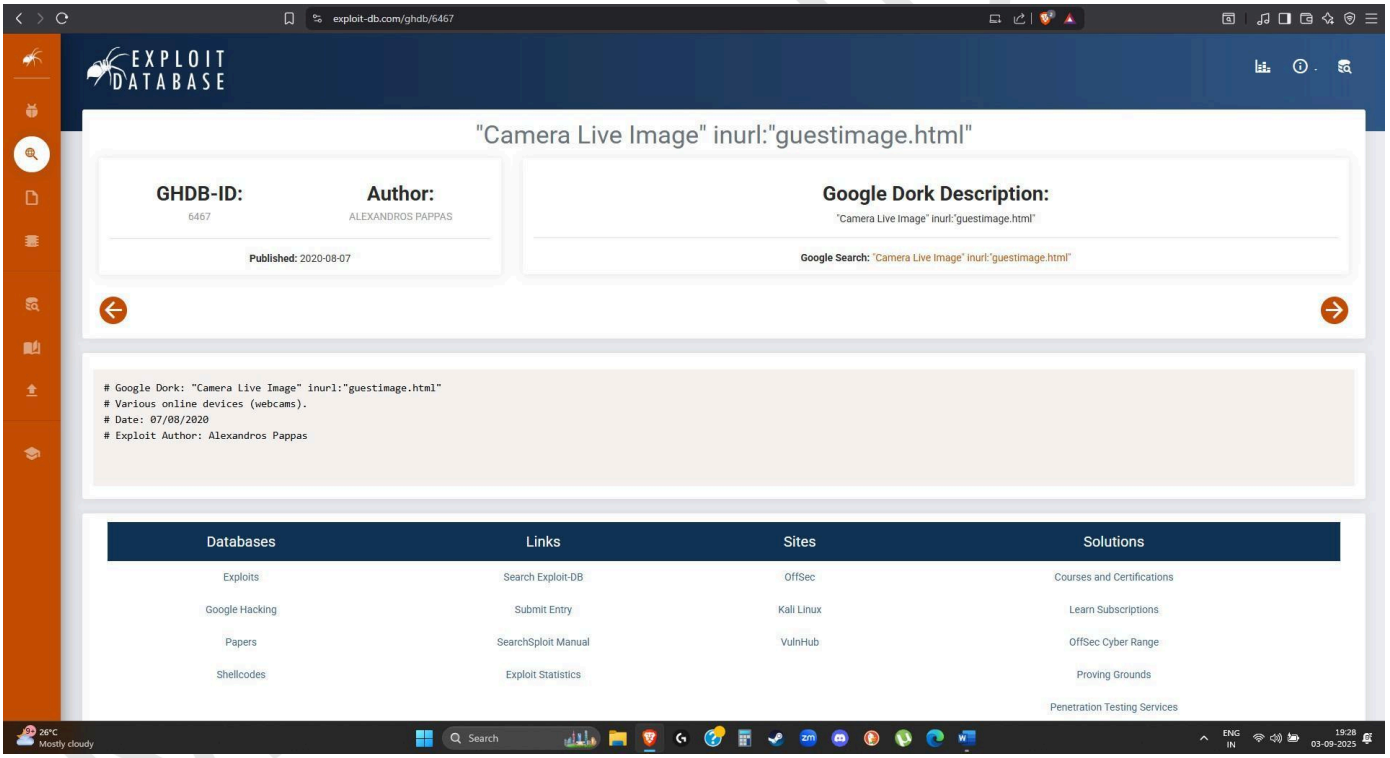
- **Google** – Most widely used global search engine.
- **Bing** – Microsoft's search engine.
- **Yahoo! Search** – Older but still in use.
- **Baidu** – Popular in China.
- **Yandex** – Popular in Russia.
- **DuckDuckGo** – Privacy-focused search engine.
- **Ask.com** – Question-answer based search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



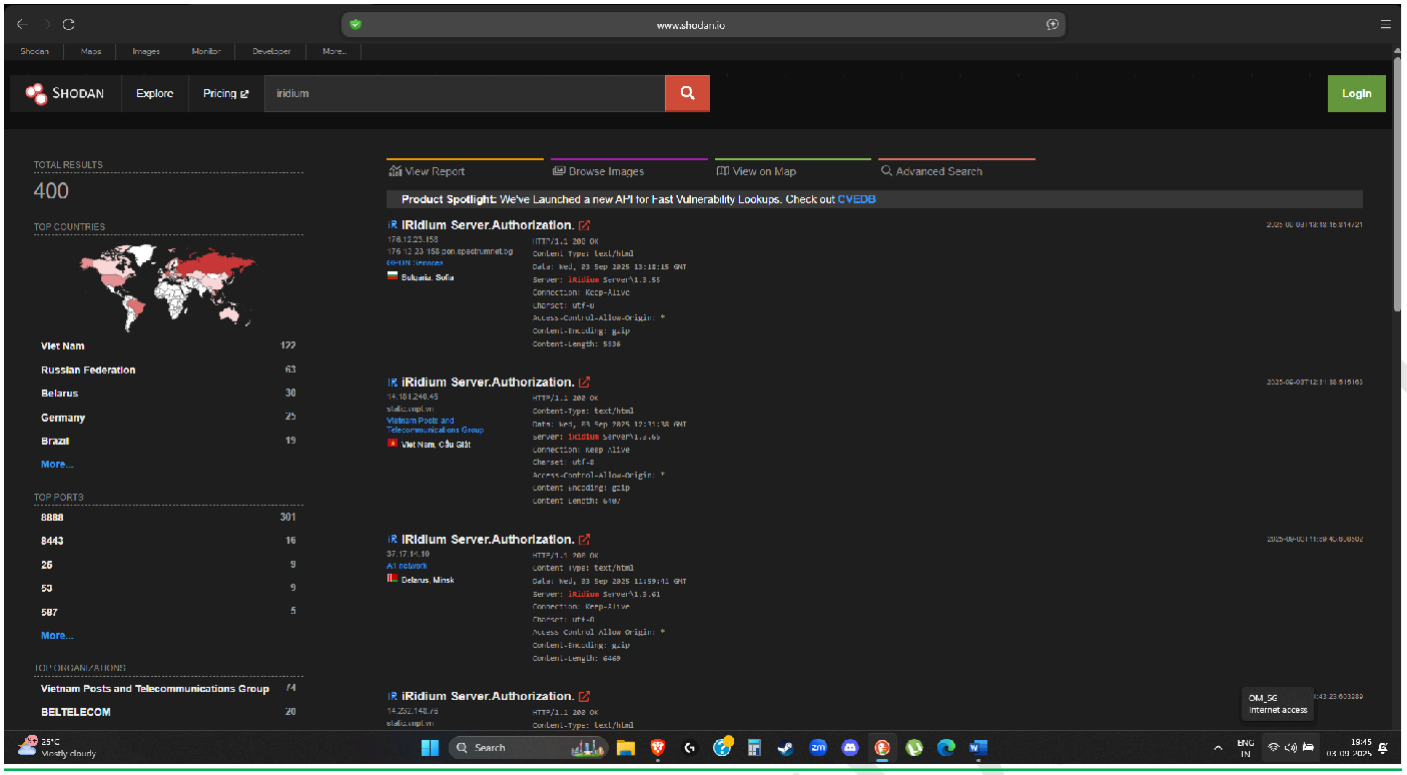
Foot-Printing using Advanced Google Hacking Database:



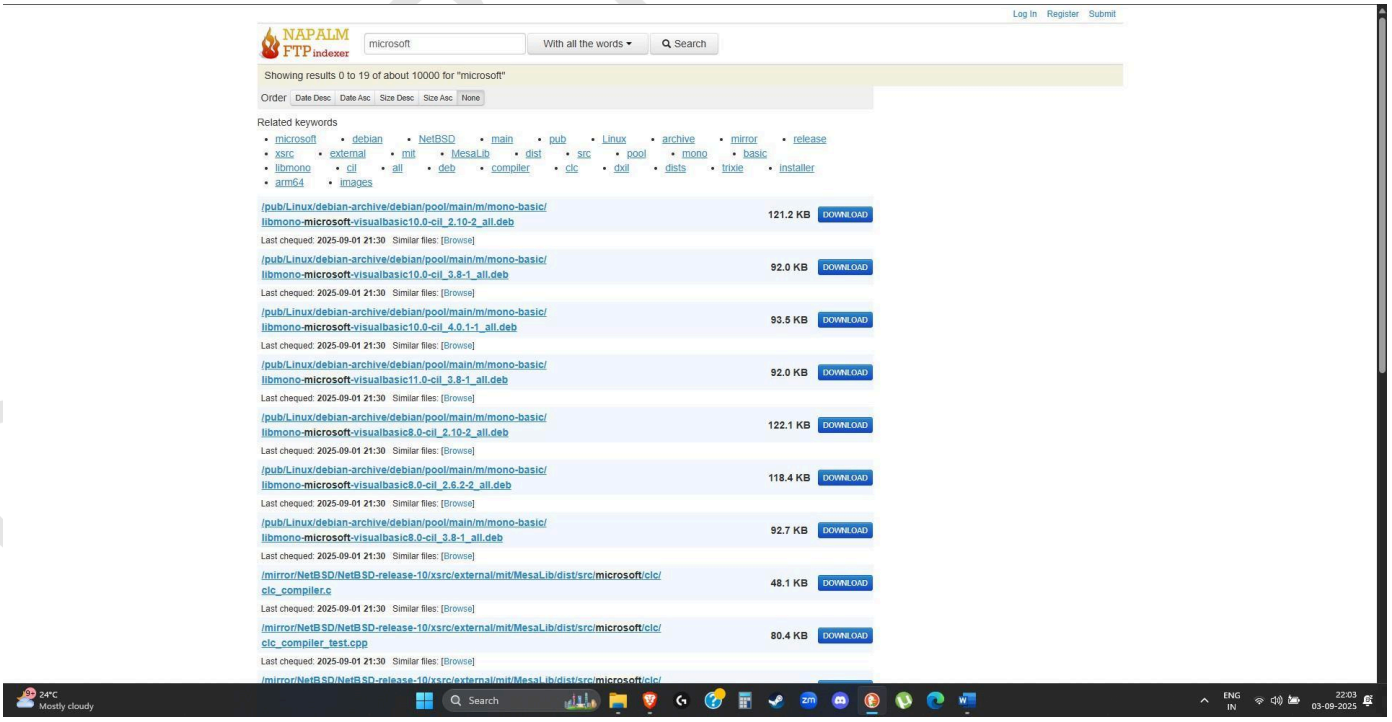




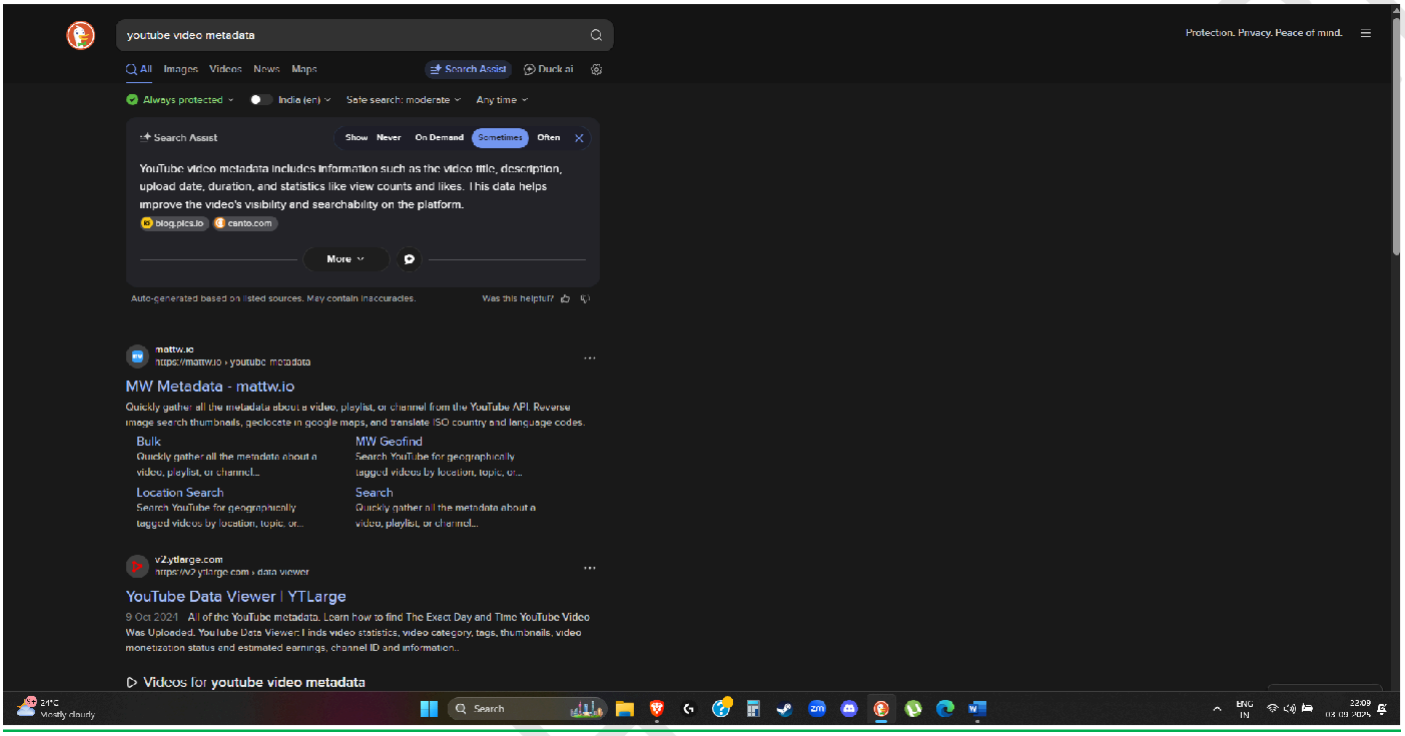
Foot-Printing using Shodan- IoT's Hacking:

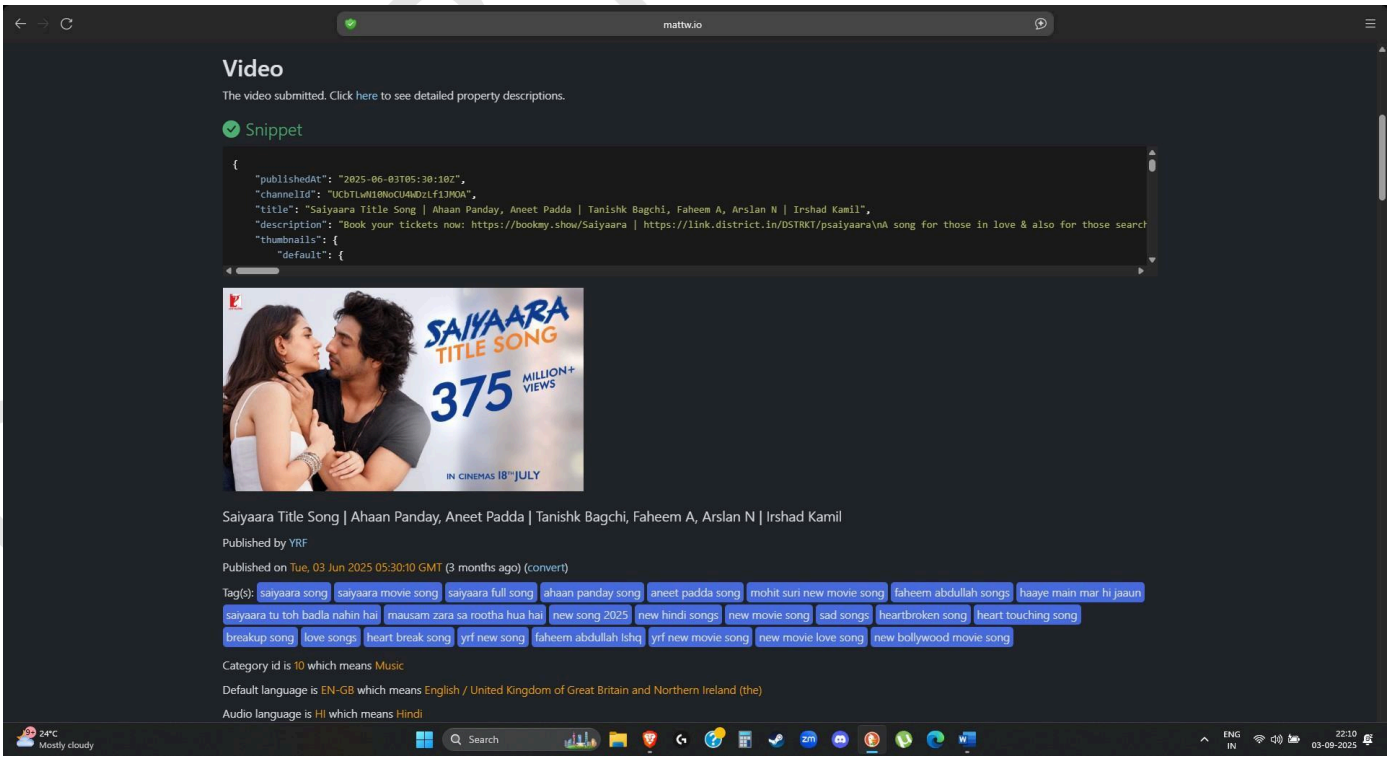


Foot-Printing using FTP Search Engine for Hacking:



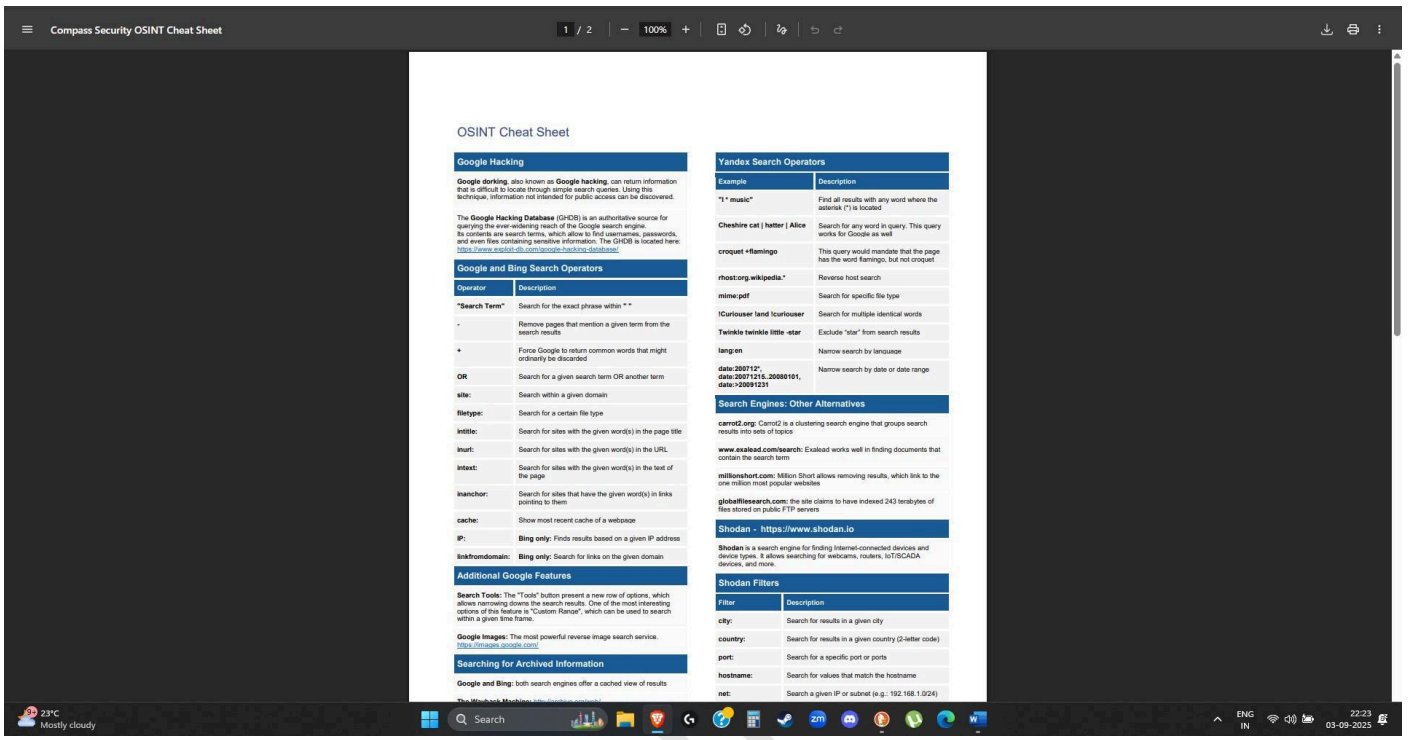
Foot-Printing using Video Search Engine(YouTube) for Hacking:





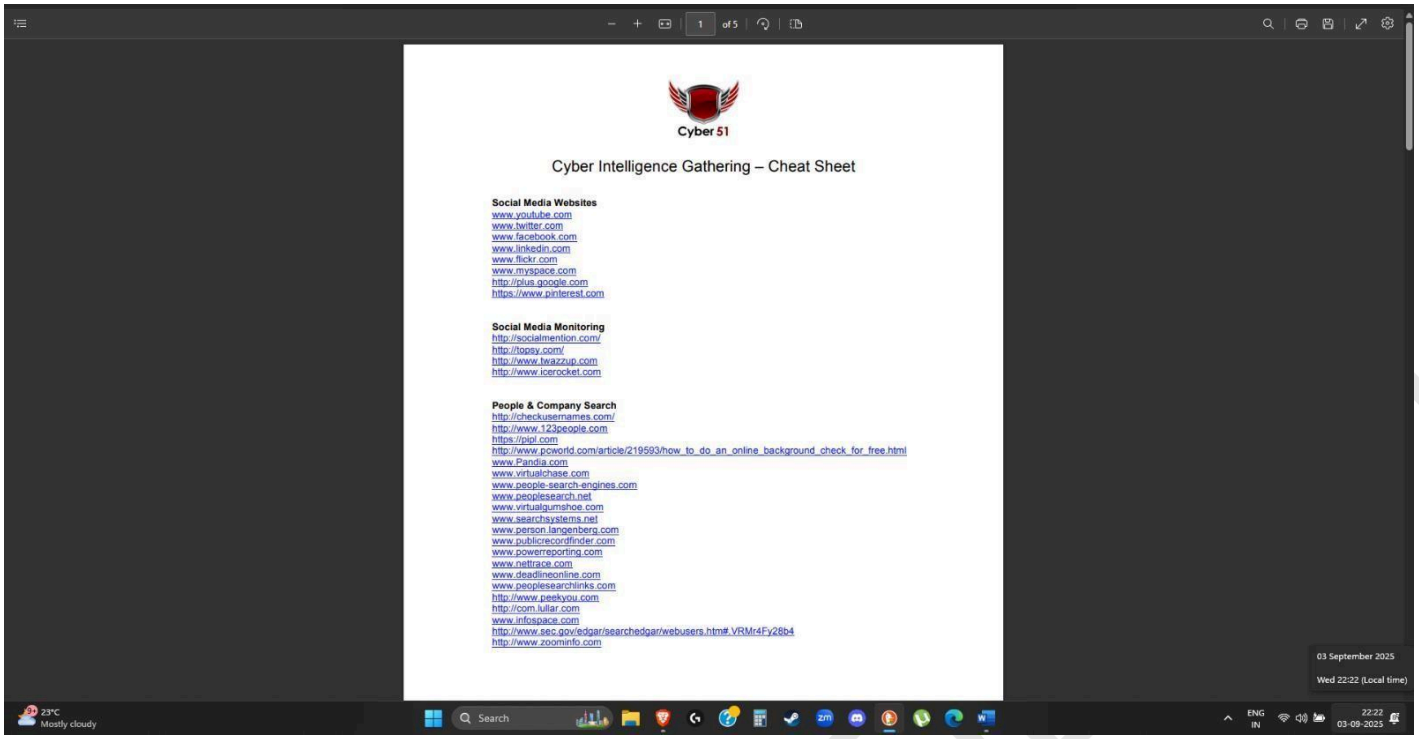
Foot-Printing using Cheat Sheets for Hacking:

