

REPORT ON FOOTPRINTING

-Tanmay Khedekar

Table of Contents: -

INDEX	PG.NO
<u>1. Introduction</u>	3
<u>1.1 Goals of Footprinting</u>	3
<u>1.2 Types of Footprinting (Active & Passive)</u>	3
<u>2. Footprinting Using Search Engine (Google Dorking)</u>	4
<u>3. Footprinting Using Netcraft (Web-based Tool)</u>	7
<u>4. Footprinting Using DNS Dumpster (Web-based Tool)</u>	8
<u>5. Footprinting Using WHOIS (Web-based Tool)</u>	10
<u>6. Footprinting Using DNS Lookup (Web-based Tool)</u>	11
<u>7. Footprinting Using Sublist3r (CLI Tool)</u>	13
<u>8. Footprinting Using Traceroute (CLI Tool)</u>	13
<u>9. Footprinting Using Recon-ng (CLI Tool)</u>	14
<u>10. Footprinting Using Nikto (CLI Tool)</u>	18
<u>11. Footprinting Using NAPALM FTP indexer (web-based tool)</u>	18
<u>12. Footprinting Using OSINT Framework (web-based tool): -</u>	19
<u>13. Footprinting Using email spider (software-based tool): -</u>	21
<u>14. Footprinting using dig tool (CLI Tool)</u>	21
<u>15. Footprinting using dnsenum (CLI Tool)</u>	22
<u>16. Objective</u>	23

1. Introduction

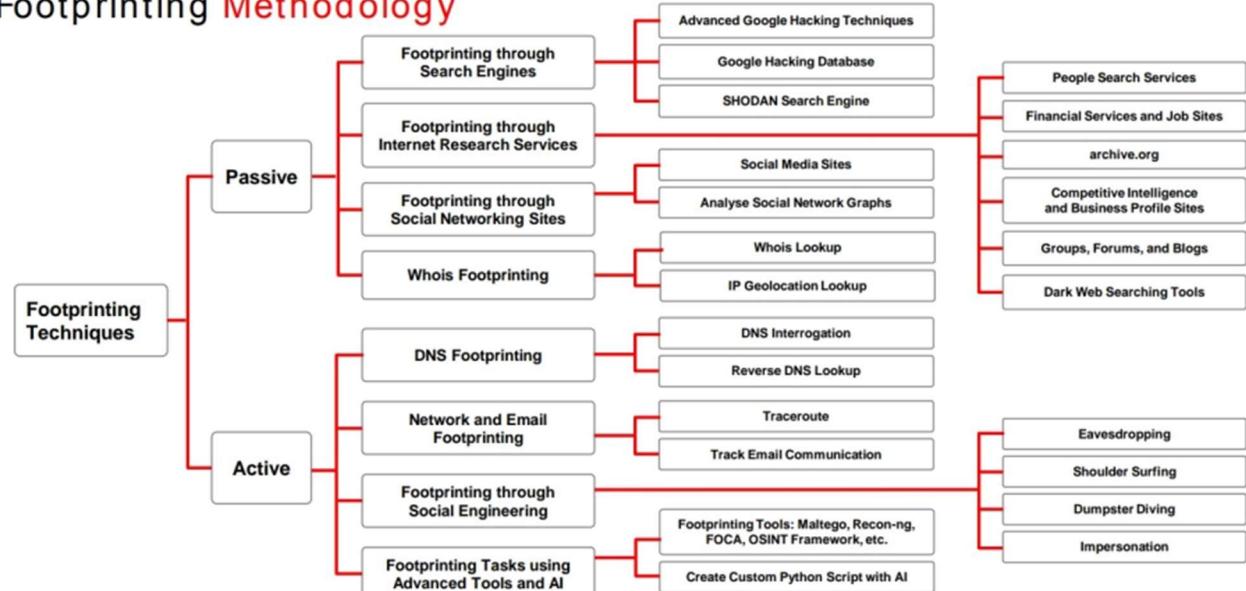
Footprinting is the initial phase of cyber security where information about a target system or organization is collected before performing any active testing. The goal is to gather publicly available data such as domains, IP addresses, technologies, network structure, and user details. This information helps identify potential entry points and understand the overall security posture of the target. Footprinting is essential for planning further penetration testing steps and reducing blind spots in the assessment.

1.1 The main goals are:

- Identify the target's public information
- Find the attack surface
- Understand how the system works
- Discover weak points that can be attacked later
- Reduce blind spots before testing

1.2 Types of Footprinting-

Footprinting Methodology



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit www.eccouncil.org

2.Footprinting Using Search Engine (Google Dorking):

These Google advanced search operators are used to collect publicly available information about a target during the reconnaissance phase. They help identify indexed pages, exposed data, and potential misconfigurations without directly interacting with the system. This improves the quality and depth of the security assessment.