- **Like OSINT cheat sheet:**



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

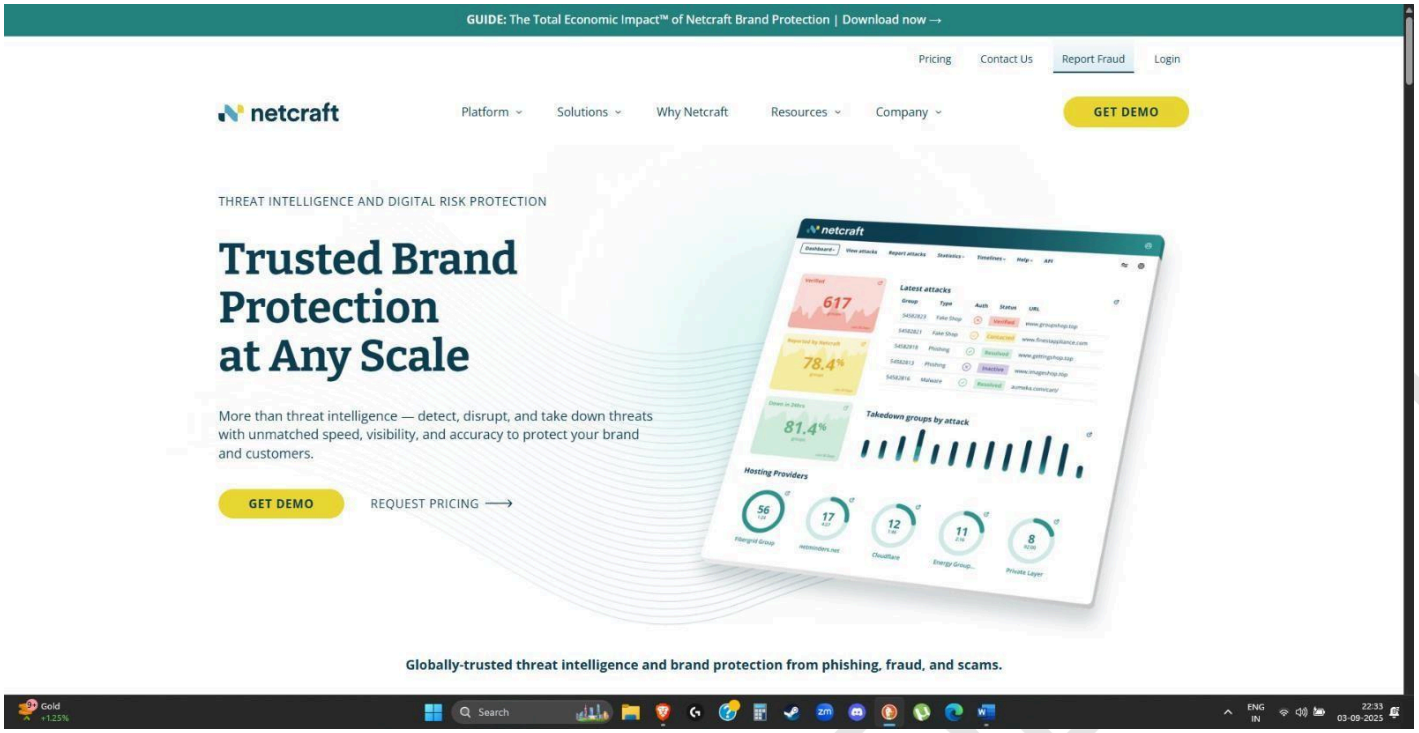
- **CIG cheat sheet:**

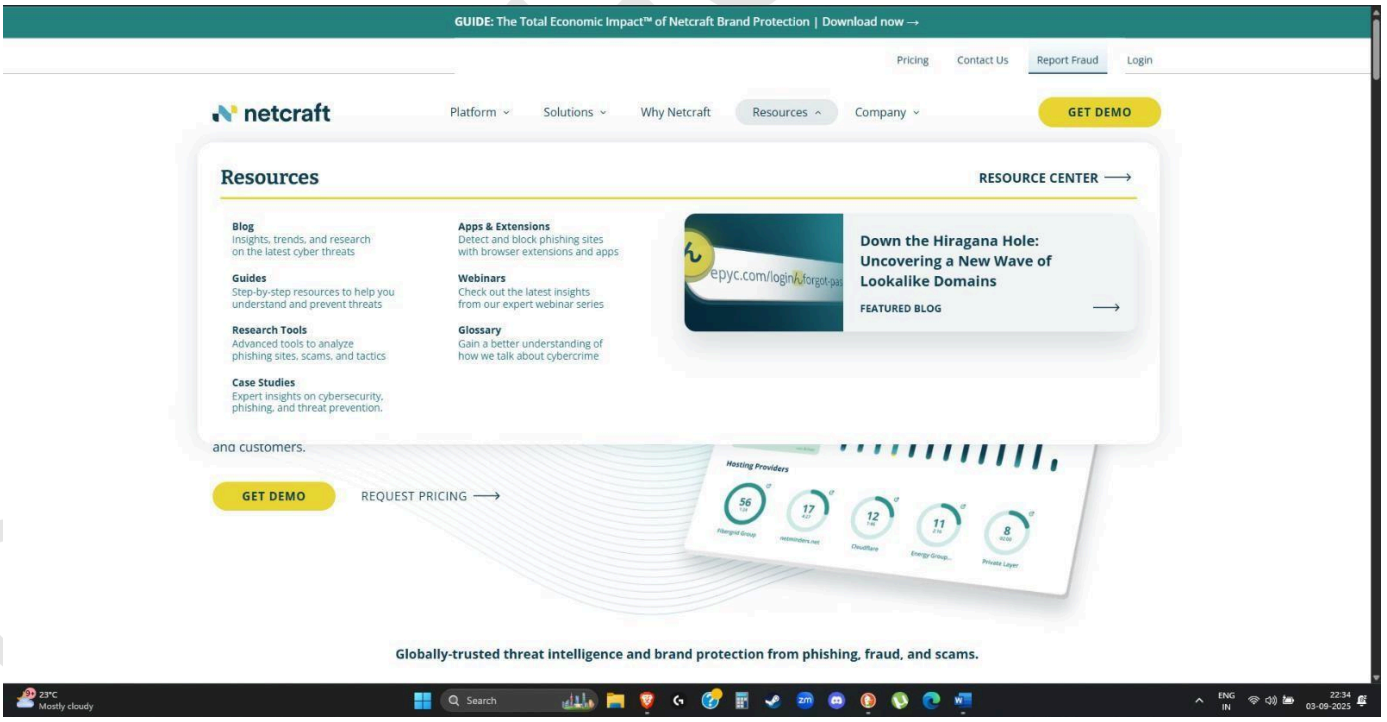


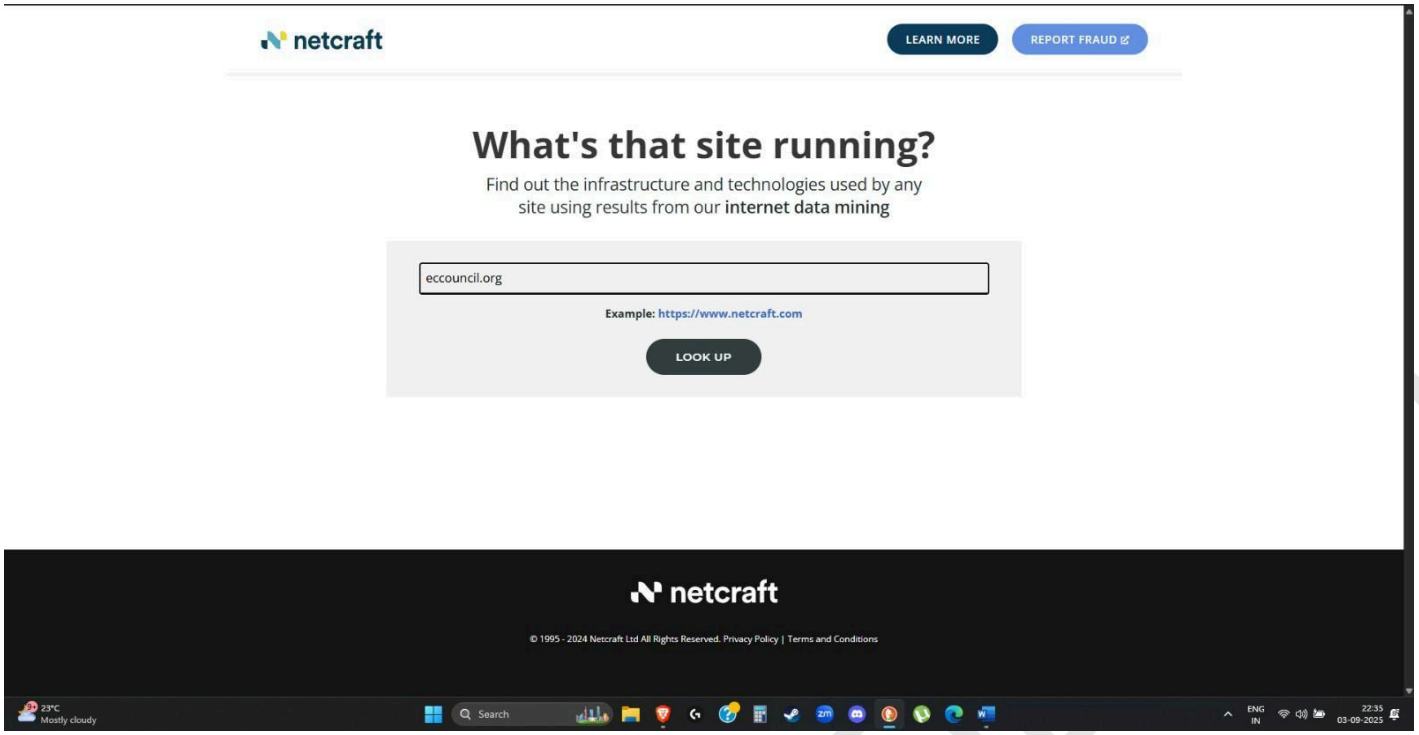
Foot-Printing using Through Internet Research Services for Hacking:

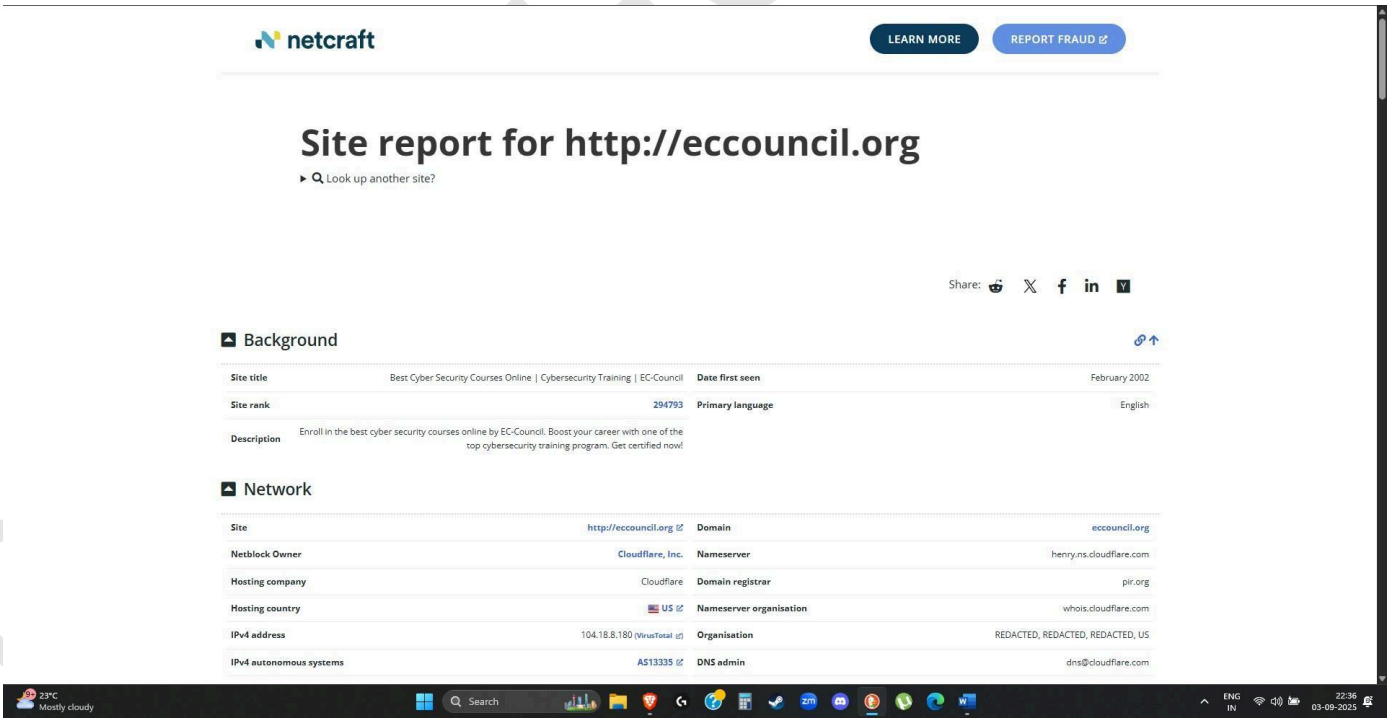
Find Company's Domains, Sub-Domains and Hosts using Netcraft and DNSdumpster:

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

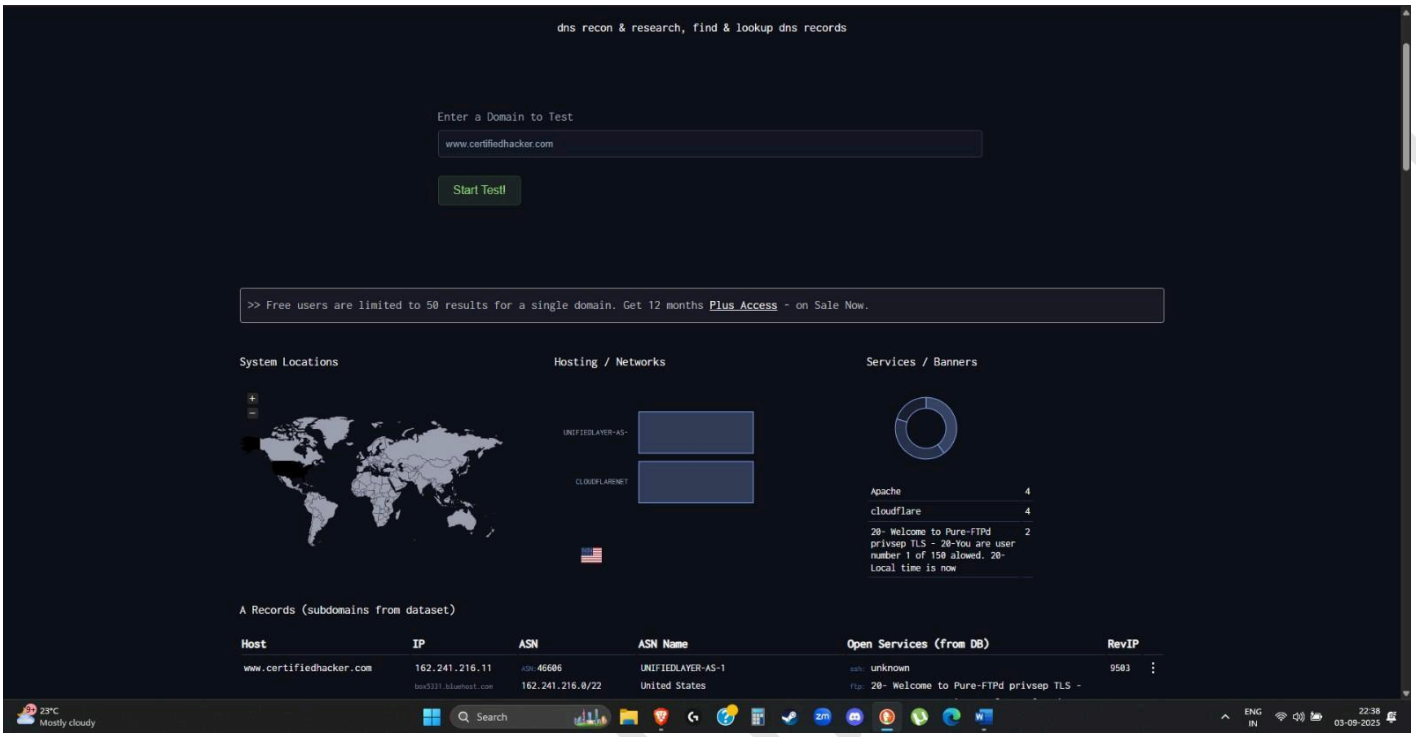

GUIDE: The Total Economic Impact™ of Netcraft Brand Protection | Download now →
Pricing
Contact Us
Report Fraud
Login
netcraft
Platform
Solutions
Why Netcraft
Resources
Company
GET DEMO
THREAT INTELLIGENCE AND DIGITAL RISK PROTECTION
Trusted Brand Protection at Any Scale
More than threat intelligence — 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
RESOURCE CENTER ⟶
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
Down the Hiragana Hole: Uncovering a New Wave of Lookalike Domains
FEATURED BLOG
and customers.
GET DEMO
REQUEST PRICING ⟶
Globally-trusted threat intelligence and brand protection from phishing, fraud, and scams.

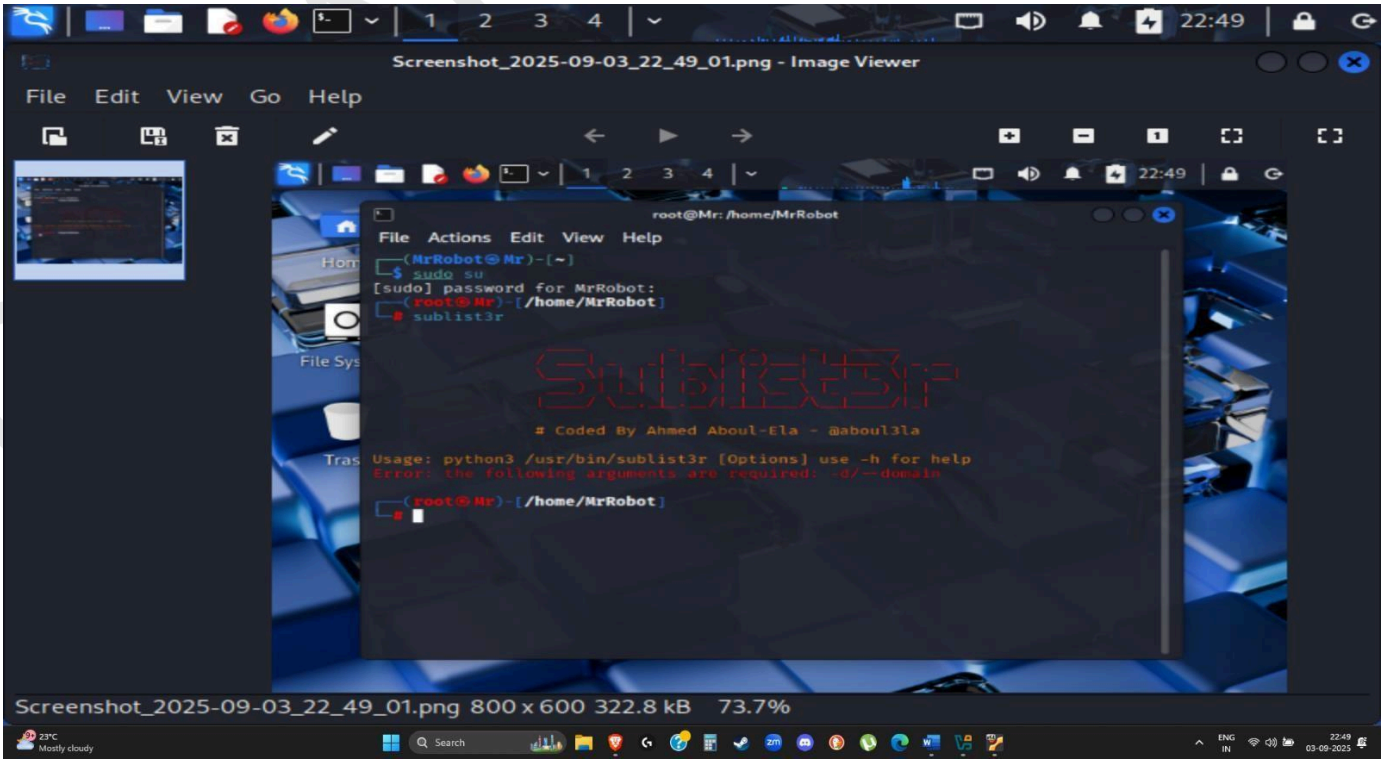

netcraft
LEARN MORE
REPORT FRAUD
What's that site running?
Find out the infrastructure and technologies used by any site using results from our internet data mining
eccouncil.org
Example: https://www.netcraft.com
LOOK UP
netcraft
© 1995 - 2024 Netcraft Ltd All Rights Reserved. Privacy Policy | Terms and Conditions
23°C
Mostly cloudy
Search
ENG
IN
22:35
03-09-2025

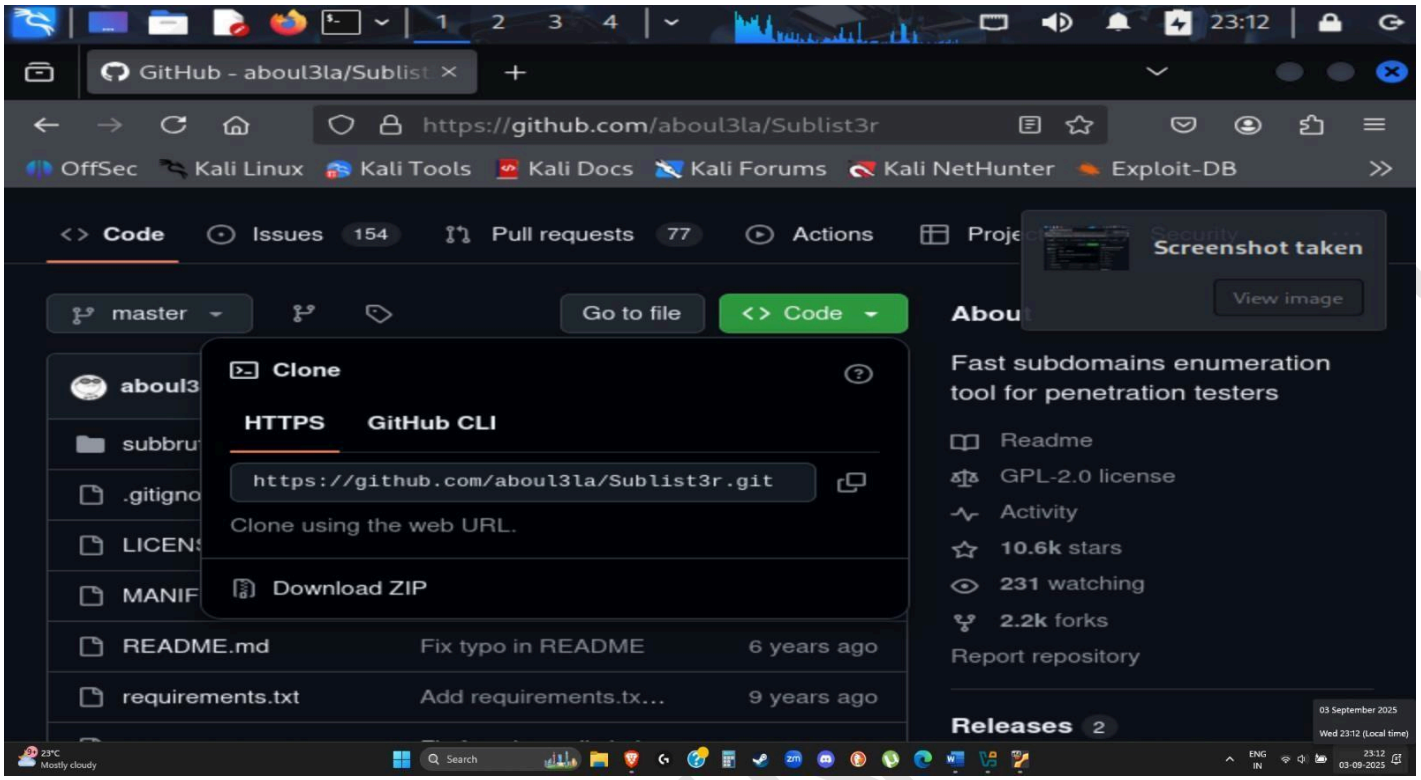

netcraft
LEARN MORE
REPORT FRAUD
Site report for http://eccouncil.org
Look up another site?
Share:
Background
Site title
Best Cyber Security Courses Online | Cybersecurity Training | EC-Council
Date first seen
February 2002
Site rank
294793
Primary language
English
Description
Enroll in the best cyber 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
ENG
IN
22:36
03-09-2025

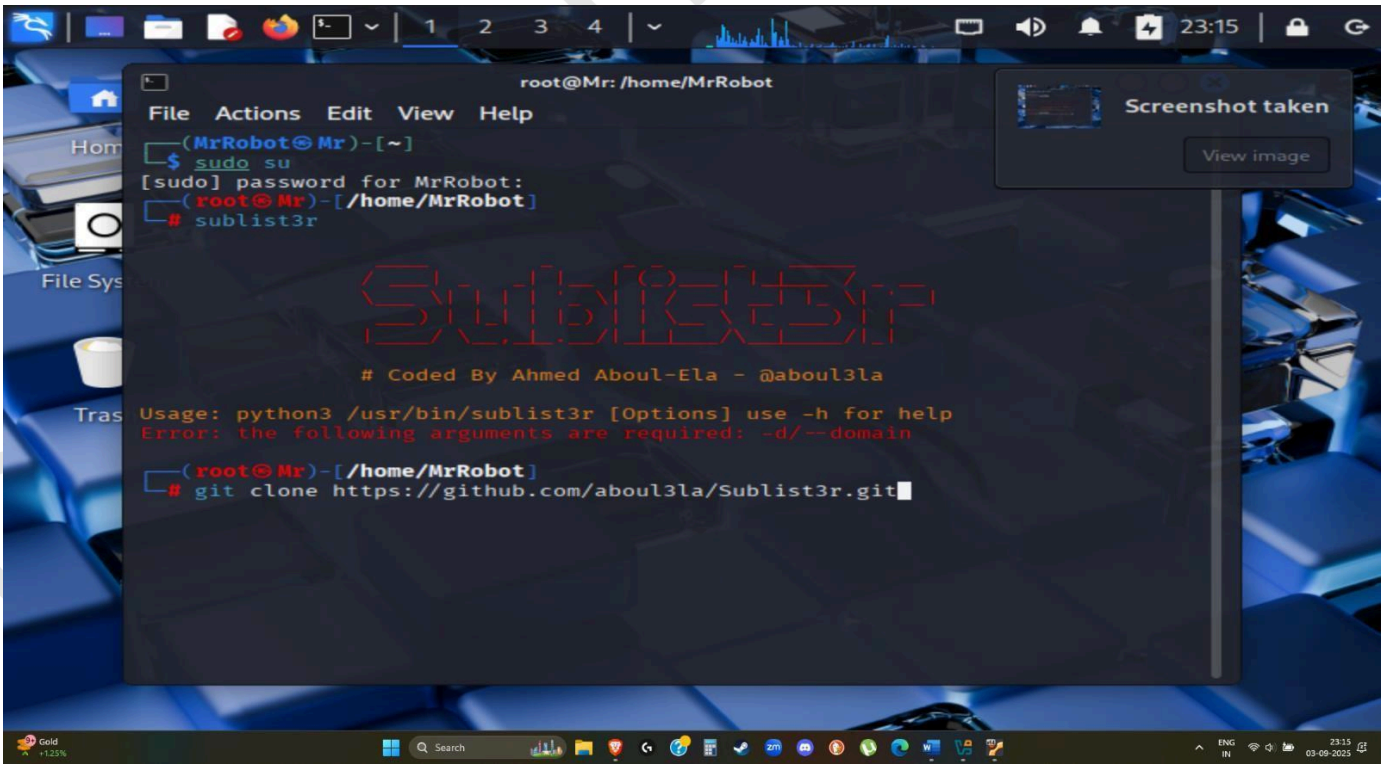
 Extracting Company Domains and Sub-Domains using DNSdumpster tools:



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

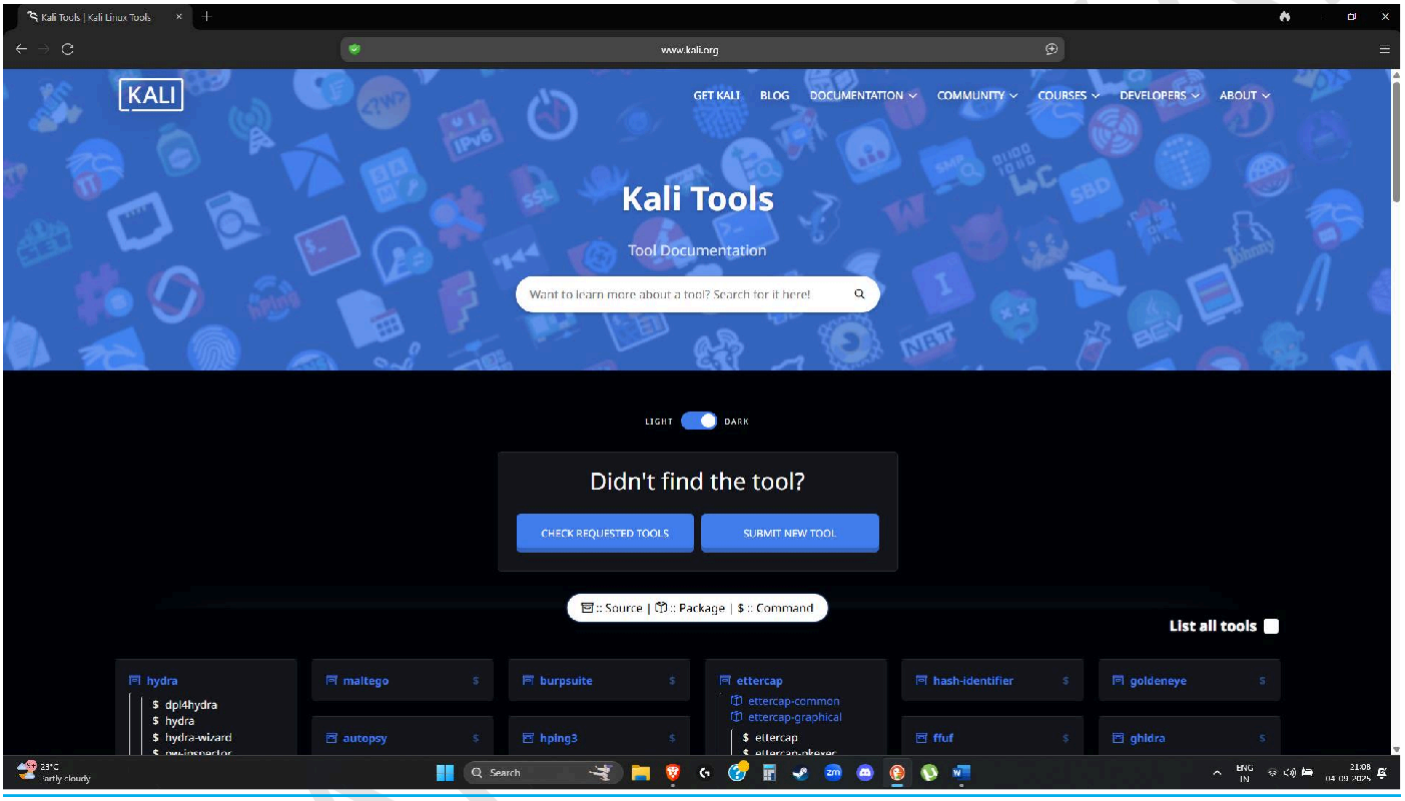



GitHub - aboul3la/Sublist
https://github.com/aboul3la/Sublist3r
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Code
Issues 154
Pull requests 77
Actions
Screenshot taken
View image
master
Go to file
Code
Clone
HTTPS
GitHub CLI
https://github.com/aboul3la/Sublist3r.git
Clone using the web URL.
Download ZIP
README.md
Fix typo in README
6 years ago
requirements.txt
Add requirements.tx...
9 years ago
Fast subdomains enumeration tool for penetration testers
Readme
GPL-2.0 license
Activity
10.6k stars
231 watching
2.2k forks
Report repository
Releases 2

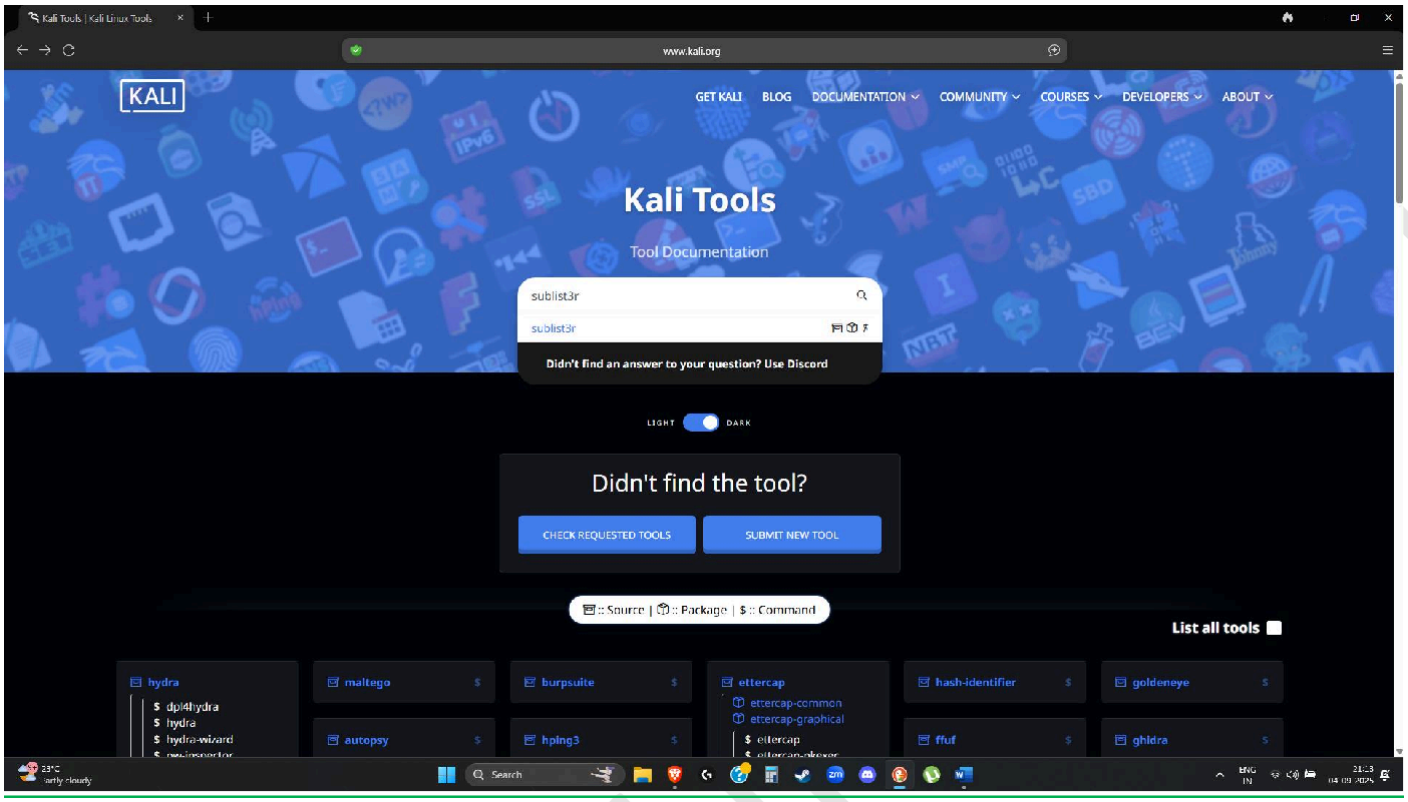

root@Mr: /home/MrRobot
File Actions Edit View Help
(MrRobot㉿Mr)-[~]
$ sudo su
[sudo] password for MrRobot:
(root㉿Mr)-[/home/MrRobot]
sublist3r
Coded By Ahmed Aboul-Ela - @aboul3la
Usage: python3 /usr/bin/sublist3r [Options] use -h for help
Error: the following arguments are required: -d/--domain
(root㉿Mr)-[/home/MrRobot]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

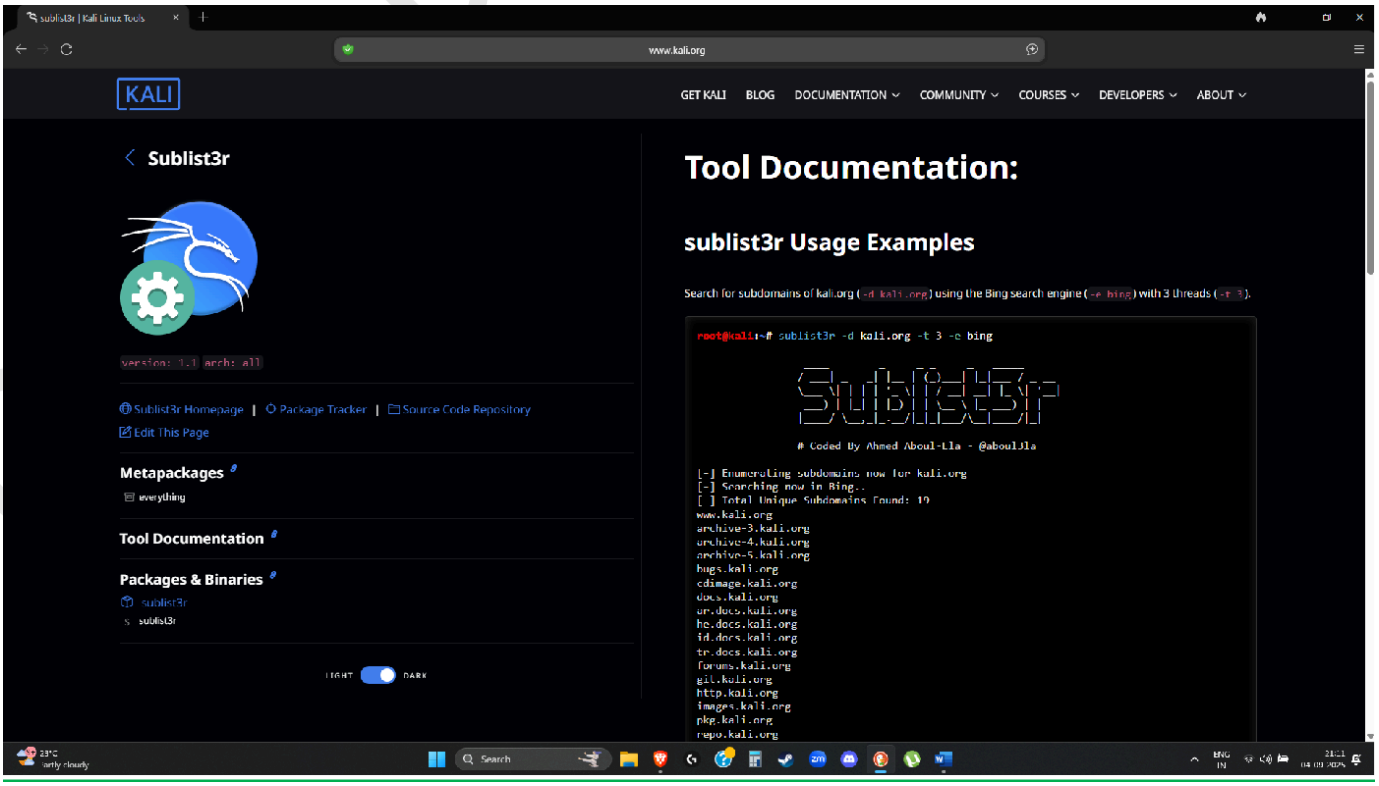
 Now understanding what is Sublist3r tool and how to use:

- **Open Kali Tools on Google:**

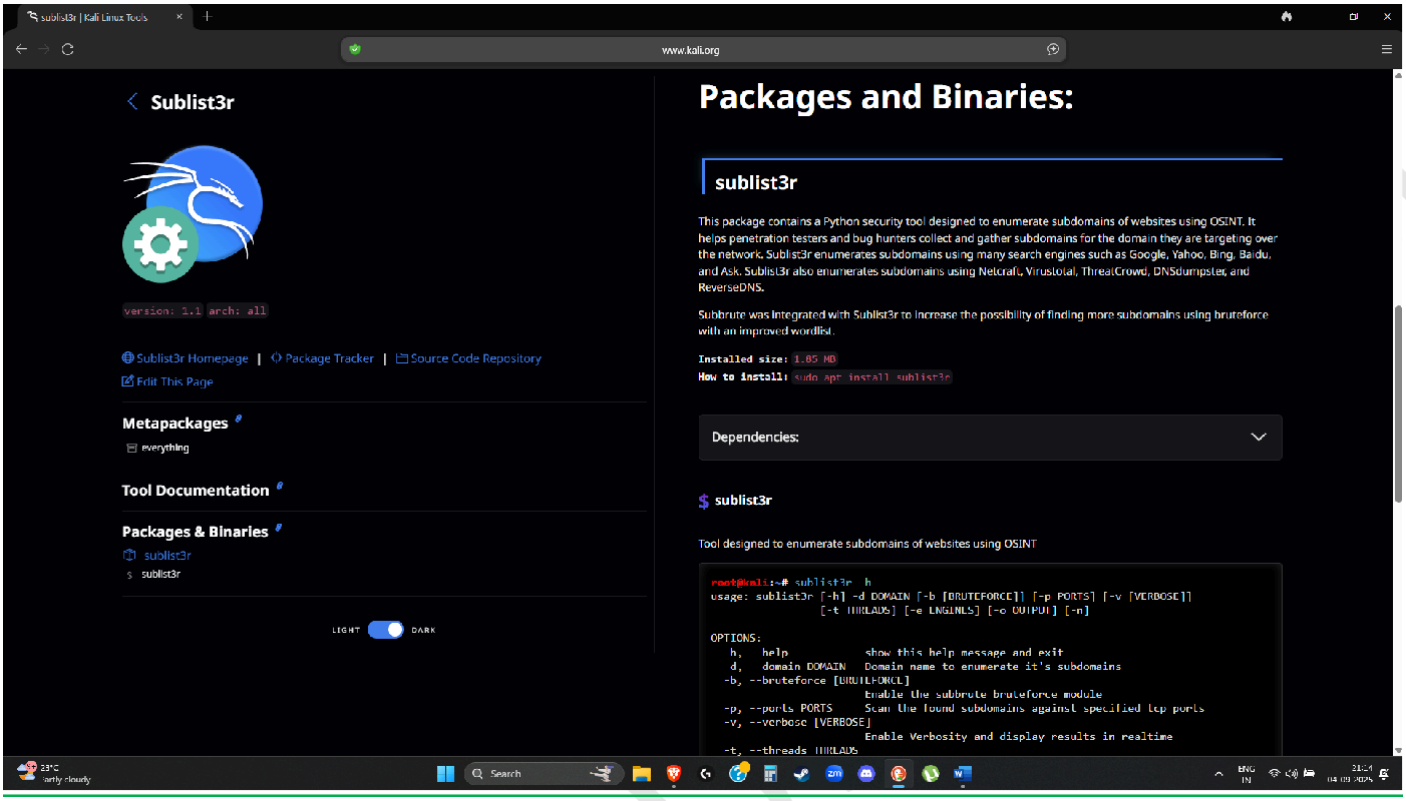


- **Type Sublist3r and Press Enter :**


Kali Tools | Kali Linux Tools
www.kali.org
KALI
GET KALI
BLOG
DOCUMENTATION
COMMUNITY
COURSES
DEVELOPERS
ABOUT
Kali Tools
Tool Documentation
sublist3r
sublist3r
Didn't find an answer to your question? Use Discord
LIGHT
DARK
Didn't find the tool?
CHECK REQUESTED TOOLS
SUBMIT NEW TOOL
:: Source | :: Package | $ :: Command
List all tools
hydra
$ dpl4hydra
$ hydra
$ hydra-wizard
maltego
burpsuite
ettercap
ettercap-common
ettercap-graphical
$ ettercap
hash-identifier
goldeneye
autopsy
hping3
ffuf
ghidra
Search


sublist3r | Kali Linux Tools
www.kali.org
KALI
GET KALI
BLOG
DOCUMENTATION
COMMUNITY
COURSES
DEVELOPERS
ABOUT
Sublist3r
version: 1.1 arch: all
Sublist3r Homepage | Package Tracker | Source Code Repository
Edit This Page
Metapackages
everything
Tool Documentation
Packages & Binaries
sublist3r
sublist3r
LIGHT
DARK
Tool Documentation:
sublist3r Usage Examples
Search for subdomains of kali.org (-d kali.org) using the Bing search engine (-e bing) with 3 threads (-t 3).
root@kali:~# sublist3r -d kali.org -t 3 -e bing
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for kali.org
[-] Searching now in Bing..
[ ] Total Unique Subdomains Found: 19
www.kali.org
archive-3.kali.org
archive-4.kali.org
archive-5.kali.org
bugs.kali.org
cdimage.kali.org
docs.kali.org
ar.docs.kali.org
he.docs.kali.org
id.docs.kali.org
tr.docs.kali.org
forums.kali.org
gil.kali.org
http.kali.org
images.kali.org
pkg.kali.org
repo.kali.org
Search

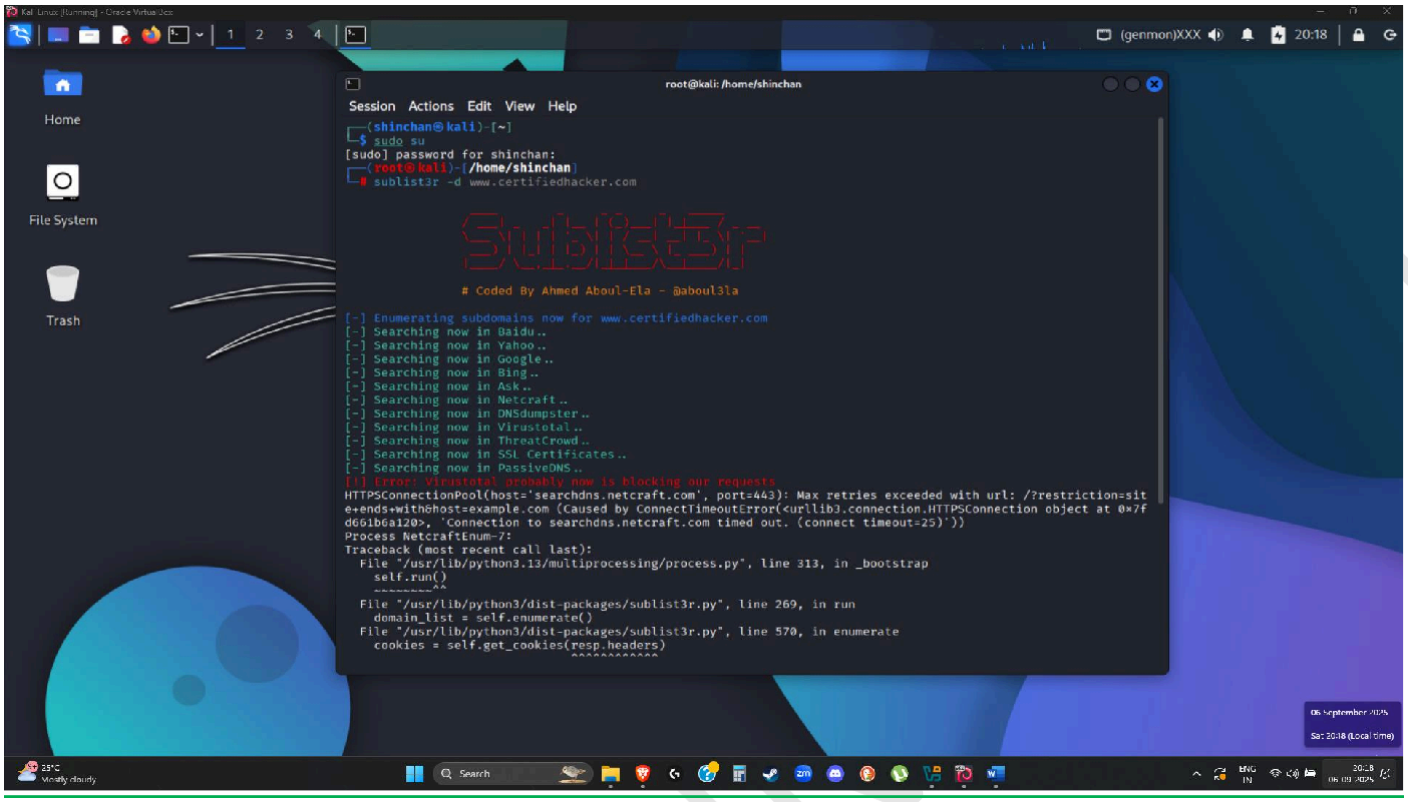
- **Type Sublist3r Package and Binaries:**

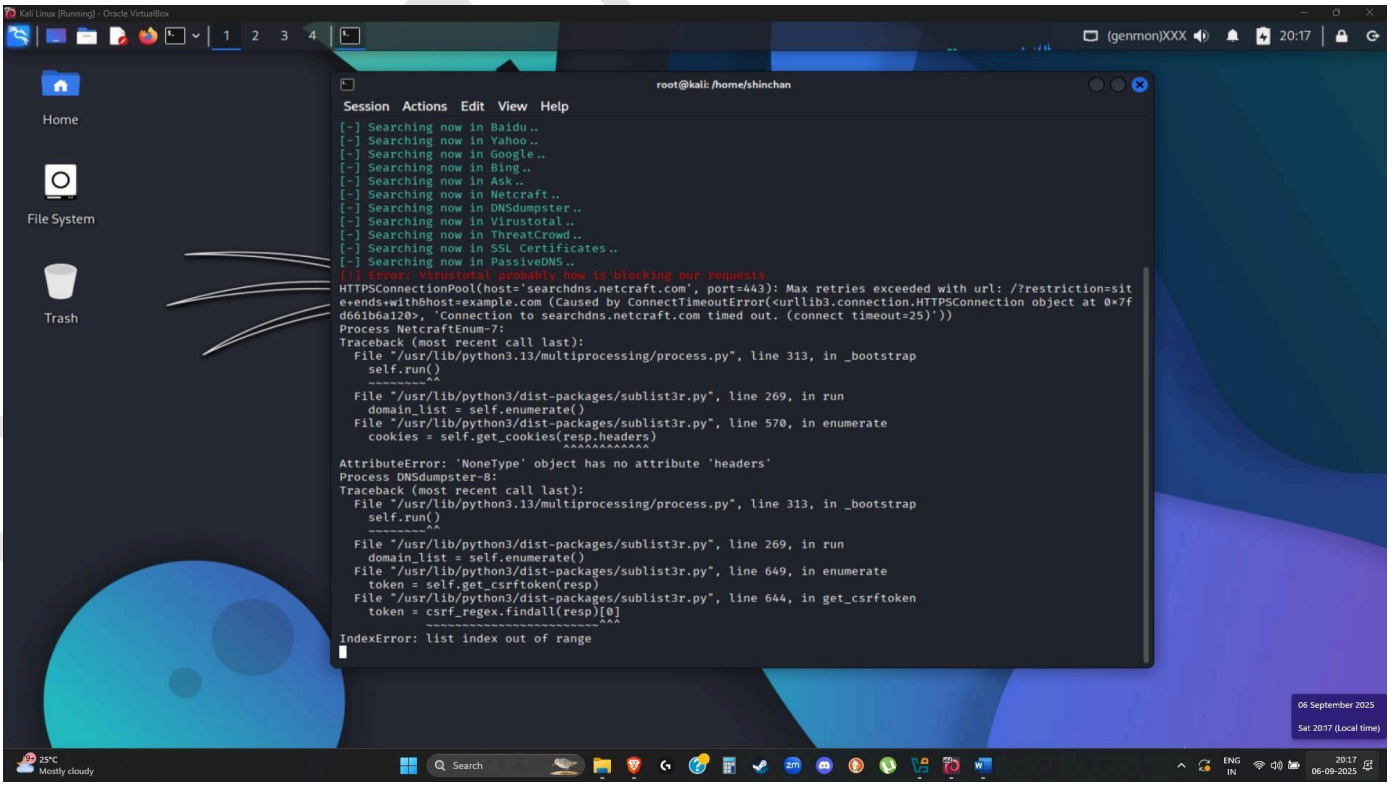


Foot-Printing Through Social Networking Sites for Hacking:

 Now understanding what is Sublist3r tool and how to use:

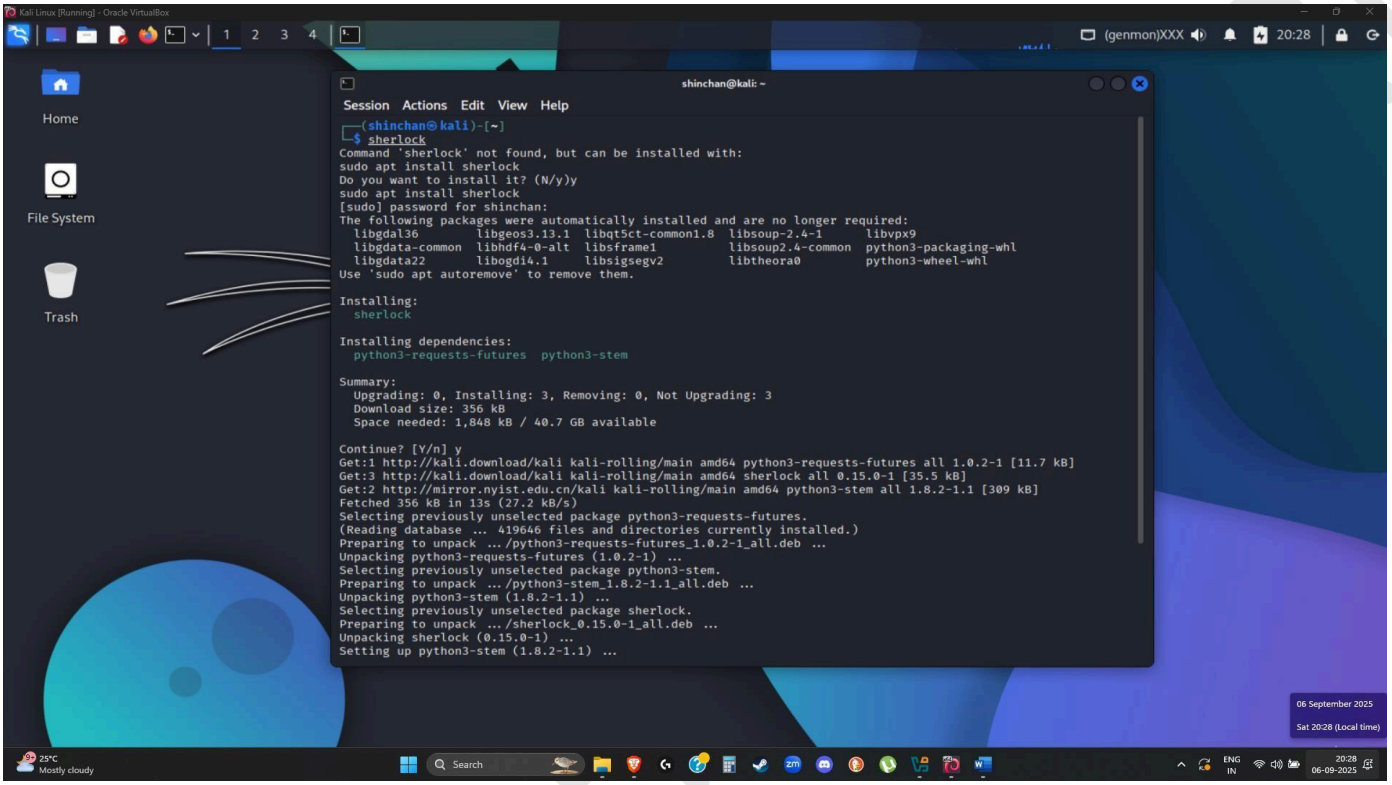
- **Type Sublist3r -d (any domain) www.certifiedhacker.com:**


Kali Linux [Running] - Oracle VirtualBox
(genmon)XXX
20:18
Home
File System
Trash
root@kali: /home/shinchan
Session Actions Edit View Help
(shinchan㉿kali)-[~]
$ sudo su
[sudo] password for shinchan:
(root㉿kali)-[/home/shinchan]
sublist3r -d www.certifiedhacker.com
Coded By Ahmed Aboul-Ela - @aboul3la
[-] 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
HTTPSConnectionPool(host='searchdns.netcraft.com', port=443): Max retries exceeded with url: /?restriction=site+ends+with&host=example.com (Caused by ConnectTimeoutError(<urllib3.connection.HTTPSConnection object at 0x7fd661b6a120>, '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()
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)
06 September 2025
Sat 20:18 (Local time)
25°C
Mostly cloudy
Search
ENG
IN
20:18
06-09-2025

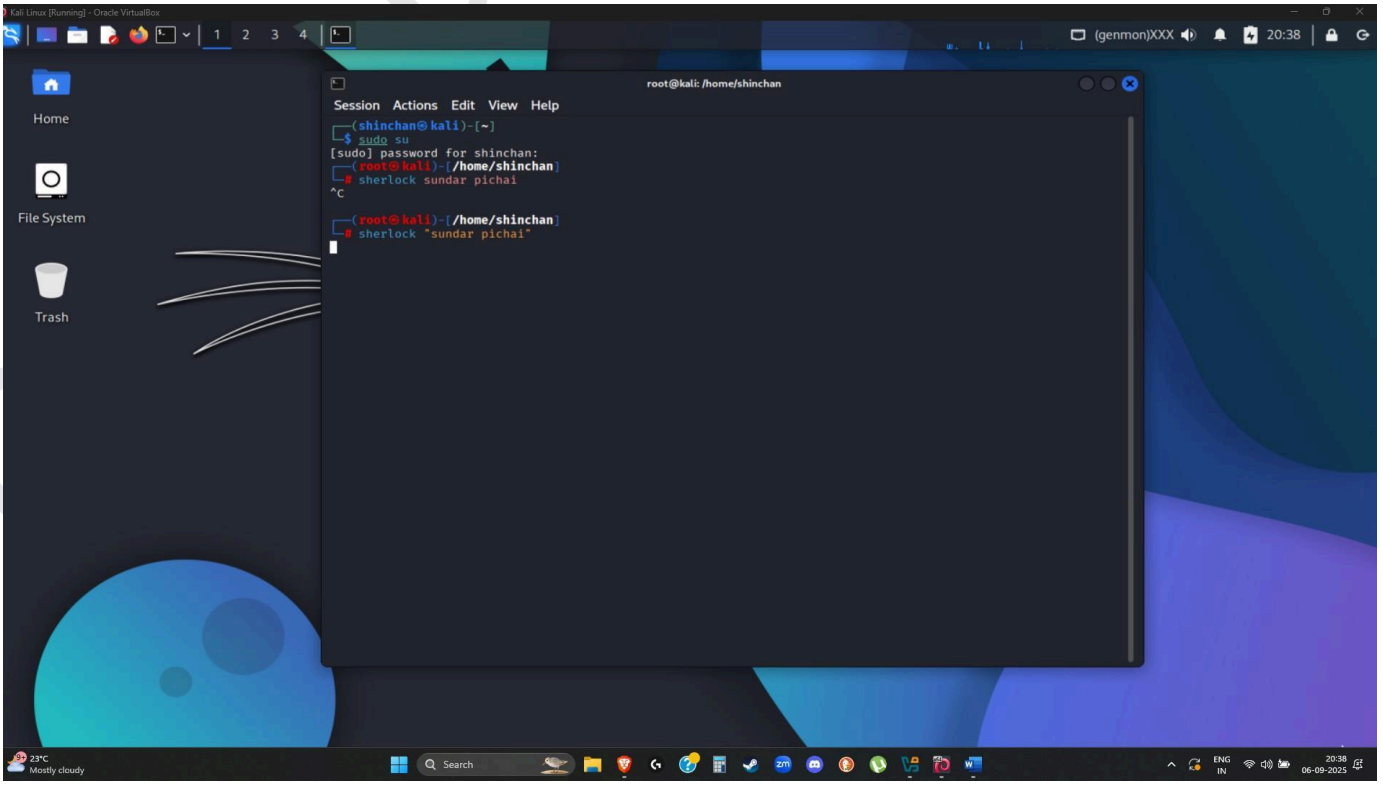

Kali Linux [Running] - Oracle VirtualBox
(genmon)XXX
20:17
Home
File System
Trash
root@kali: /home/shinchan
Session Actions Edit View Help
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in 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
HTTPSConnectionPool(host='searchdns.netcraft.com', port=443): Max retries exceeded with url: /?restriction=site+ends+with&host=example.com (Caused by ConnectTimeoutError(<urllib3.connection.HTTPSConnection object at 0x7fd661b6a120>, '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()
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()
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
06 September 2025
Sat 20:17 (Local time)
25°C
Mostly cloudy
Search
ENG
IN
20:17
06-09-2025

Now Gathering Information Through Social Media Sites using Sherlock:

- First Install Sherlock by typing ‘sherlock command’.