Popular Google advanced search operators

Search Operator	Purpose
[cache:]	Displays the web pages stored in the Google cache
[link:]	Lists web pages that have links to the specified web page
[related:]	Lists web pages that are similar to the specified web page
[info:]	Presents some information that Google has about a particular web page
[site:]	Restricts the results to those websites in the given domain

Search Operator	Purpose
[allintitle:]	Restricts the results to those websites containing all the search keywords in the title
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allinurl:]	Restricts the results to those containing all the search keywords in the URL
[inurl:]	Restricts the results to documents containing the search keyword in the URL
[location:]	Finds information for a specific location

Fig.2.1 – Popular Google advance search engine

How to Use it: -Open Browser and Search Google and after search google Type Advance search operators:

Ex.a) intitle:login site: testfire.net

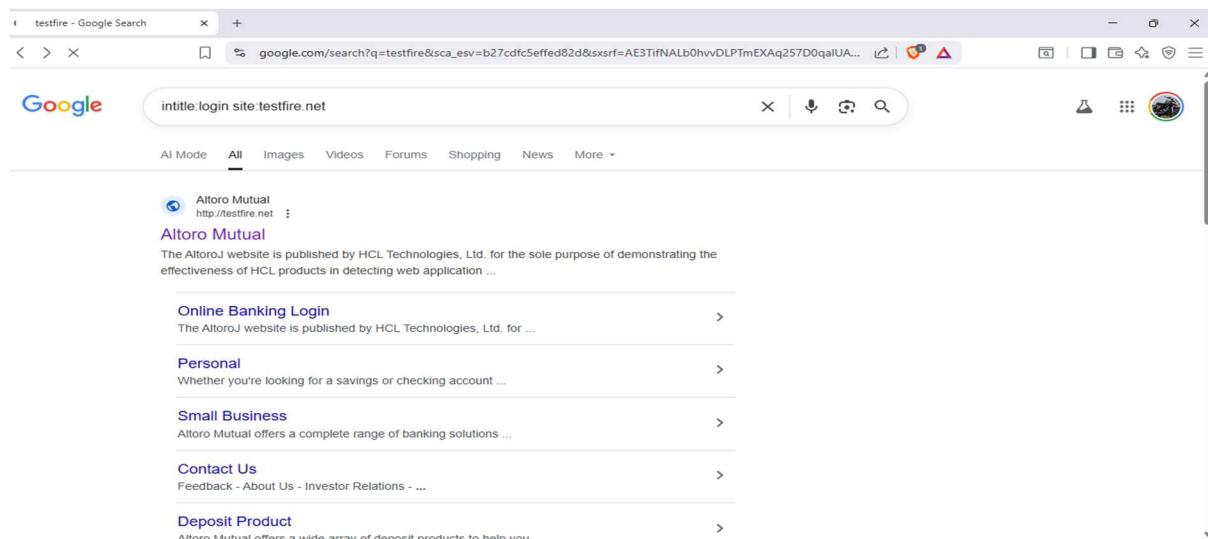


Fig.2.2 – Google Dorking using this get direct login page

b)info: testfire.net

Google search results for "info:testfire.net". The results include:

- Altoro Mutual** (<http://testfire.net>)
We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.
Deposit Product, Personal, Online Banking Login, Loan Products
- Altoro Mutual** (<http://testfire.net/login>)
Secure Login ONLINE BANKING LOGIN · PERSONAL · SMALL BUSINESS ; PERSONAL · Deposit Product · Checking · Loan Products · Cards · Investments & Insurance · Other ...
- Contact Us**
Filling out the online form is the most efficient method of contact. If you are requesting a change to your account, please call the phone number listed below.
Feedback, About Us, Investor Relations

Fig.2.3 – Google Dorking, using we get target info.

c)intext: personal site: testfire.net

Google search results for "intext:personal site:testfire.net". The results include:

- Altoro Mutual** (<http://testfire.net?content=personal>)
Personal
Whether you're looking for a savings or checking account, credit card, or personal loan, our solutions are designed to make banking as efficient and cost ...
- Altoro Mutual** (<http://testfire.net>)
PERSONAL · Deposit Product · Checking · Loan Products · Cards · Investments & Insurance · Other Services · SMALL BUSINESS.
- Altoro Mutual** (<http://altoro.testfire.net/login>)
Online Banking Login
Secure Login ONLINE BANKING LOGIN · PERSONAL · SMALL BUSINESS ; PERSONAL · Deposit Product · Checking · Loan Products · Cards · Investments & Insurance · Other ...
- Altoro Mutual** (http://testfire.net?content=personal_other)

Fig.2.4 – Google Dorking, using we get personal intext of that target.

d)allintitle: testfire.net

Google search results for "allintitle: testfire.net":