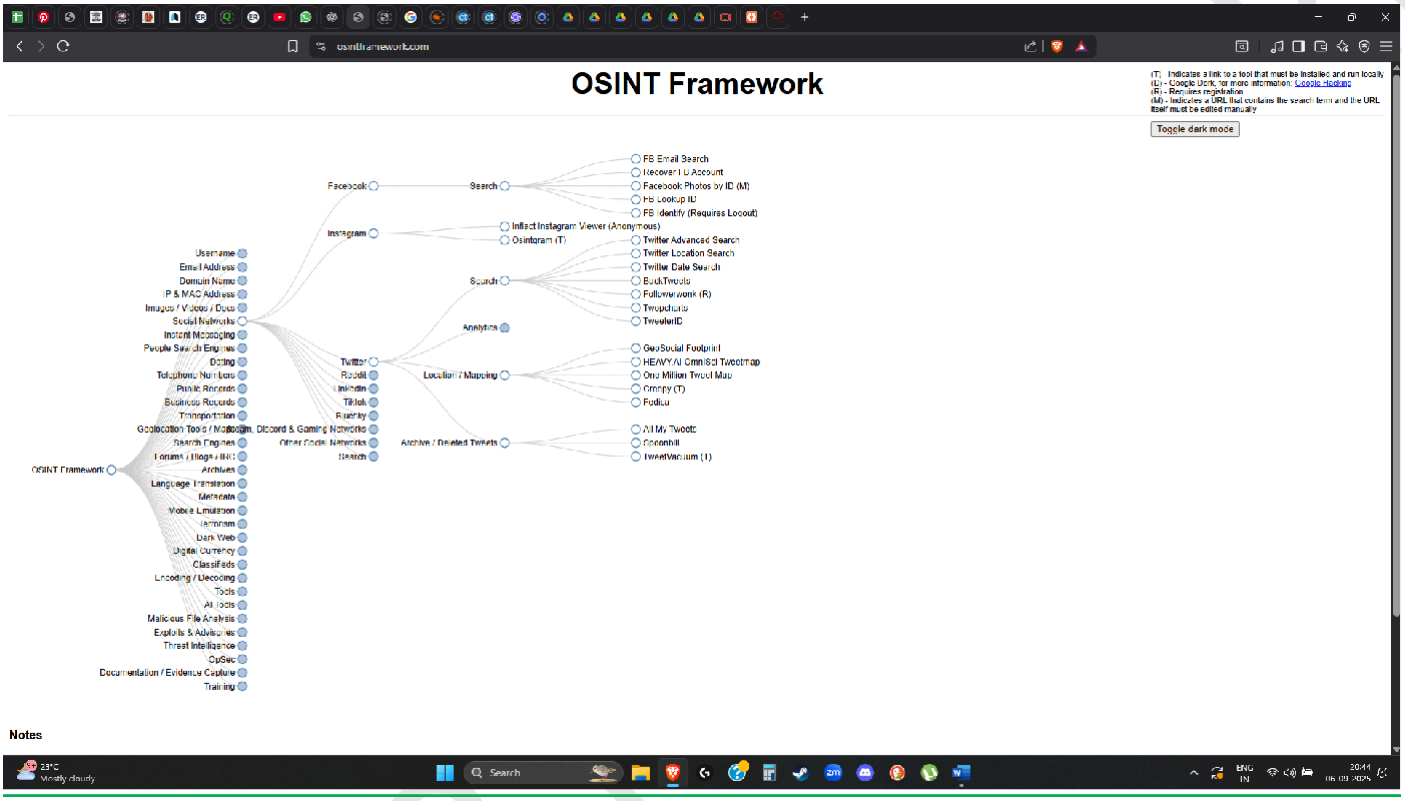
- Now use Sherlock to gather information, for example:



Foot-Printing for Social Media Hacking using

OSINT Framework:

- Performed using OSINT Framework.



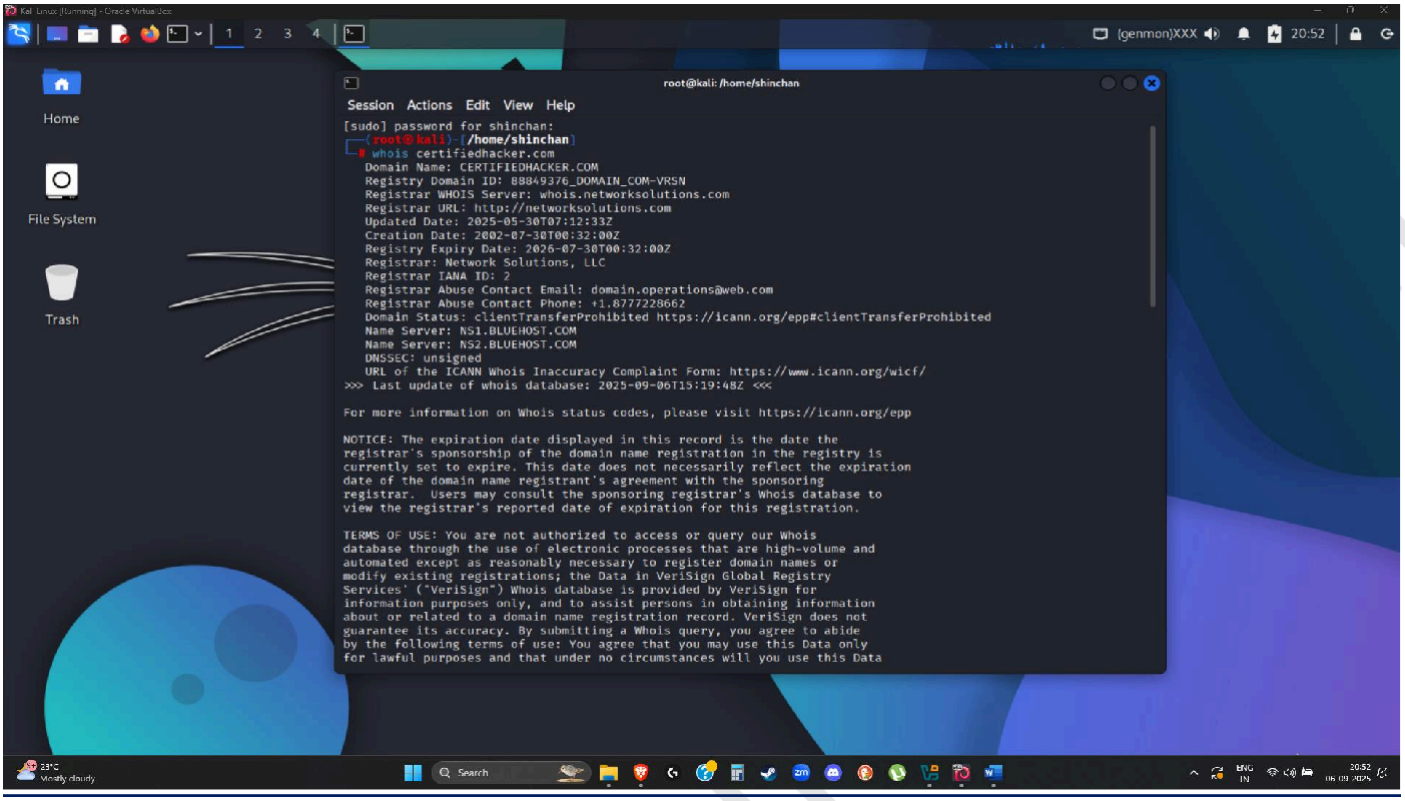
Foot-Printing by performing Whois for Hacking:

- Performed to reveal available information on a Hostnames, ip addresses or Domains.

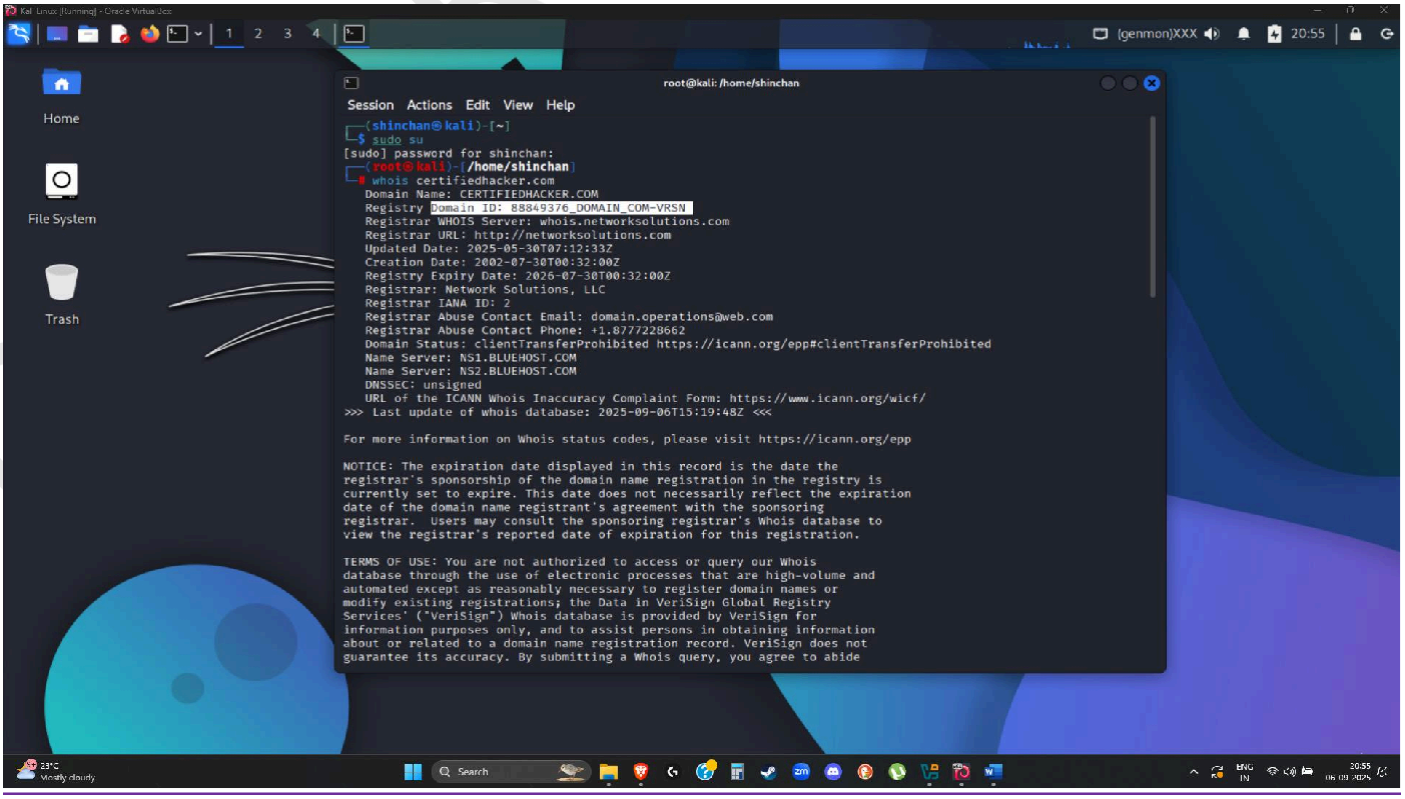
 Example next page:

- Like Domain name, Domain id

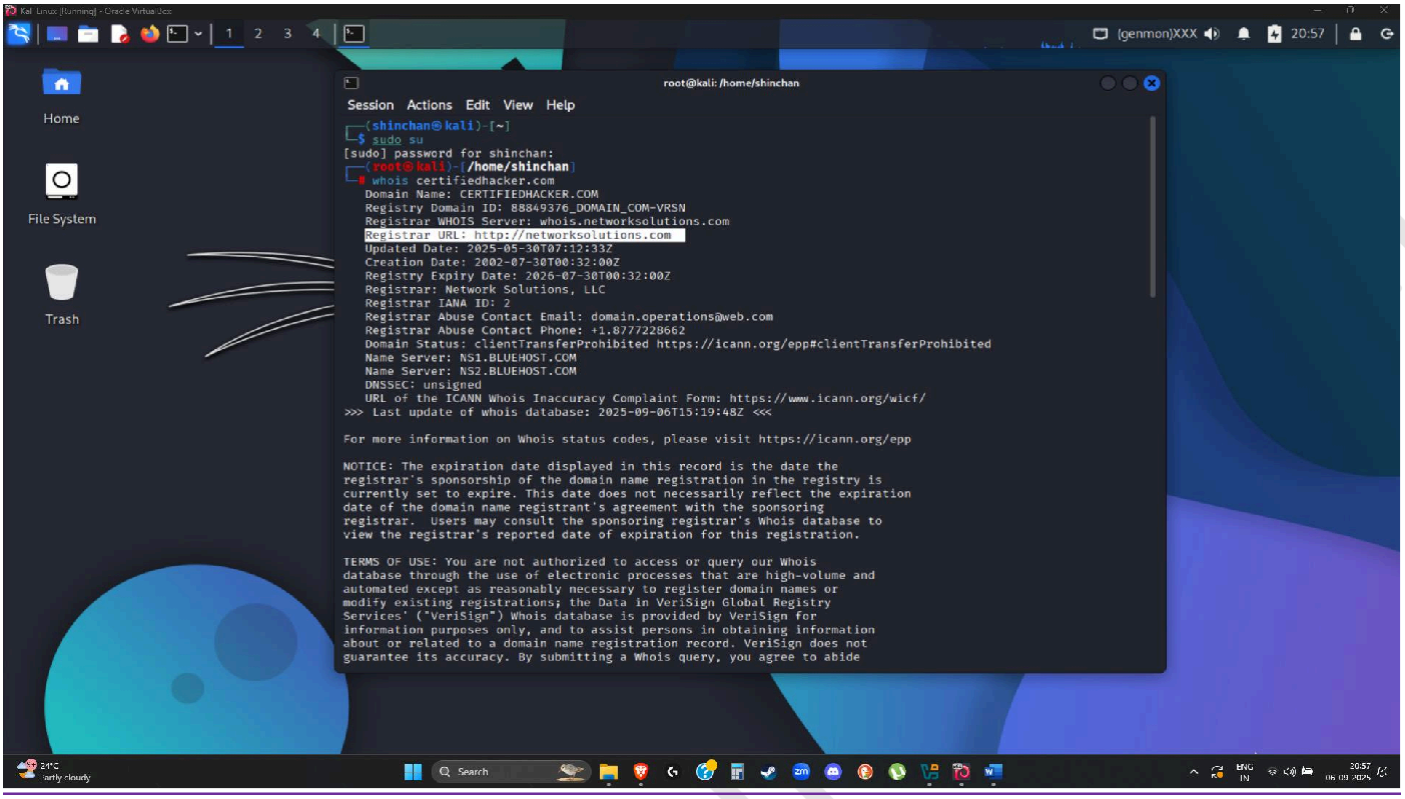
Domain Name:



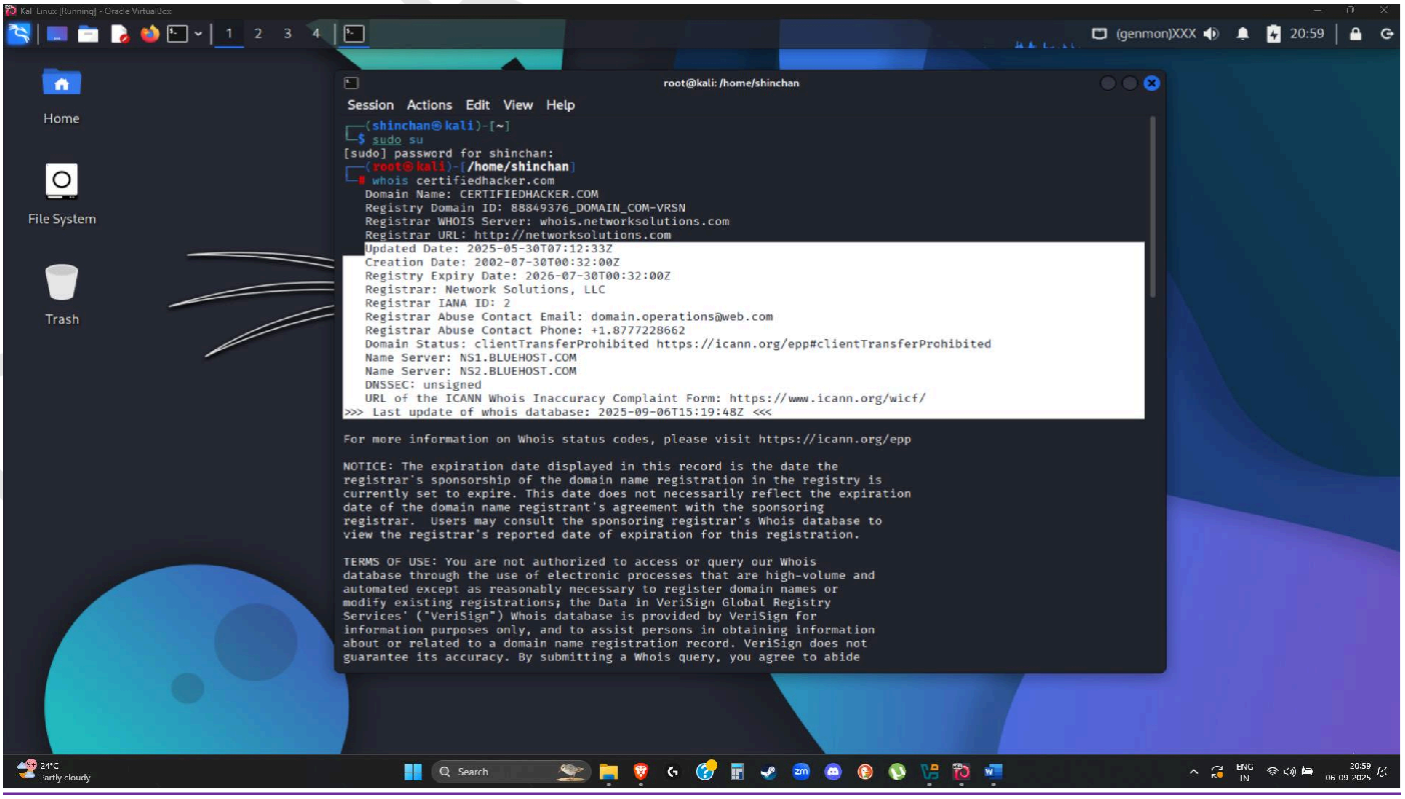
Domain ID:



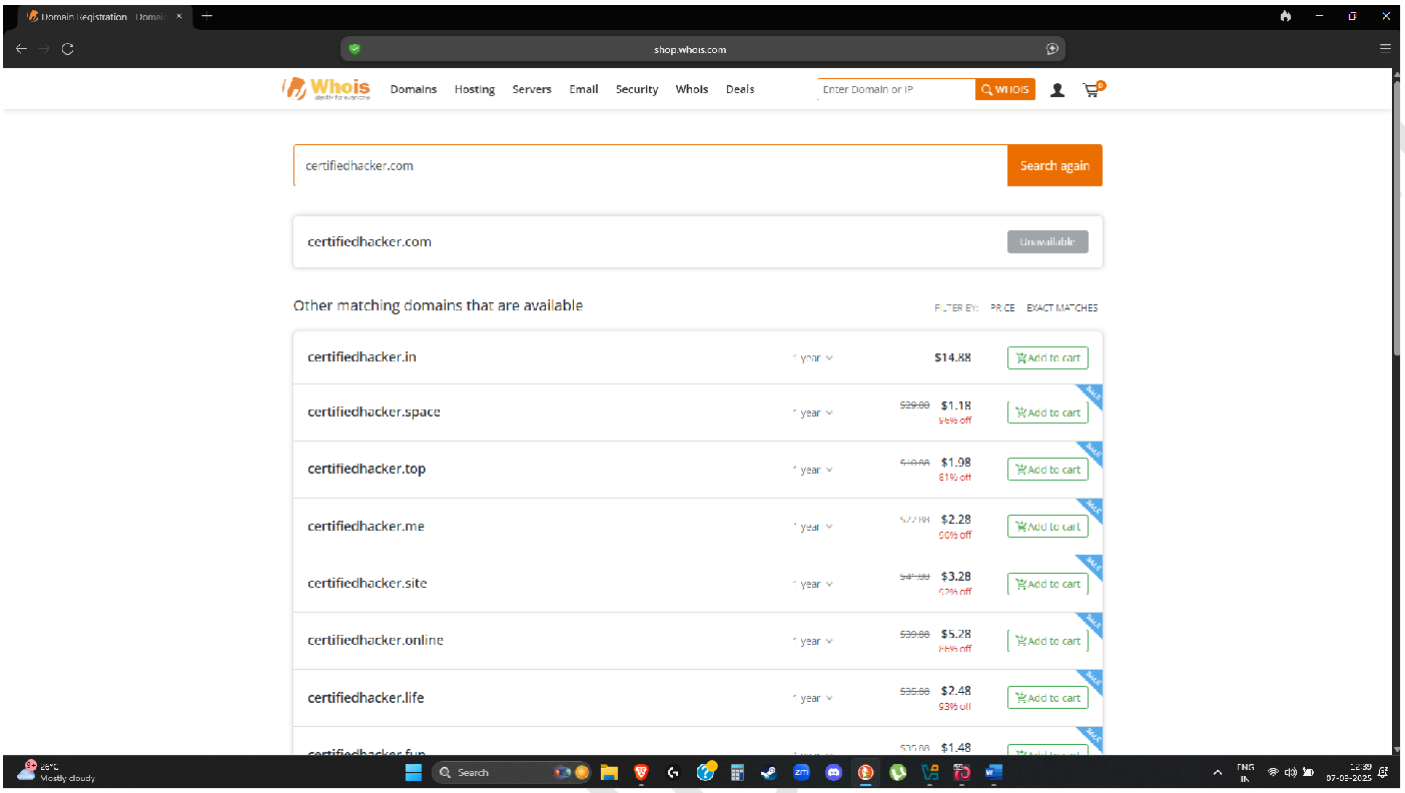
Registar URL:



Everything you want regarding it:



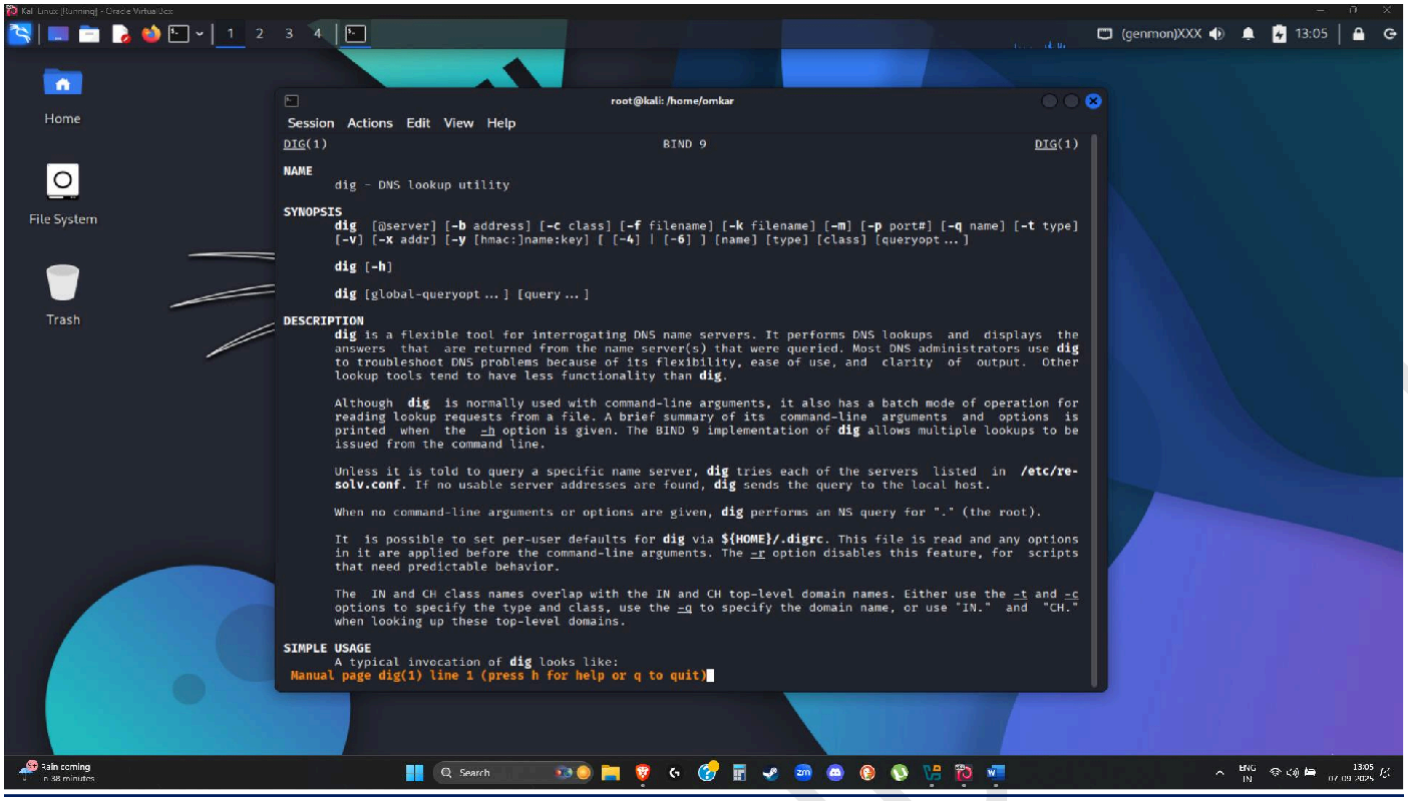
 You may use Whois Domain and search on Search Engines:



Foot-Printing by performing DNS for Hacking:

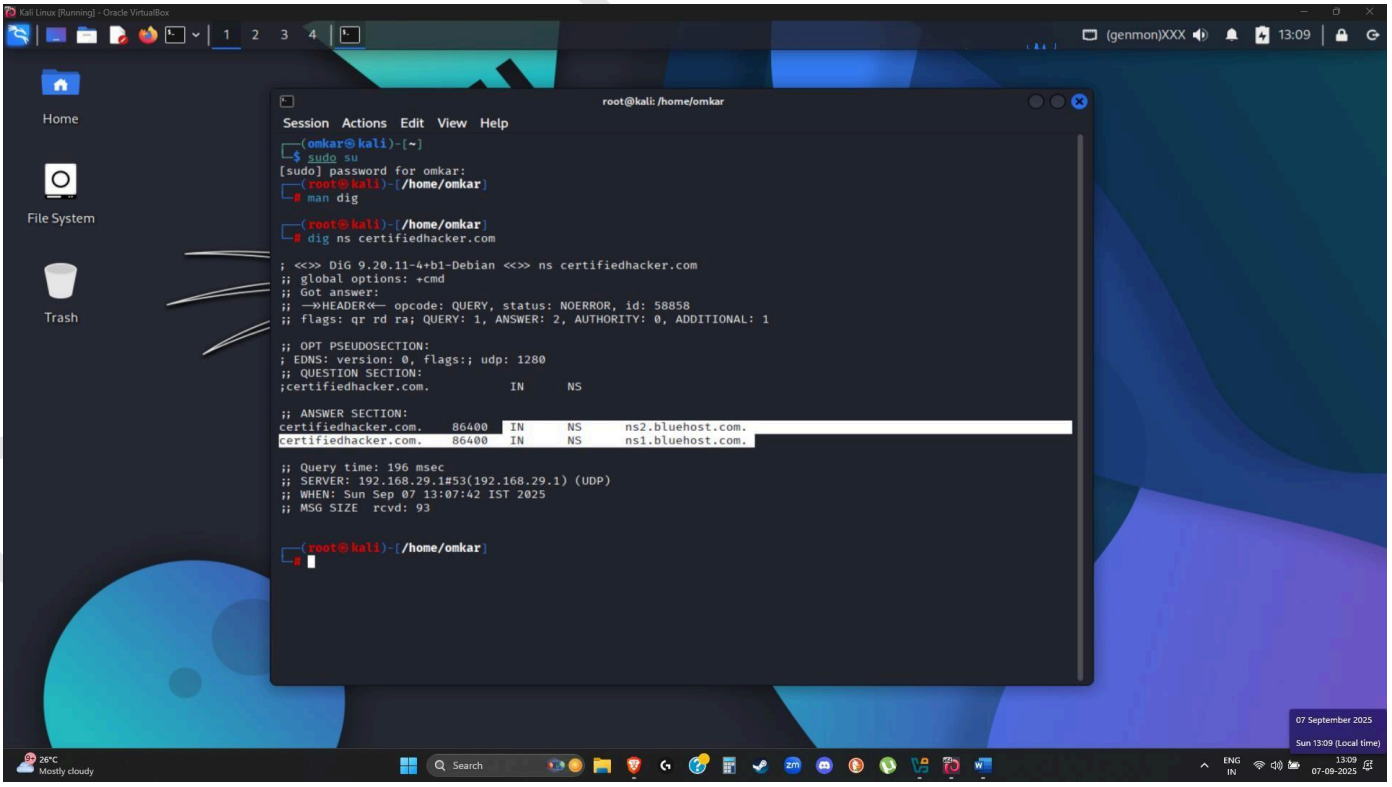
DNS or Domain name System, reveals information about DNS zone data.

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



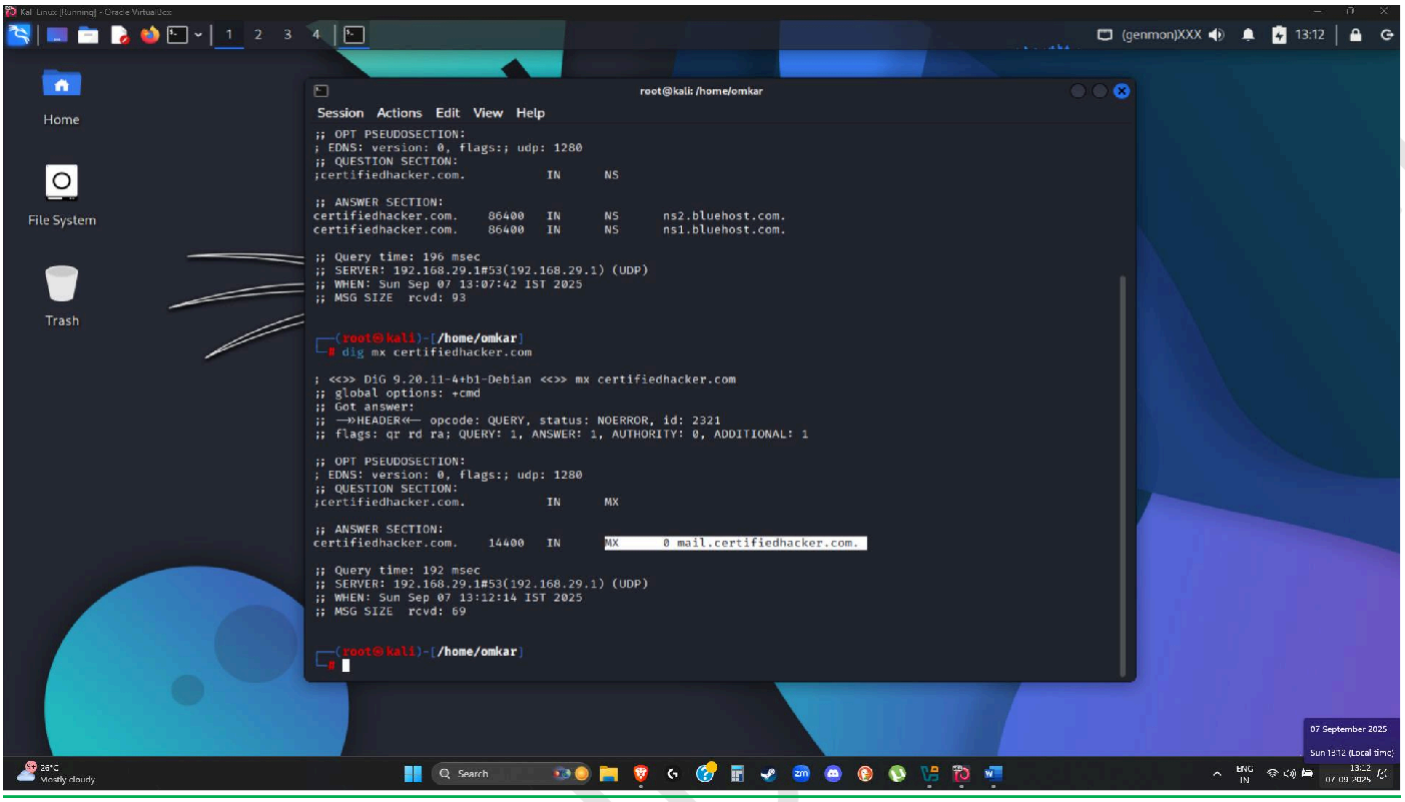
- Perform in **Kali Linux**- command *dig ns certifiedhacker.com*

We found Name Server (NS) records of domain.



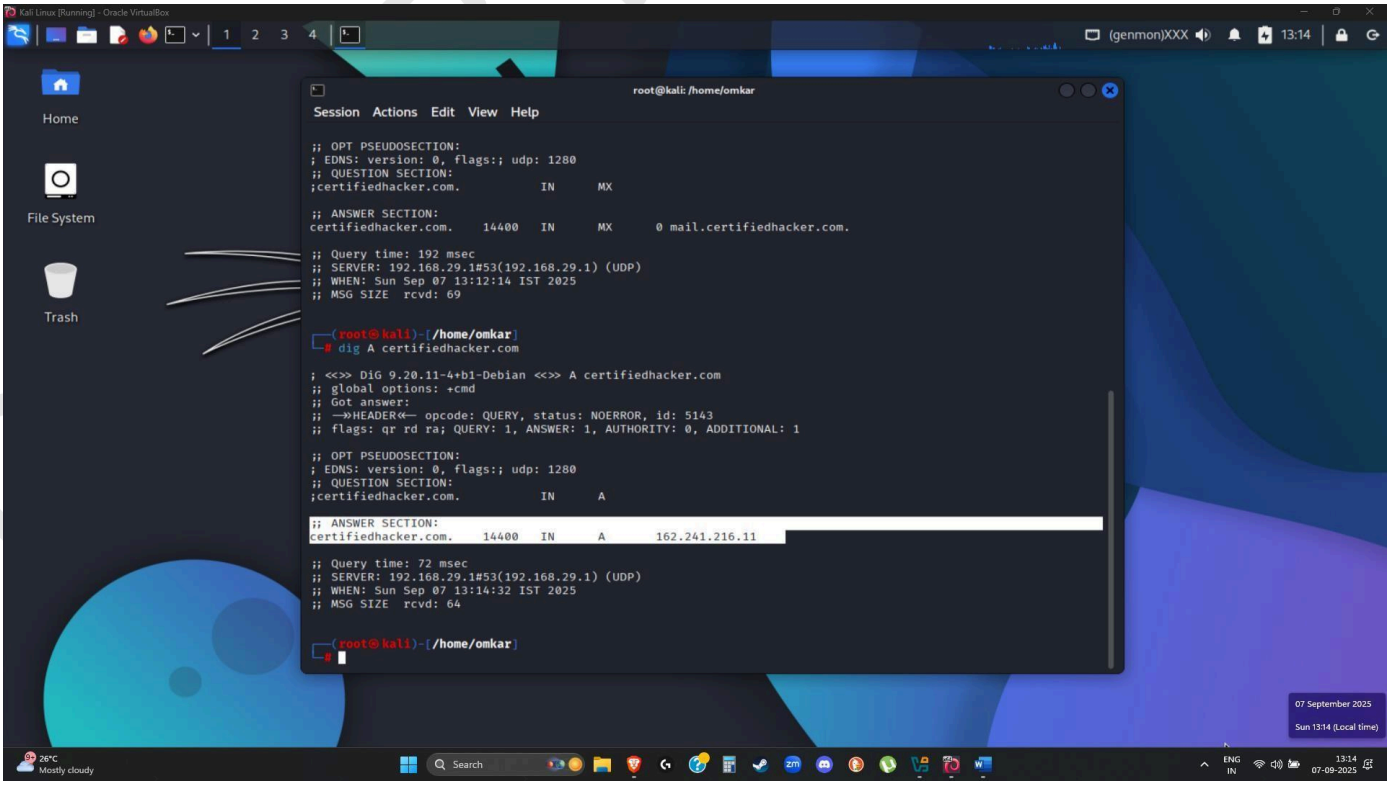
- Perform in **Kali Linux-** command *dig mx certifiedhacker.com*

  To find mx (mail)record of domain



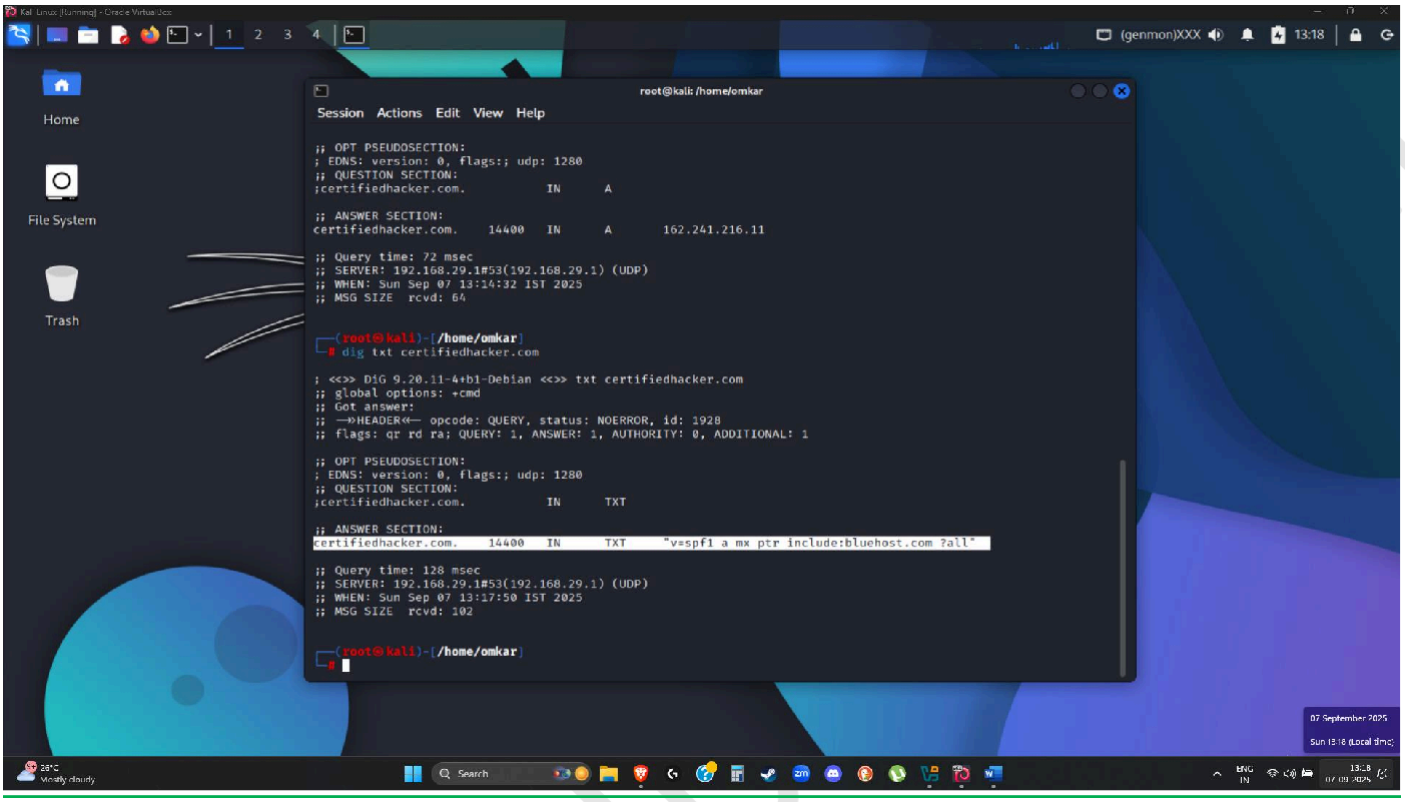
- Perform in **Kali Linux-** command *dig A certifiedhacker.com*

  To find A (means ip) record of domain



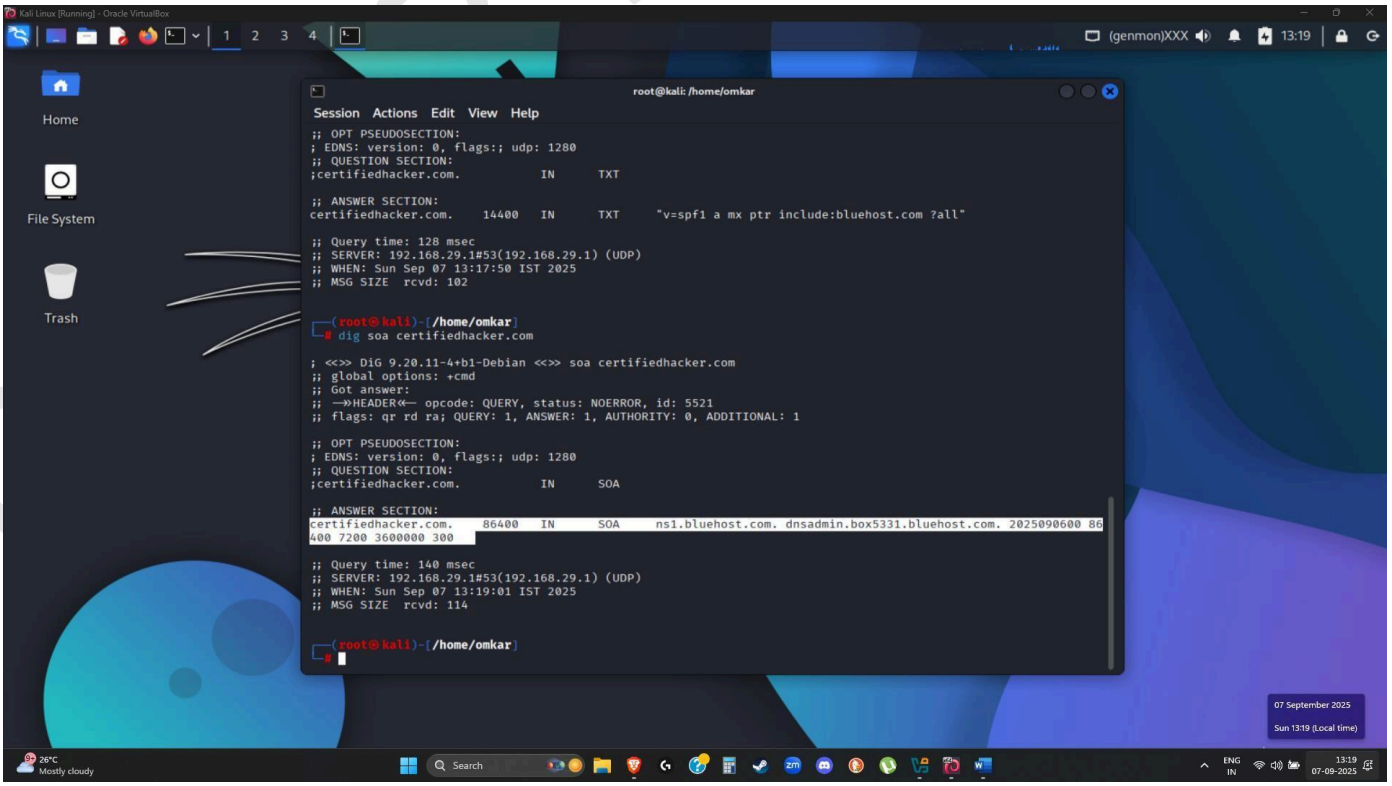
- Perform in **Kali Linux-** command *dig txt certifiedhacker.com*

  To find TXT record of domain



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

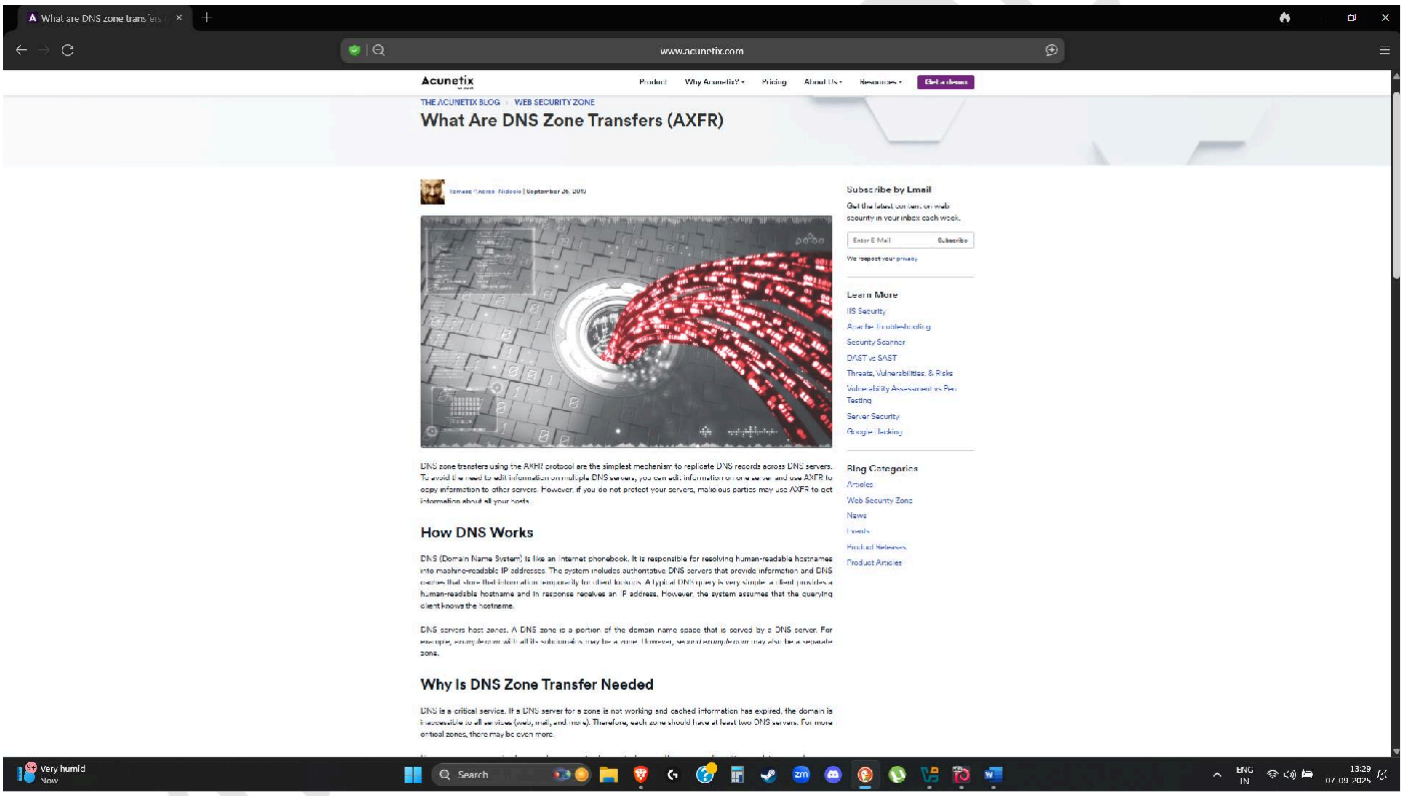
  To find SOA record of domain



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

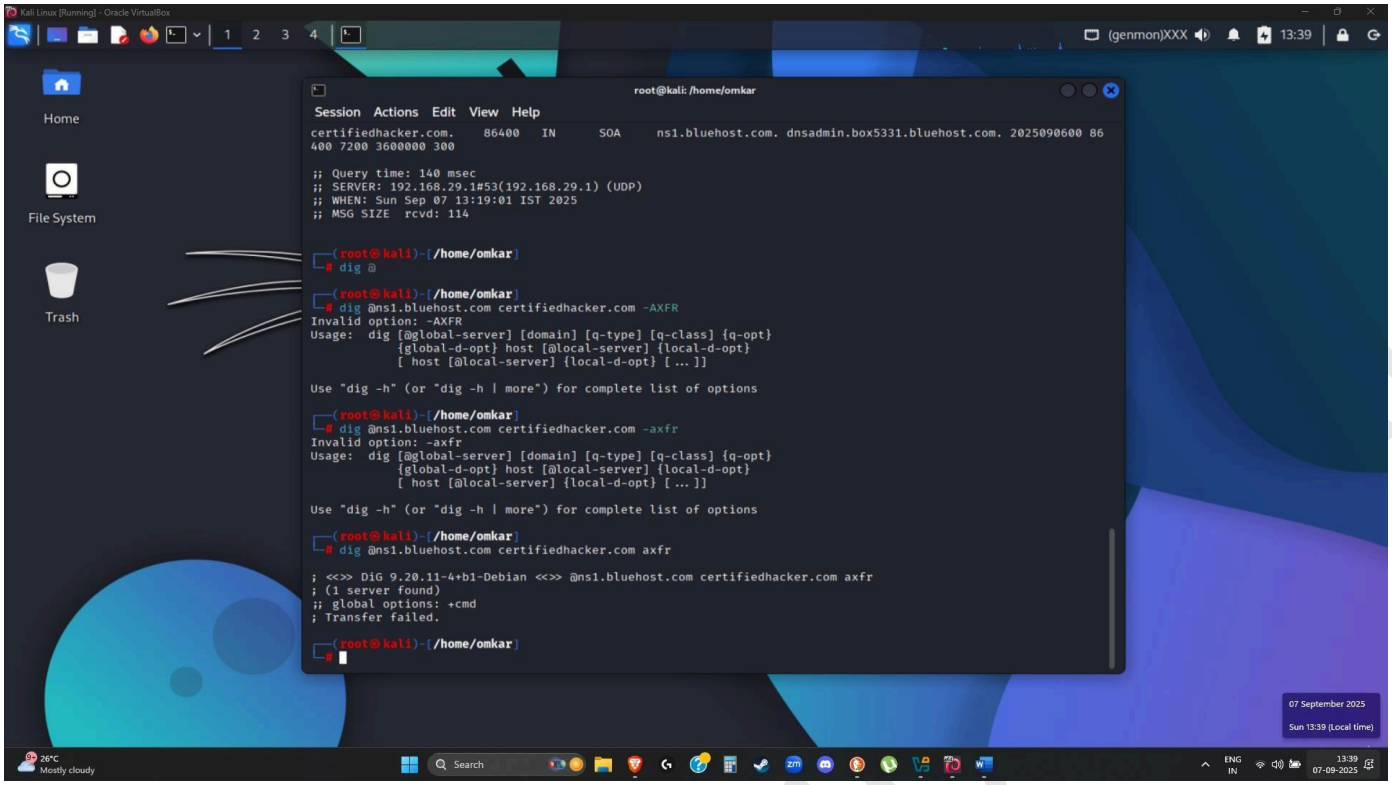
Performing it and creating its Replica (Clone), so that the system which provides information and DNS caches that will store that information for client lookups.

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.



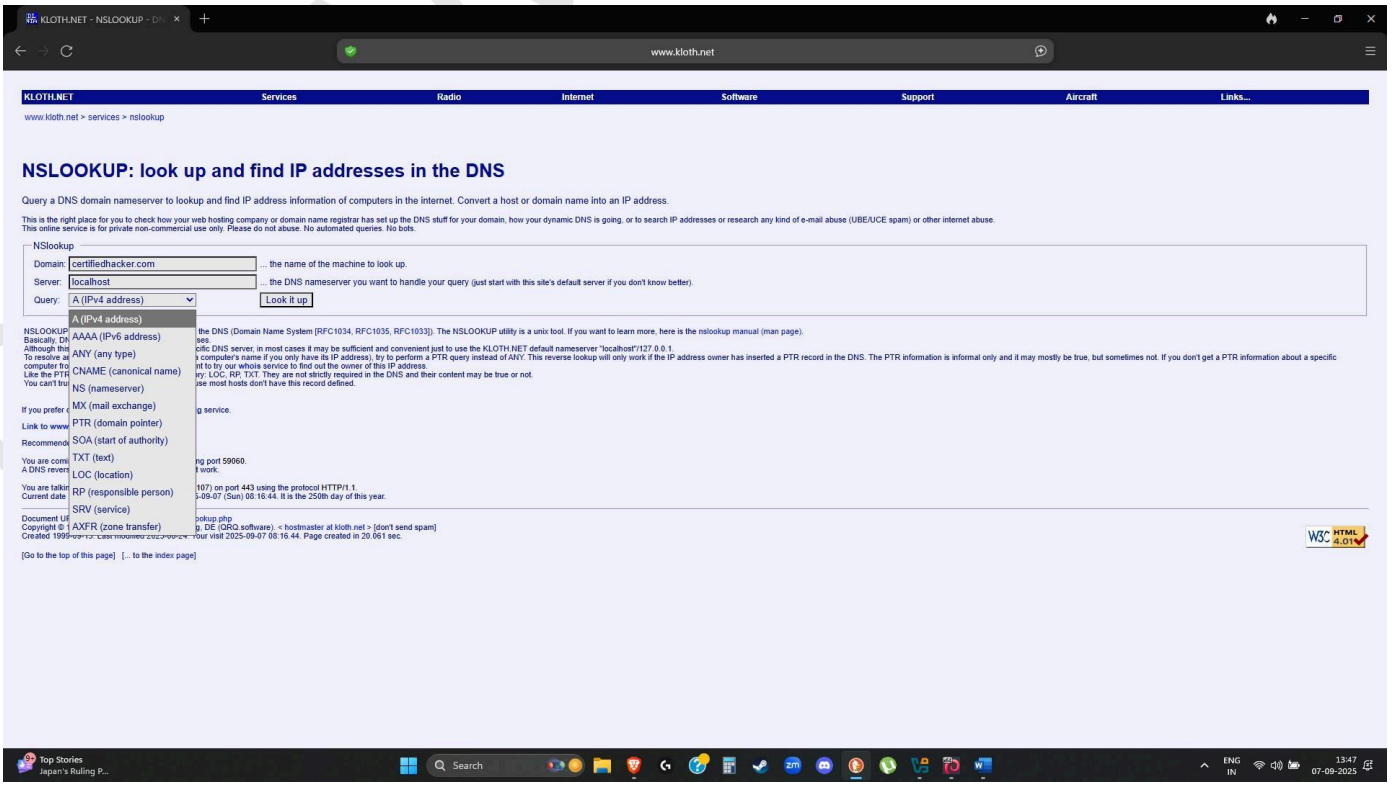
- Now Perform in **Kali Linux**- command *dig @ns1.bluehost.com certifiedhacker.com axfr*

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



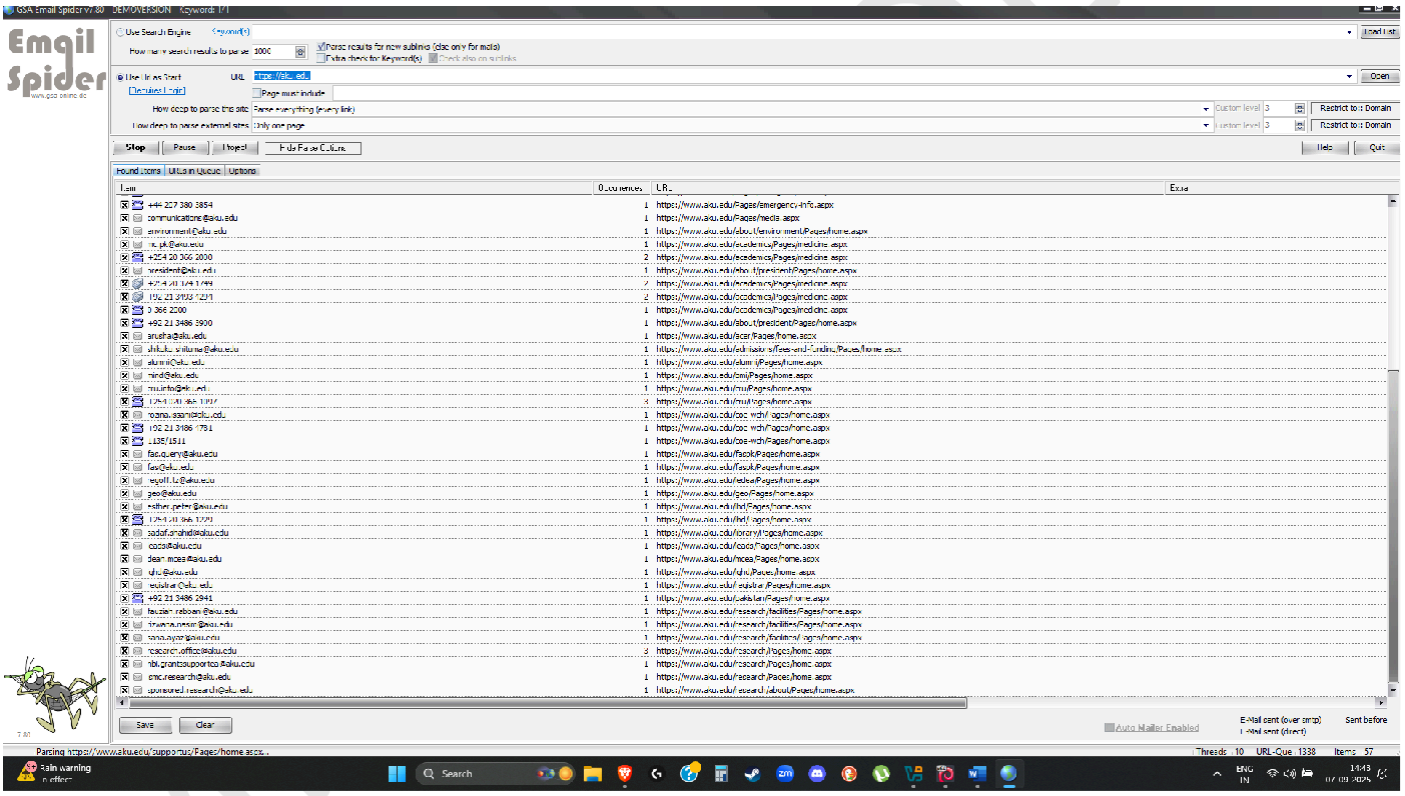
- You may use Kloth DNS and search on Search Engines to understand:

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



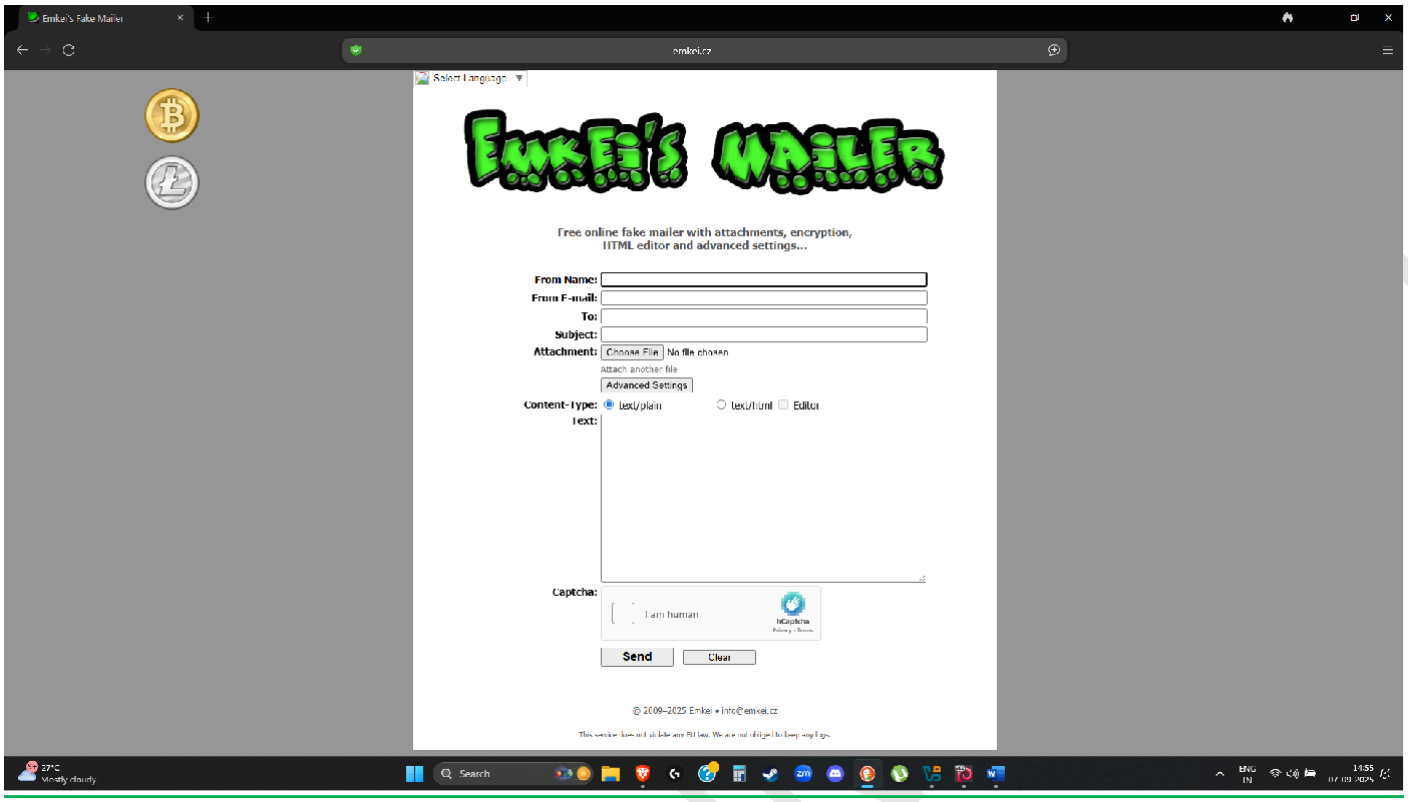
Performing E-mail Foot-Printing for Hacking:

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



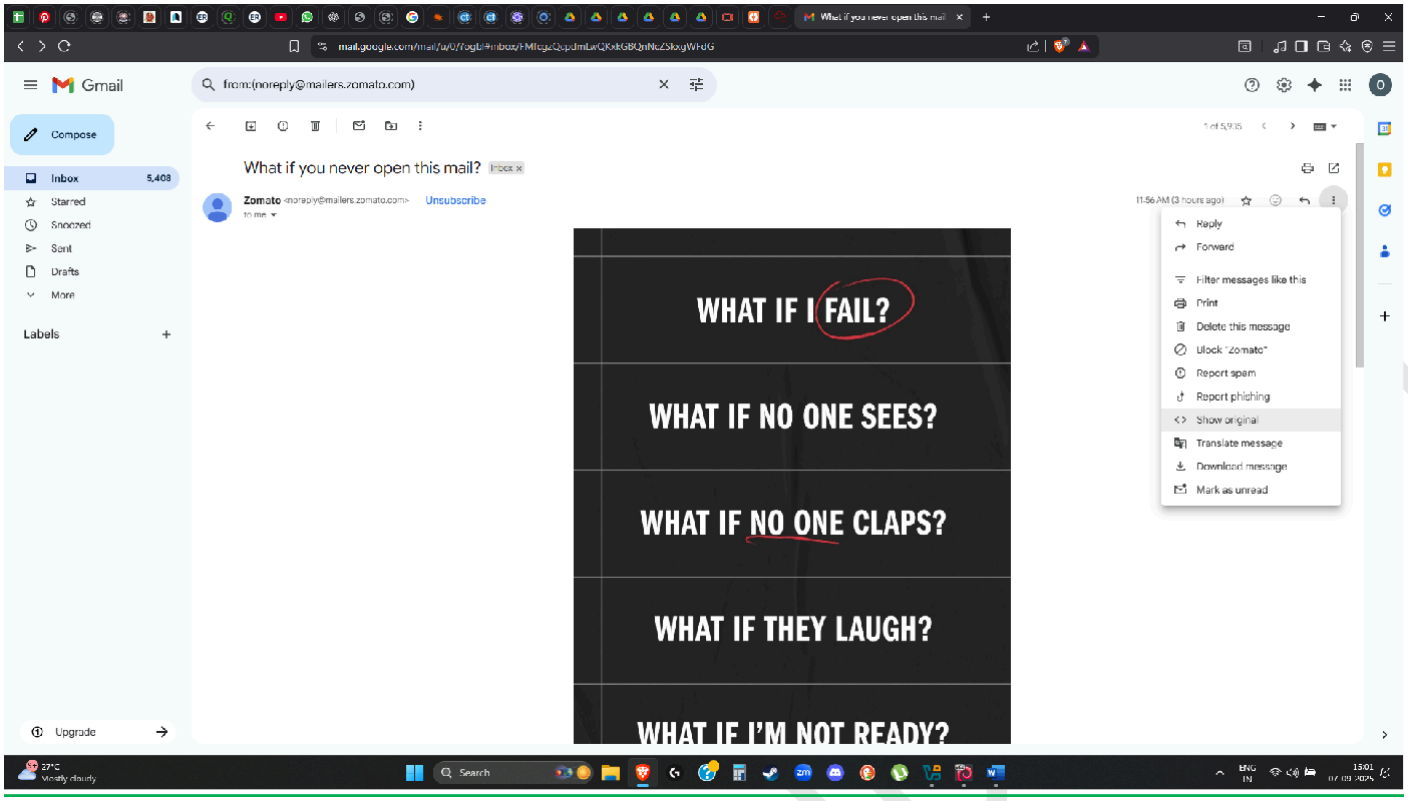
- Now how fake E-mails are done through where, So to understand:

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

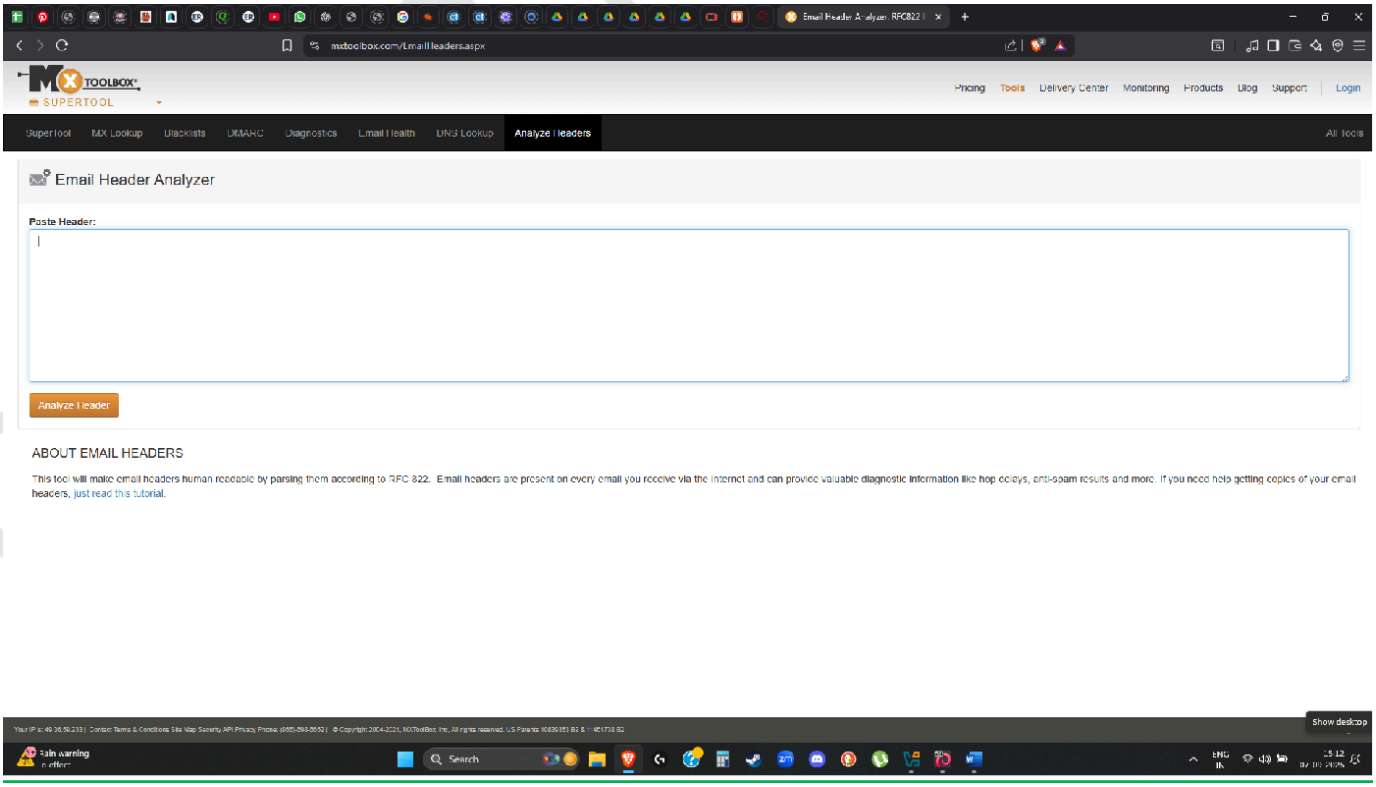


Now how to know fake E-mails, So to avoid it:

- 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.



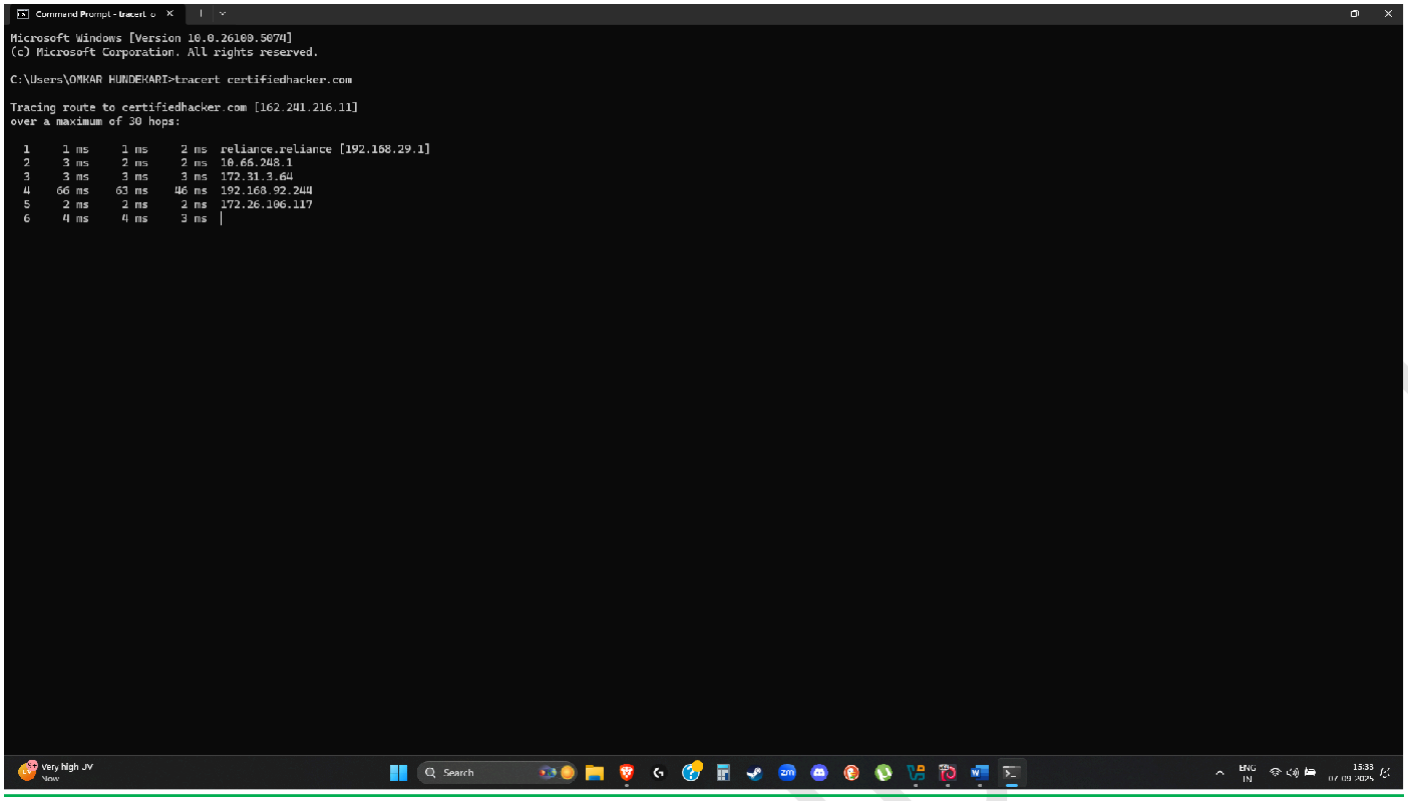
- Perform Network Trace Routing in Windows

  Network Foot-Printing is the process of gathering information of target organization.
- Example- **Ip address, Host name, Domain, Sub-Domains.**

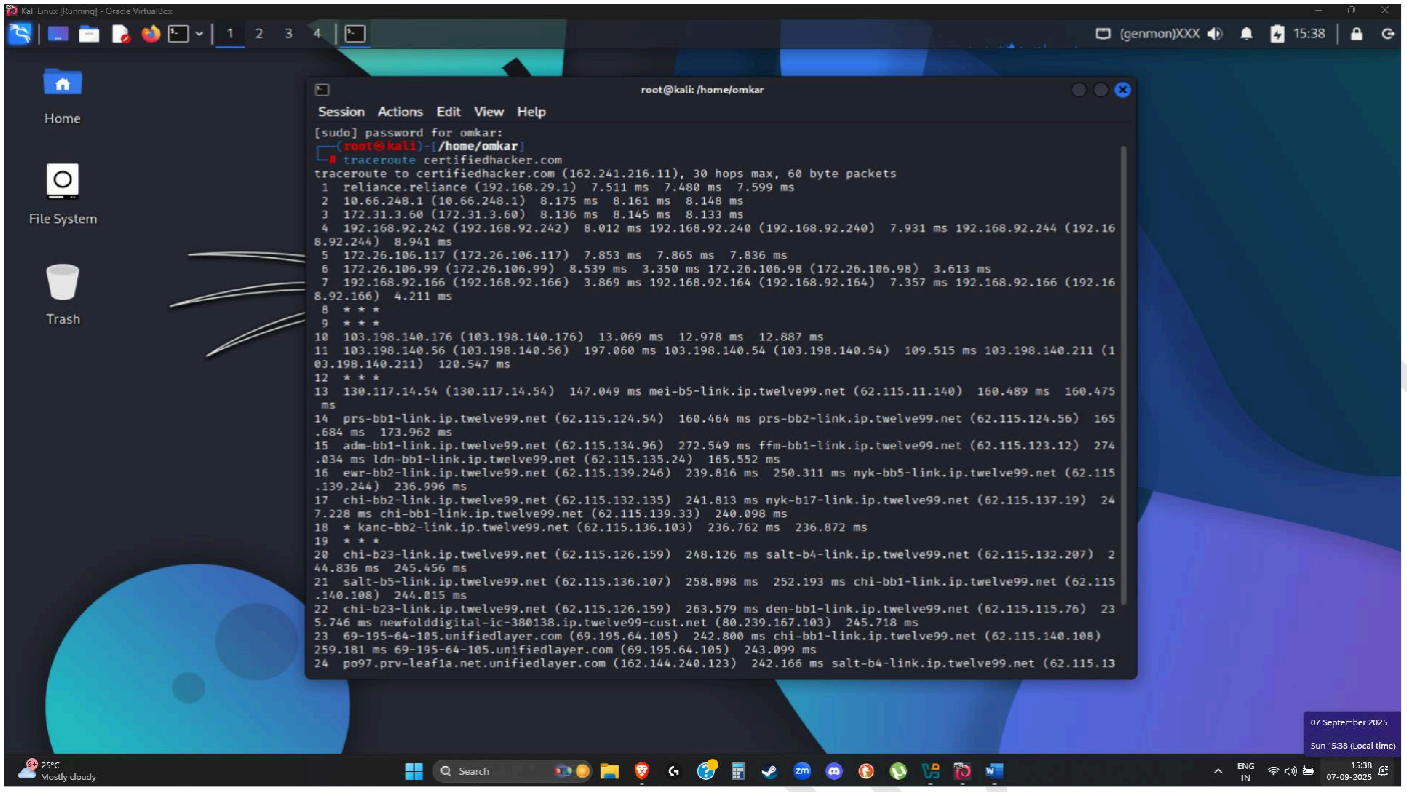
- In this we can also check from our network, to whom we are Targeting.
- Also we can check between our Network and our Target, How many Hops and Routers are connected.

- 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.

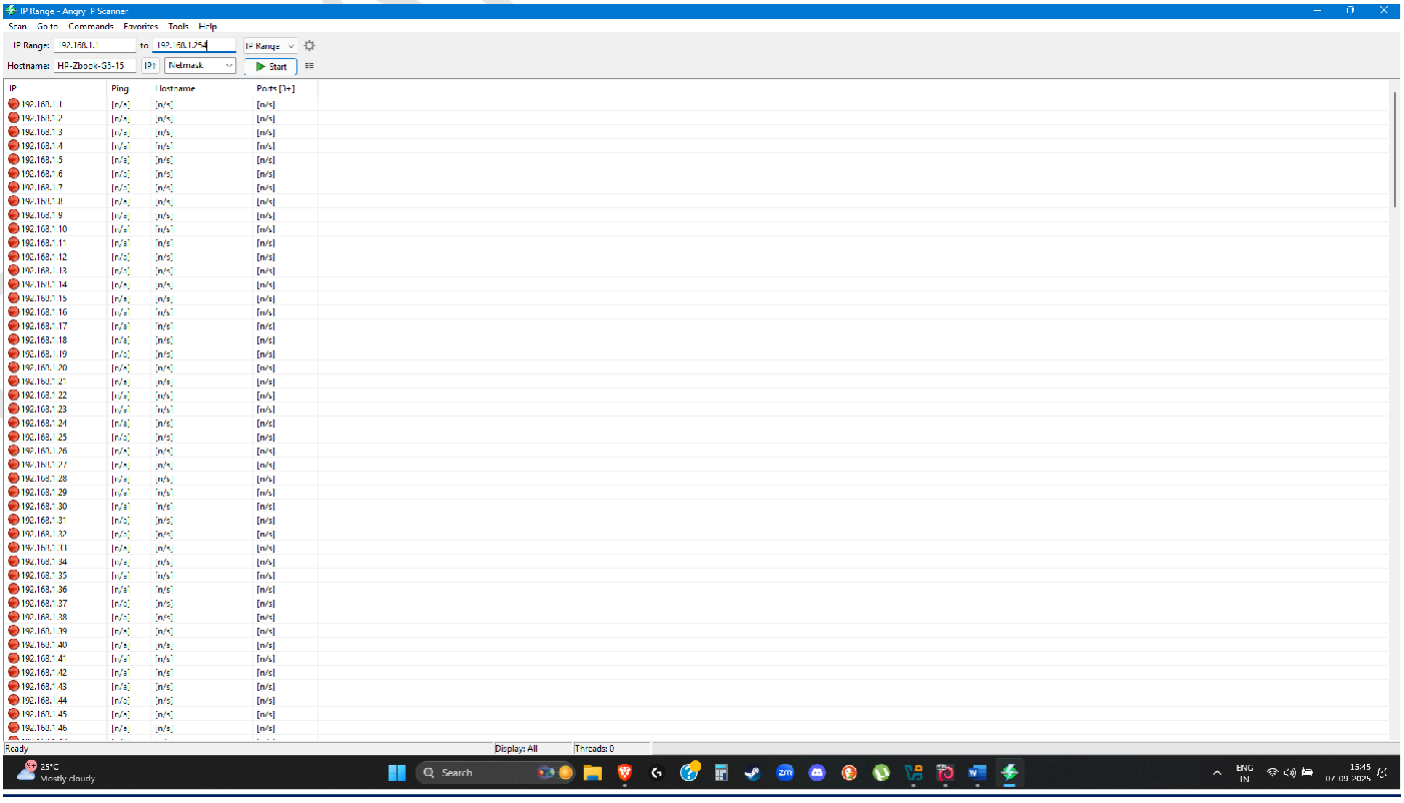


- In [Kali Linux.]
- Example- OpenTerminal.
- Type traceroute (any Domain) certifiedhacker.com.
- It will Trace route, showing System Gateway and till last how many hops and ip's are connected to certifiedhacker.



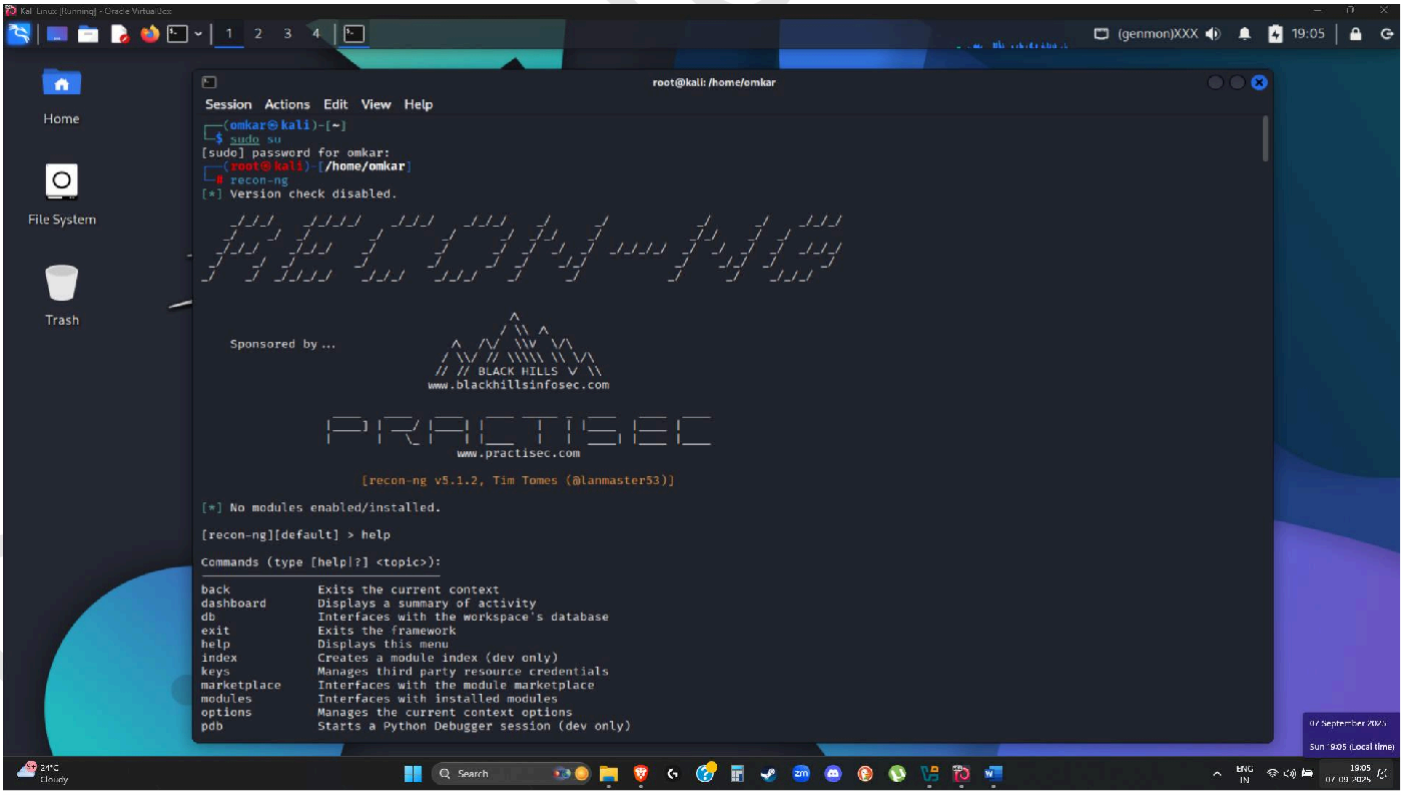
- Tool to find how many Systems are there in Network:

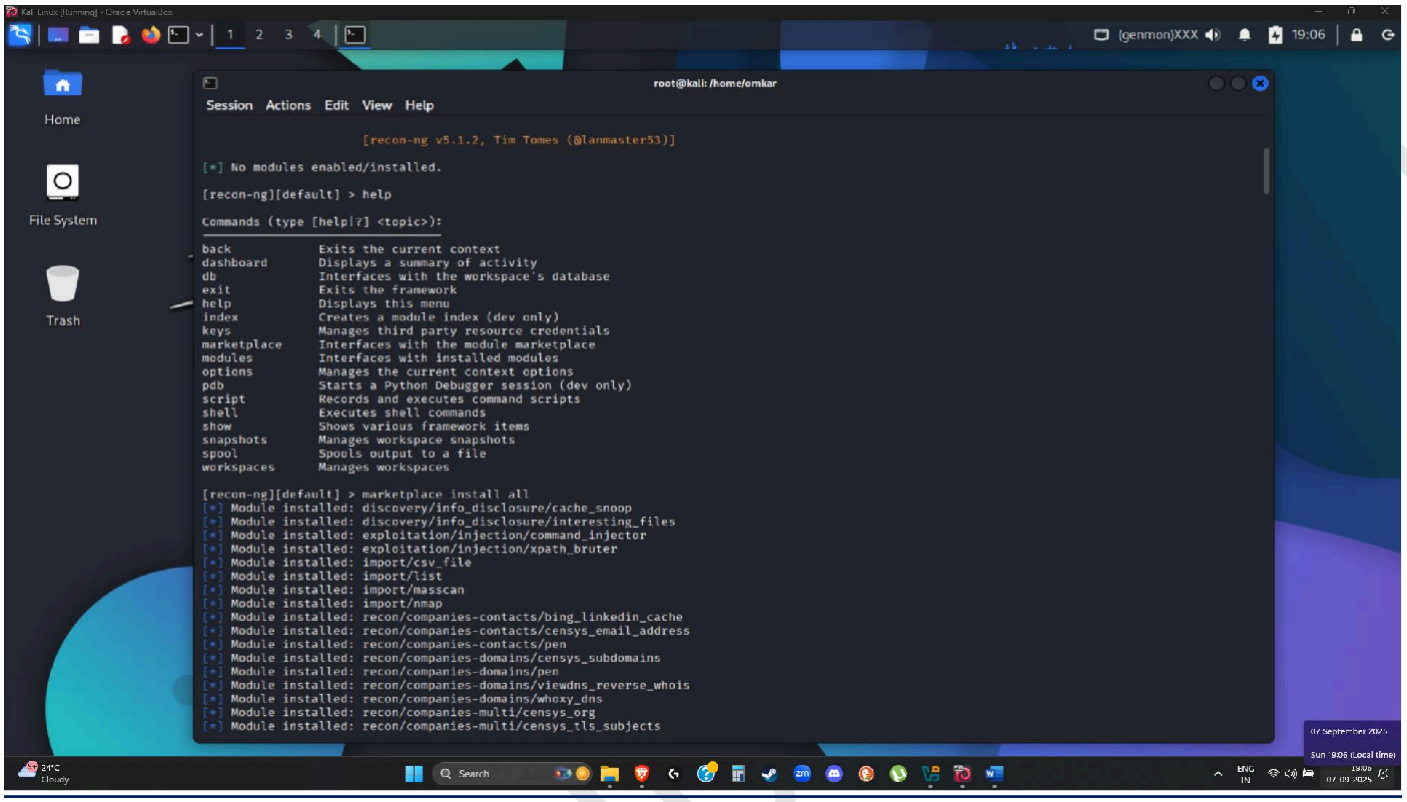
- Tool is Angry IP Scanner:

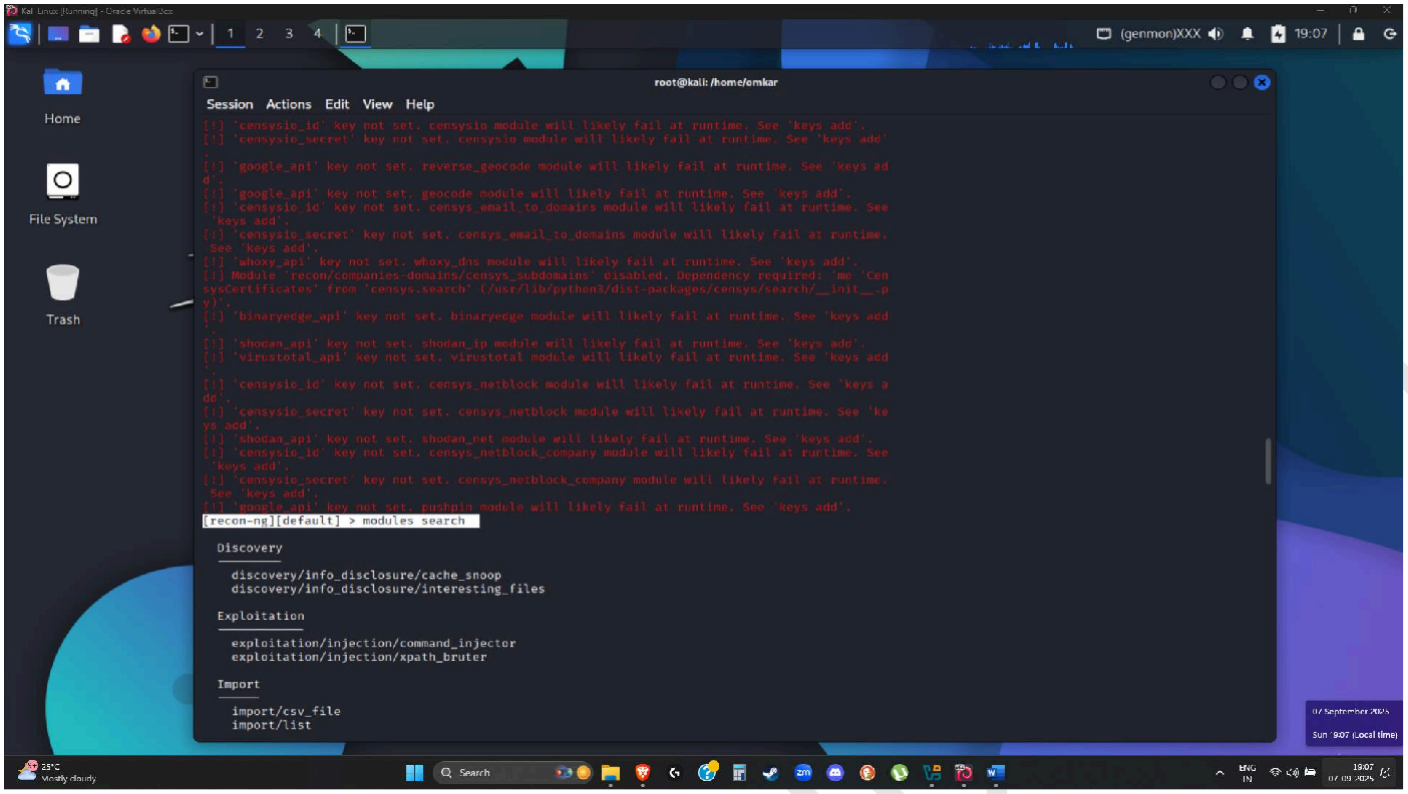


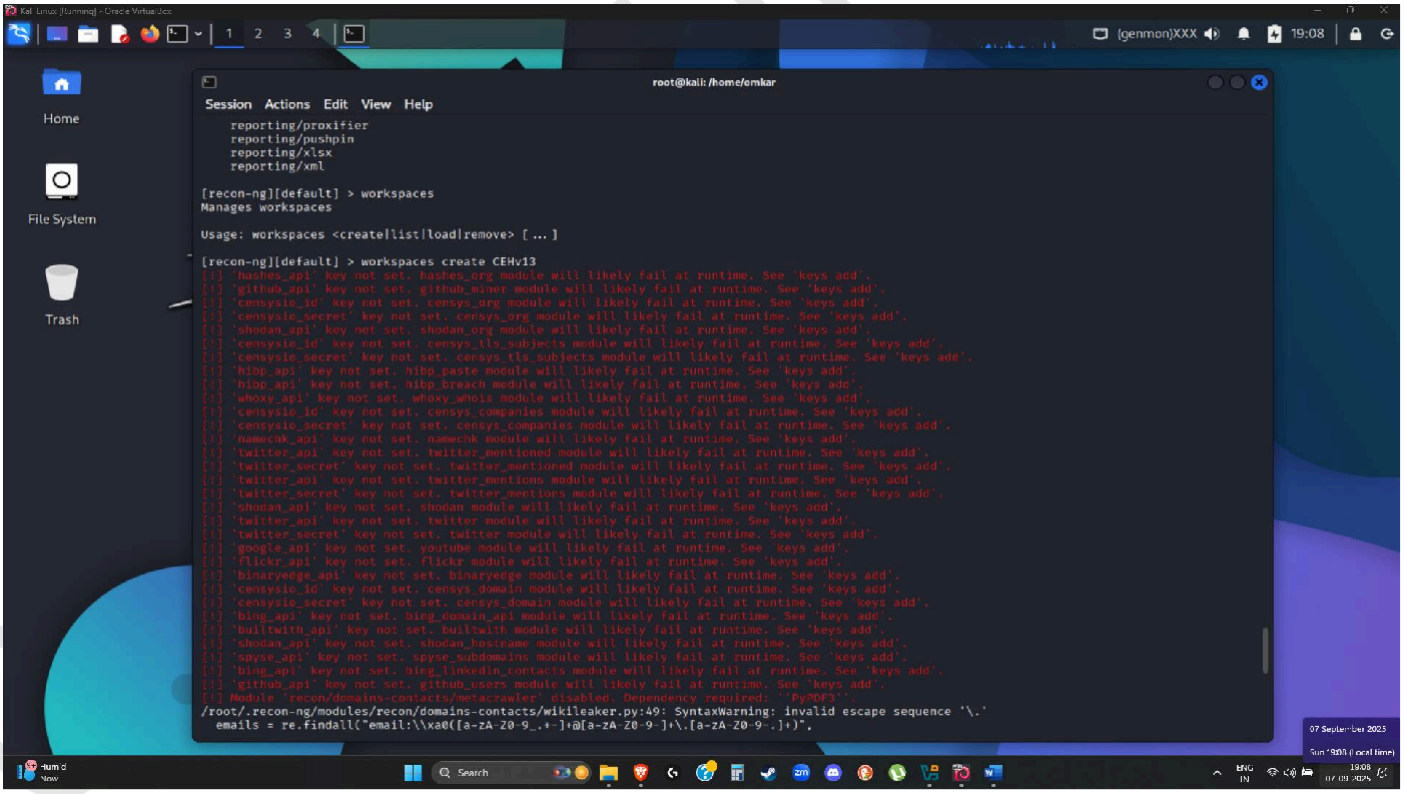
Performing Reconnaissance Kali Linux:

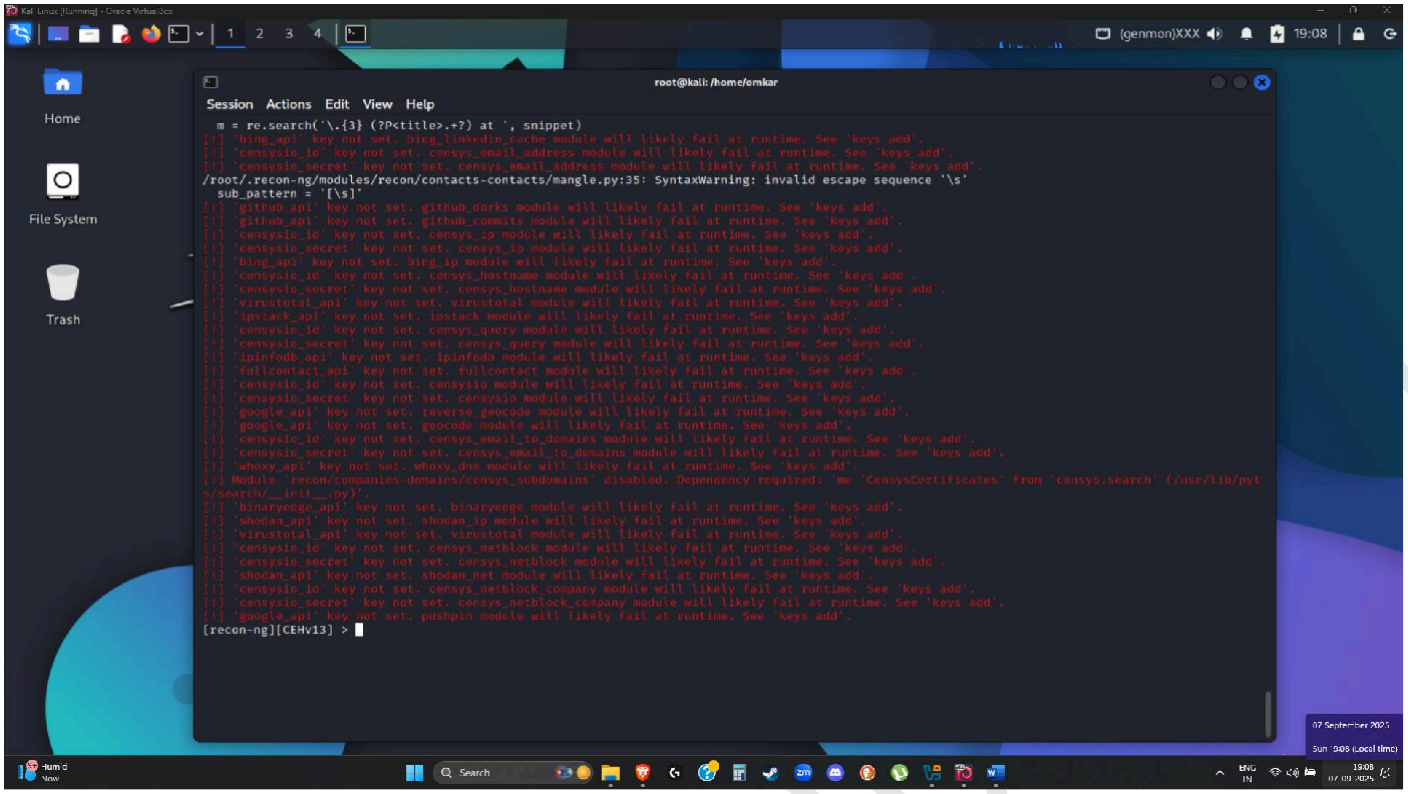
- This recon-ng Tool in **Kali Linux** is used to gather information.
- It will show no content.
- Type next command help.
- And at last type command- marketplace install all.
- It will start installing.
- After installing, to check everything installed, command- modules search
- Now you can create your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

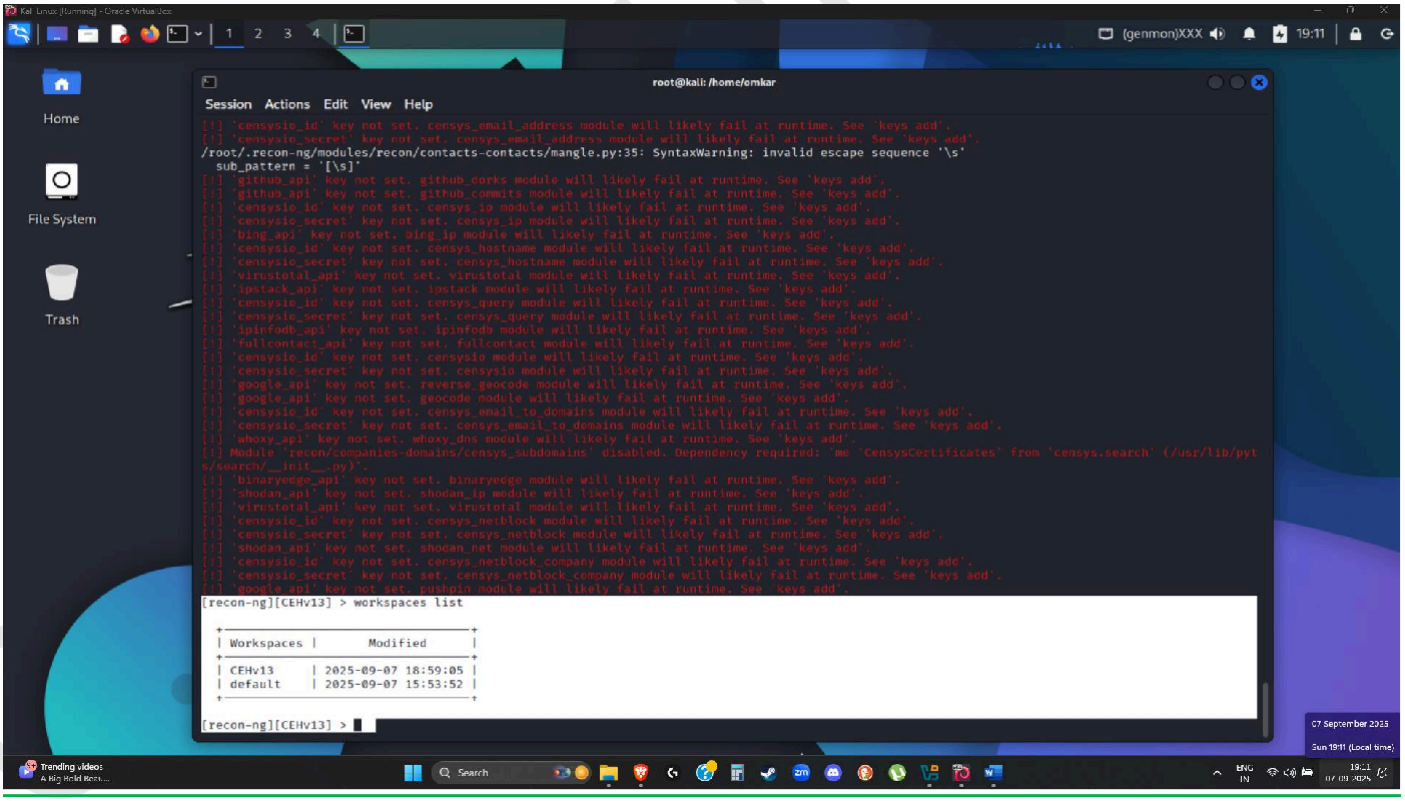



root@kali: /home/emkar
Session Actions Edit View Help
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installed.
[recon-ng][default] > help
Commands (type [help|?] <topic>):
back Exits the current context
dashboard Displays a summary of activity
db Interfaces with the workspace's database
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: import/nmap
[*] 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/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-multi/censys_org
[*] Module installed: recon/companies-multi/censys_tls_subjects
Home
File System
Trash
Search

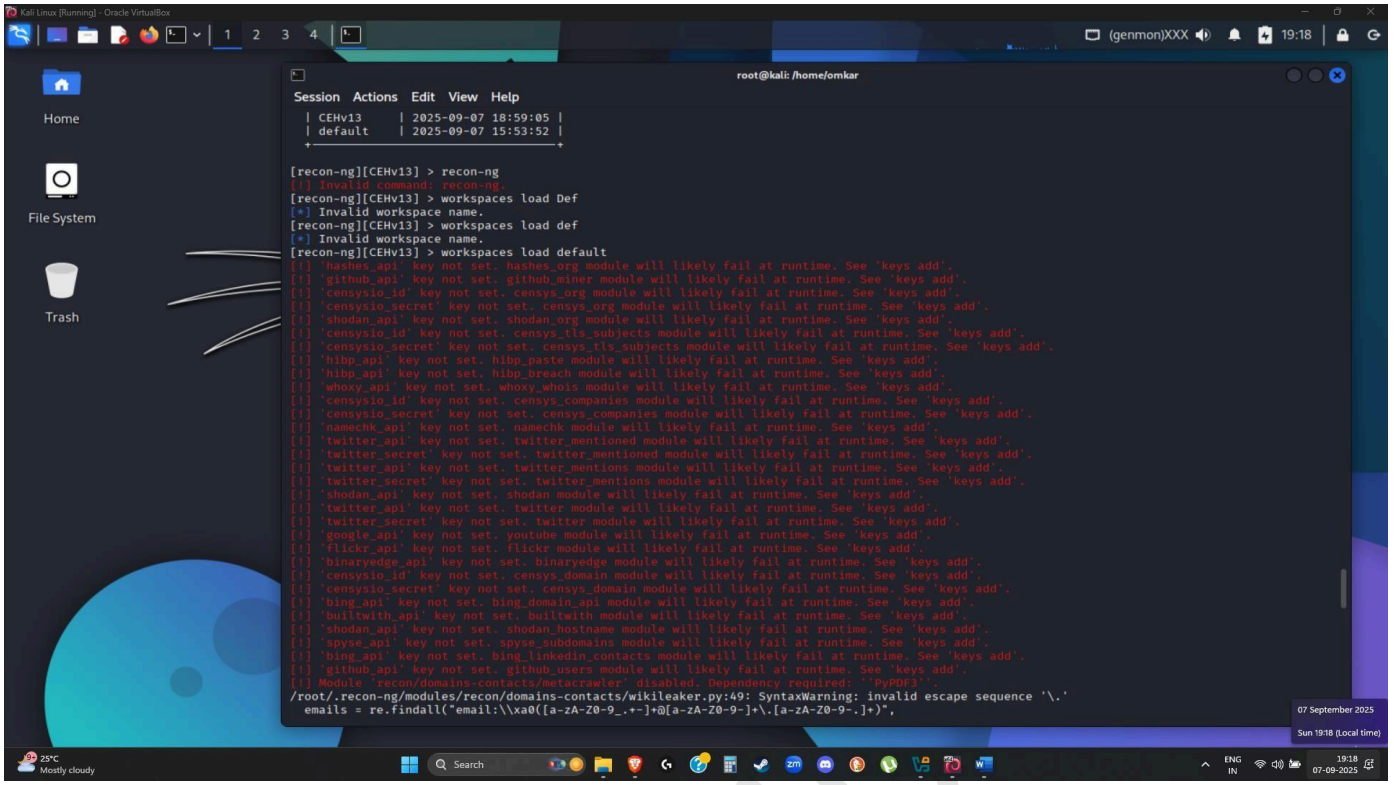

root@kali: /home/emkar
Session Actions Edit View Help
[!] 'censysio_id' key not set. censysio module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censysio module will likely fail at runtime. See 'keys add'
[!] 'google_api' key not set. reverse_geocode module will likely fail at runtime. See 'keys add'.
[!] 'google_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'.
[!] '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'.
[!] 'google_api' key not set. pushpin 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
Home
File System
Trash
(genmon)XXX
19:07
07 September 2025
Sun 19:07 (Local time)


root@kali: /home/emkar
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
[!] 'hashes_api' key not set. hashes_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_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'.
[!] 'hibp_api' key not set. hibp_paste module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_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_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'.
[!] 'spyse_api' key not set. spyse_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-ng/modules/recon/domains-contacts/wikileaker.py:49: SyntaxWarning: invalid escape sequence '\.'
emails = re.findall("email:\\xa0([a-zA-Z0-9_.+-]+@[a-zA-Z0-9-]+\.[a-zA-Z0-9-.]+)",
Home
File System
Trash
(genmon)XXX
19:08
07 September 2025
Sun 19:08 (Local time)

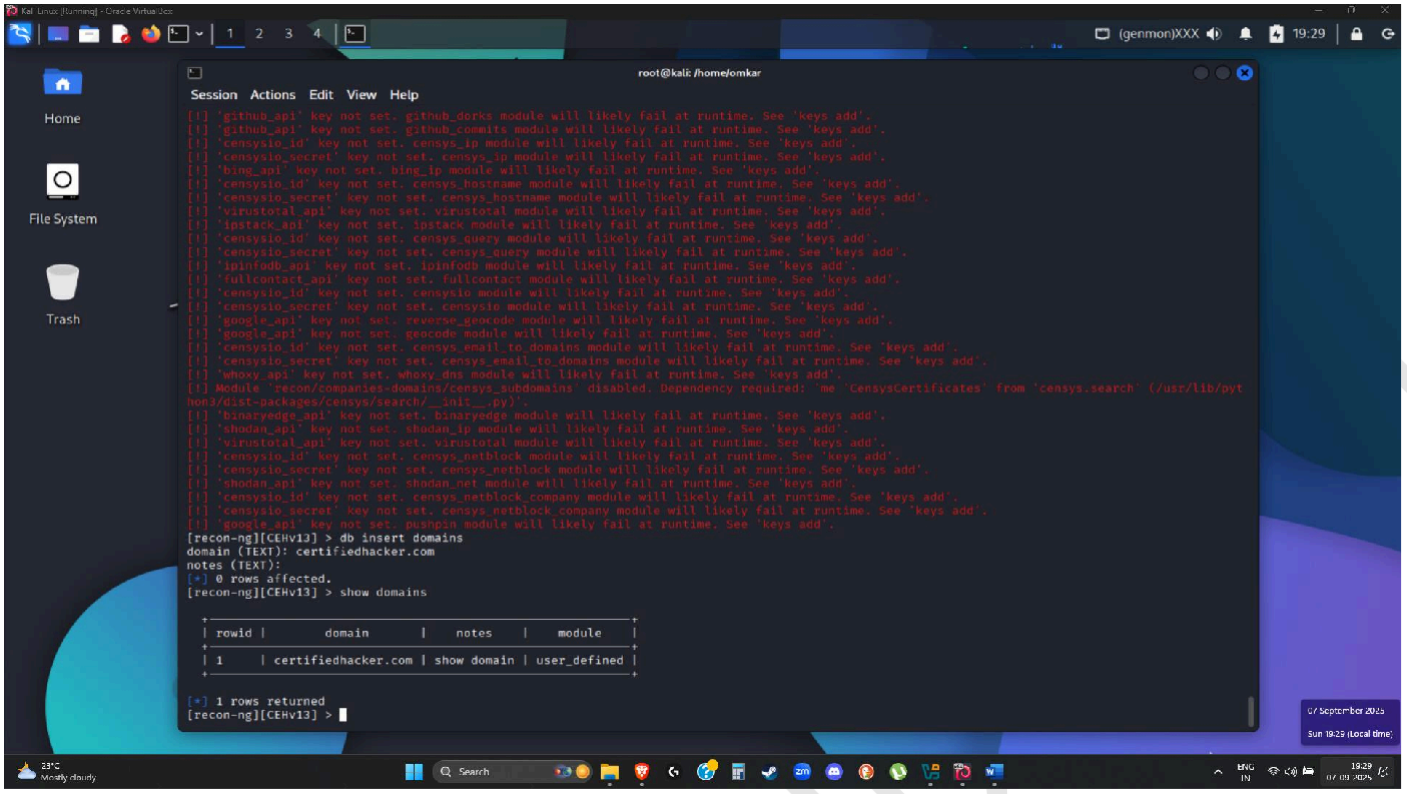




- Now you can change your workspace from created to default and default to created by command- workspaces load default or workspaces load CEHv13.



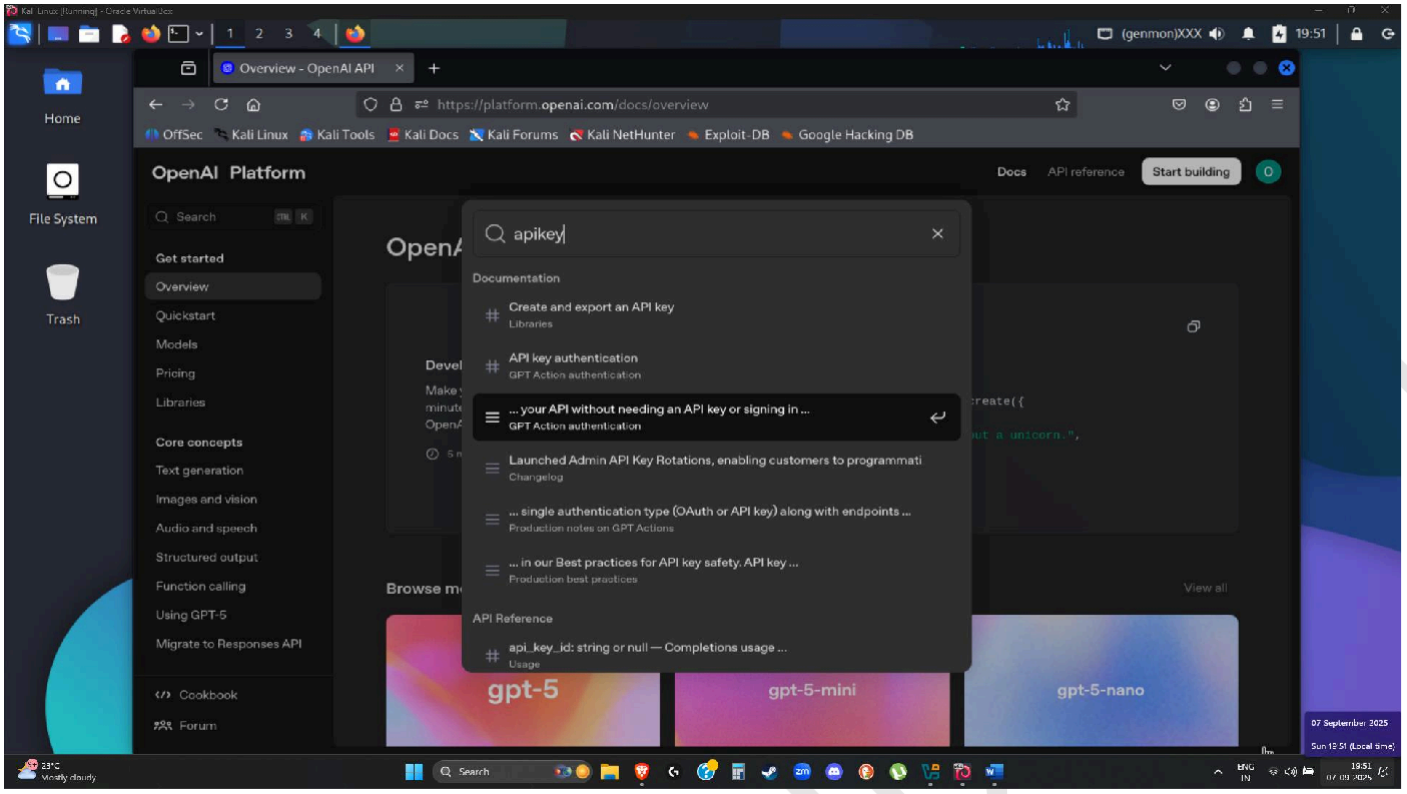
- Now performing Reconnaissance, command- db insert domains
- Now type text (domain)- certifiedhacker.com
- New command- show domain
- So we can see certifiedhacker.com domain is created.



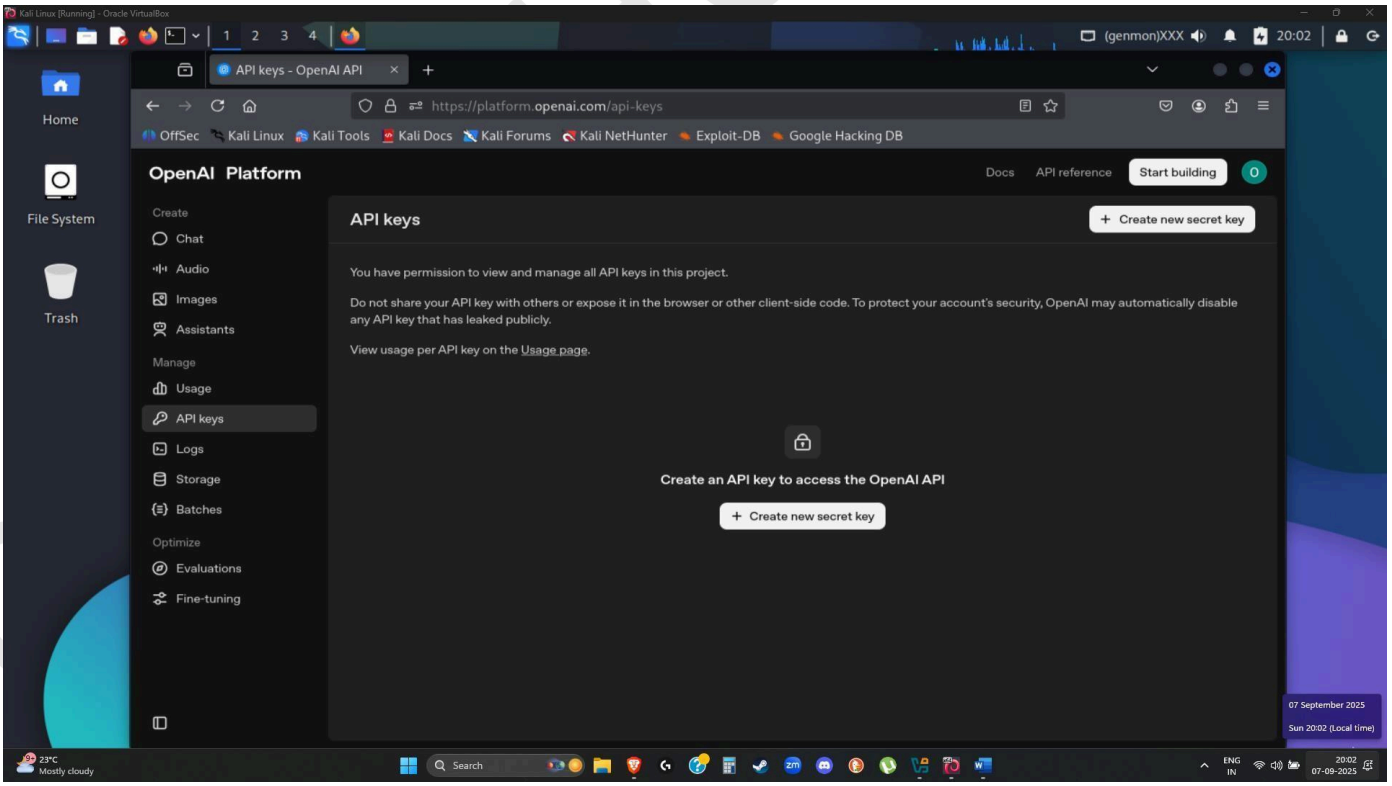
- So we can see, there are so many modules we can use to gather information.

Performing Foot-Printing using AI:

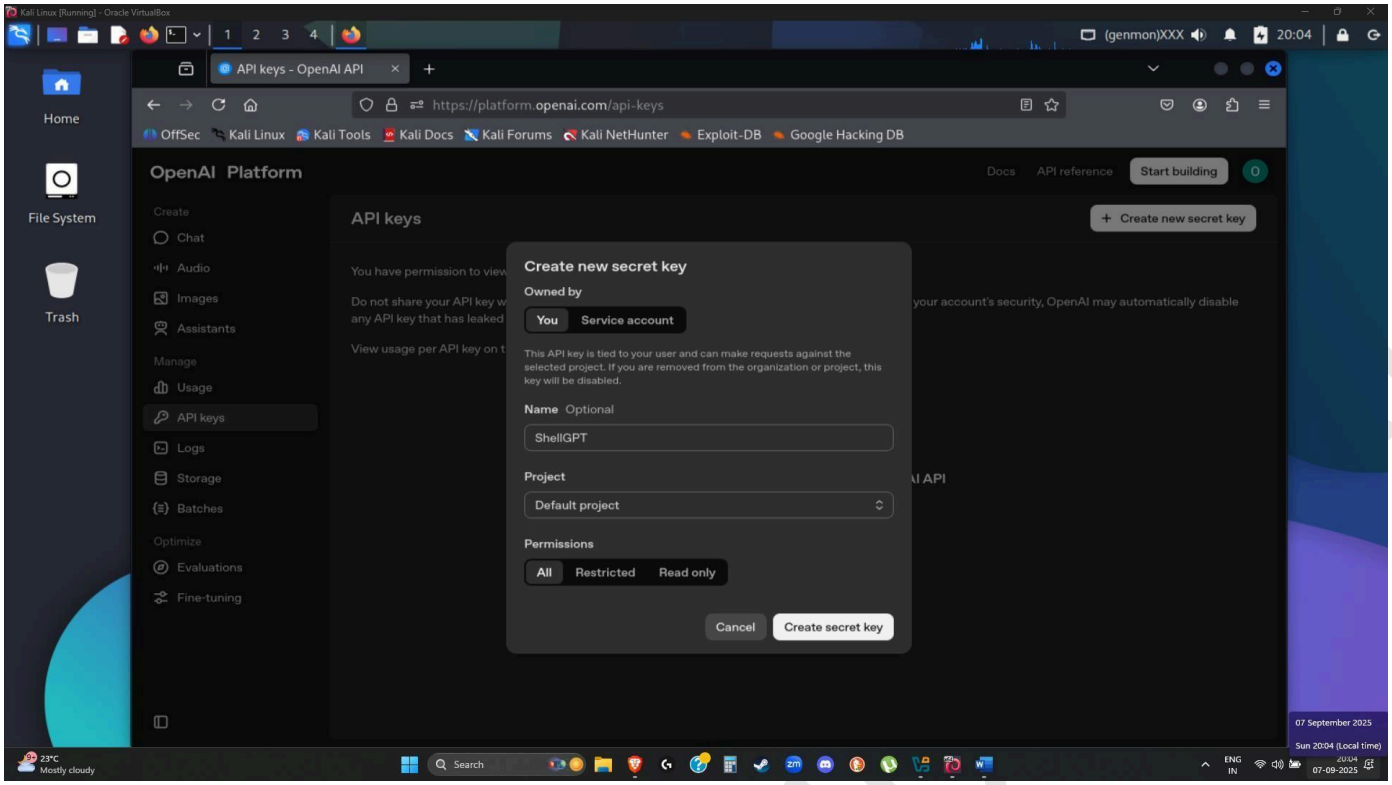
- First open Google in Kali Linux
- Search Platform openai
- Login in **openai** and perform
- Search apikey



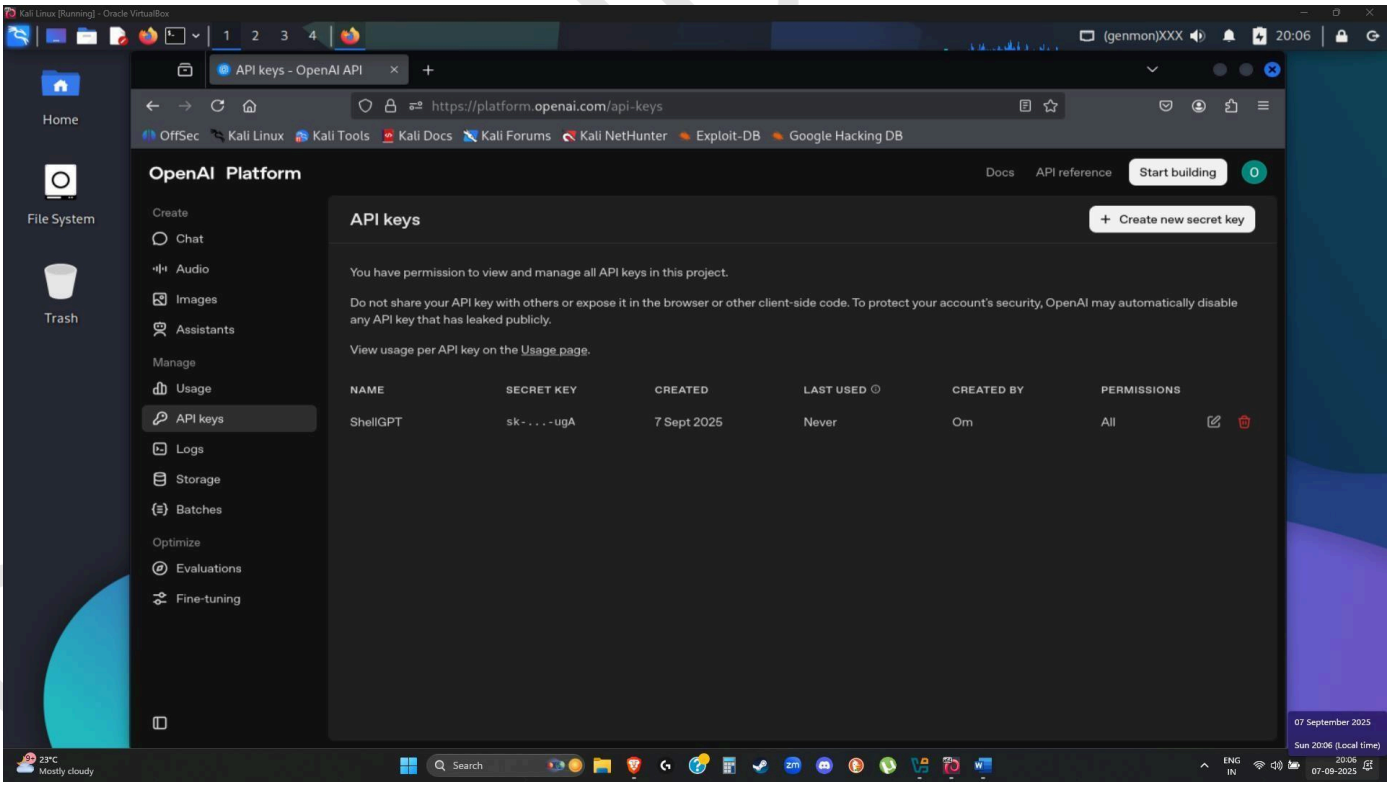
- First create API secret Key.



- Created API secret Key.

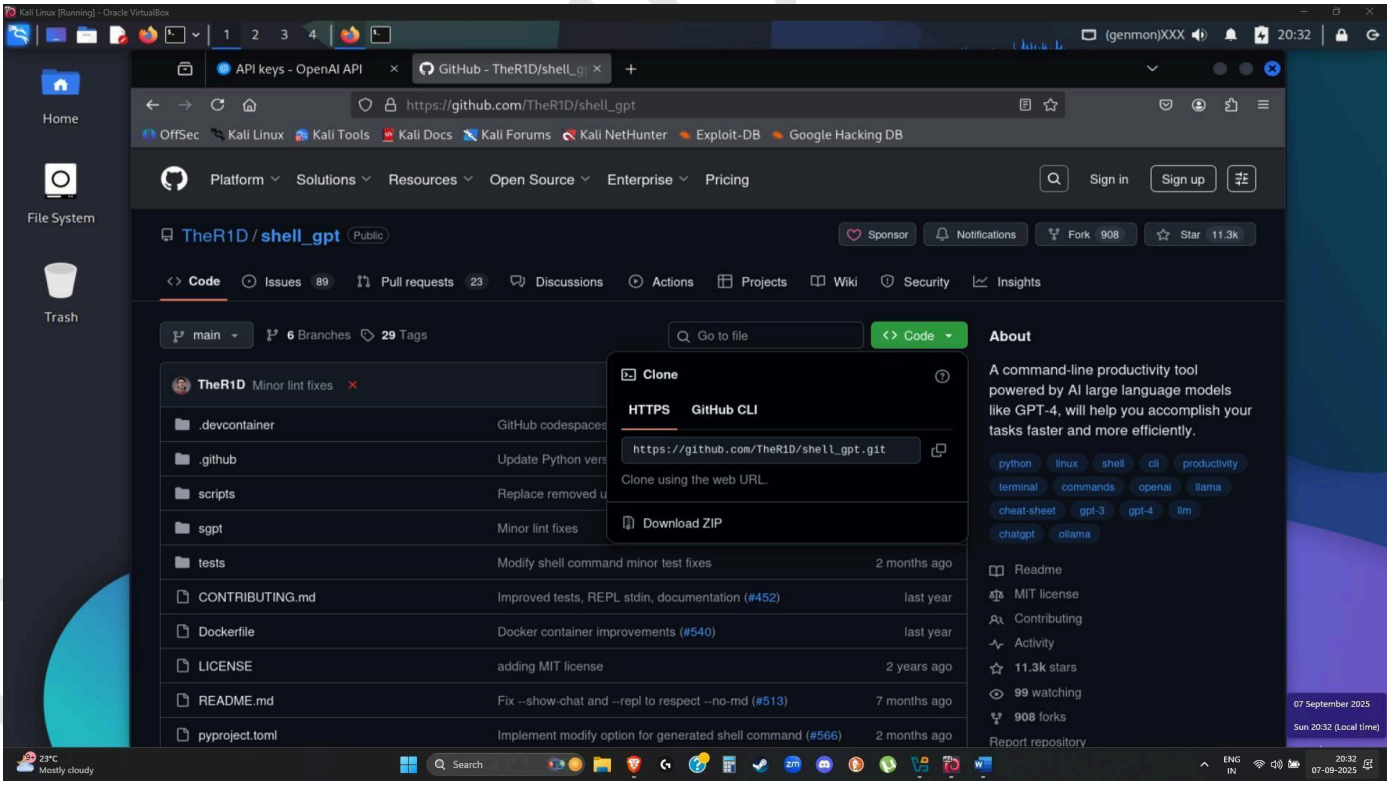


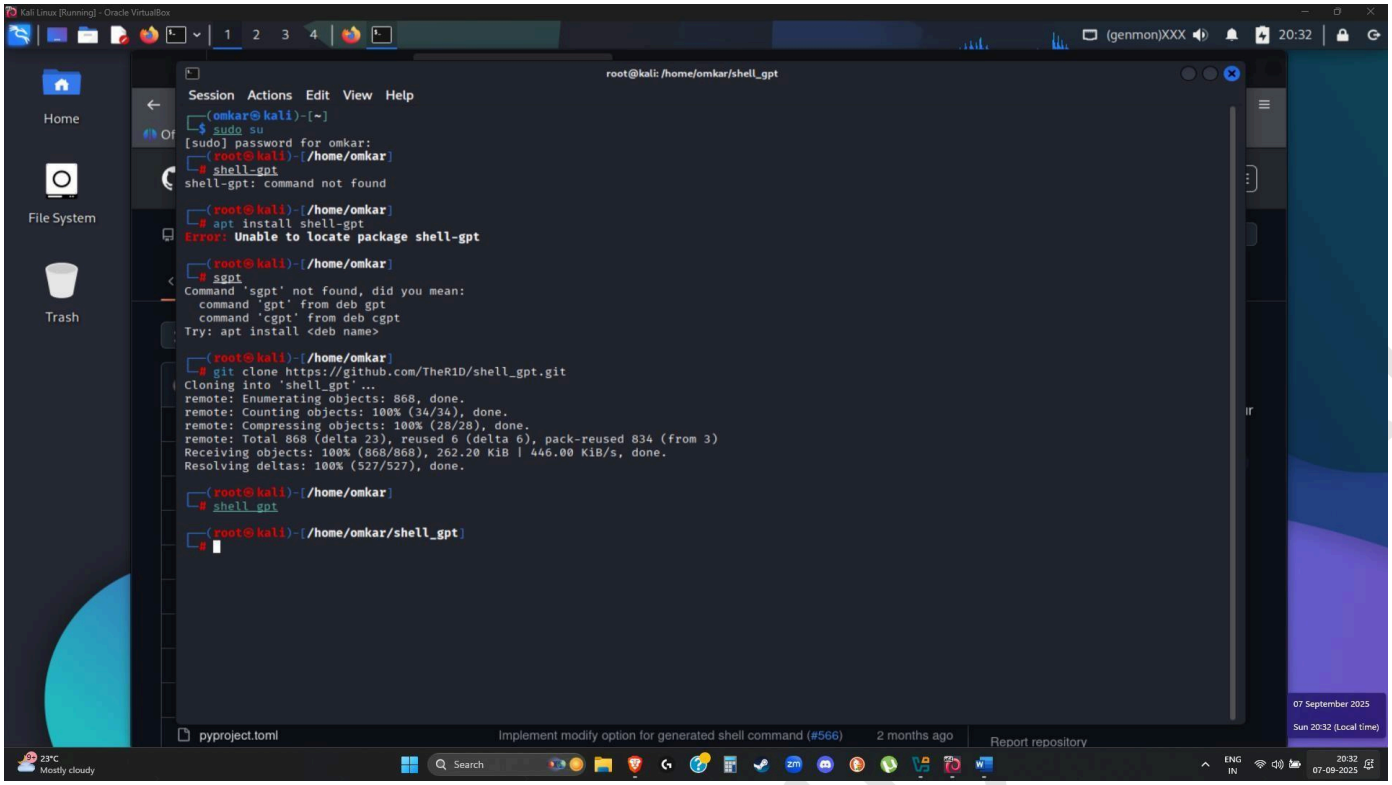
- Generated and Saved API key



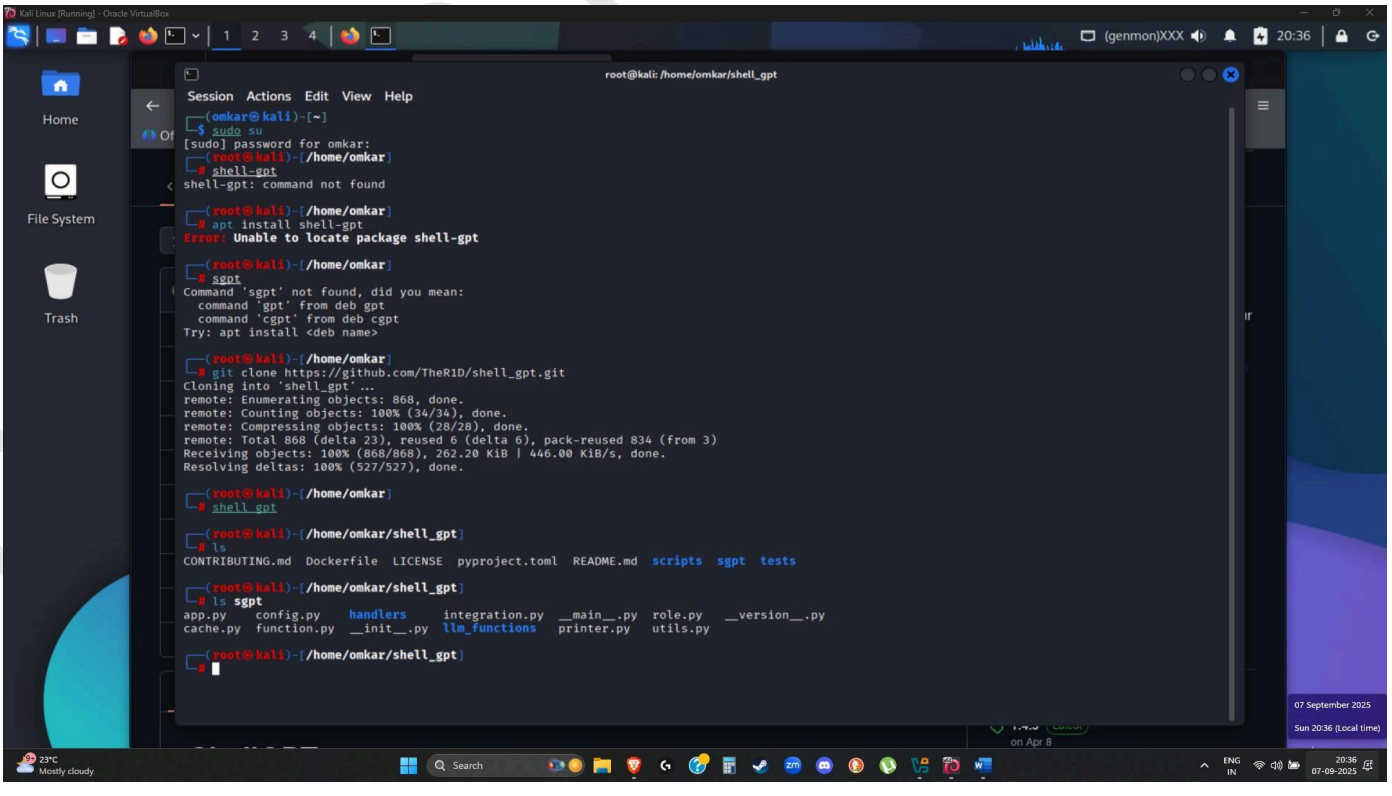
- In Kali Linux run Terminal

- 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**





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

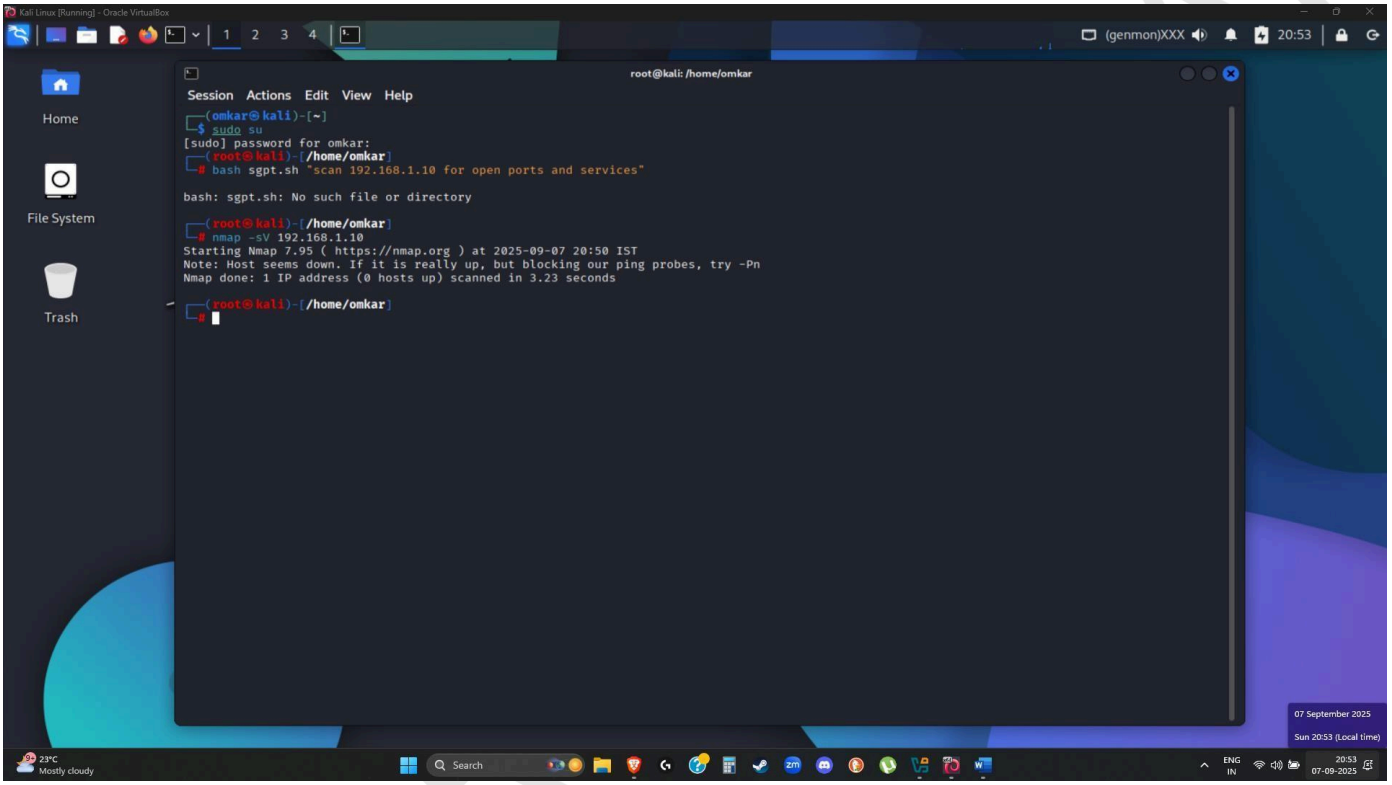


- Now we use command in shell-gpt.

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

- For open ports and services.

  nmap -sV 192.168.1.10



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.