- AltoroJ / testfire.net - ZAP
AltoroJ, also known as Altoro Mutual and Testfire, is an open source sample banking J2EE web application maintained by HCL Software. It is a traditional app ...
- Altoro Mutual
http://www.testfire.net/pr/Docs.xml
- Slideshare
Penetration Testing Report for http://altoro.testfire.net/.pdf
Penetration Testing Report for http://altoro.testfire.net/ - Download as a PDF or view online for free.
- GitHub
ZAP does not detect SQL Injection in demo.testfire.net login ...
20 Oct 2021 — Using ZAP to scan the demo.testfire.net web site, it doesn't detect some basic SQL

Fig.2.5 – Google Dorking, using we get related all title of that target.

e)testfire.net inanchor:admin

Google search results for "testfire.net inanchor: admin":

- Altoro Mutual
http://testfire.net/login
- Online Banking Login
Online Banking Login Username: Password: Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.
- Altoro Mutual
We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.
Online Banking Login Deposit Product Loan Products Personal
- Slideshare
Penetration Testing Report for http://altoro.testfire.net/.pdf
The penetration test was conducted on http://altoro.testfire.net to identify and assess security vulnerabilities that could potentially be exploited by ...

Fig.2.6 – Google Dorking, using find webpages that other sites link to using specific anchor text.

3. Footprinting using Netcraft (Web base tool):

Netcraft Website is a **public online database** that provides detailed information about who owns a **domain name, IP address, server names, subdomains, operating System**.

How to use it: - Open Browser search Netcraft and open Netcraft website after opening website gives targeted domain.

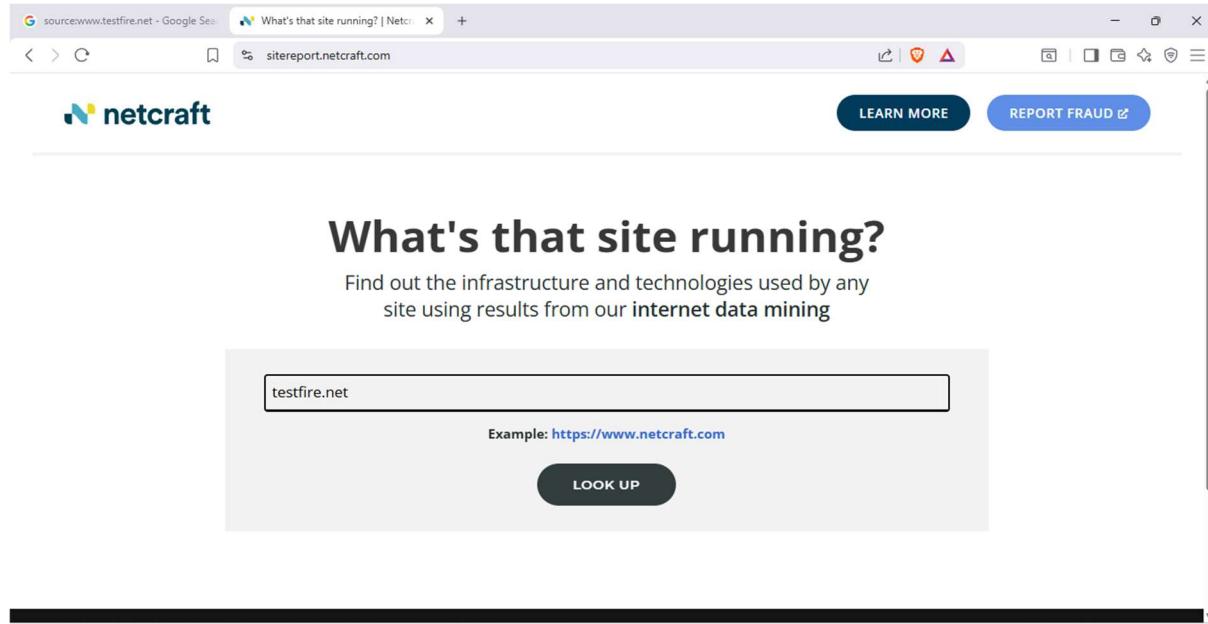


Fig.3.1 – shows netcraft website

- Here it finds some Name server and other information

Background			
Site title	Altro Mutual	Date first seen	April 2000
Site rank	5513	Primary language	English
Description	Not Present		
Network			
Site	http://testfire.net	Domain	testfire.net
Netblock Owner	Rackspace Backbone Engineering	Nameserver	asia3.akam.net
Hosting company	Rackspace	Domain registrar	registrar.amazon
Hosting country	US	Nameserver organisation	whois.markmonitor.com
IPv4 address	65.61.137.117	Organisation	Identity Protection Service, PO Box 786, Hayes, UB9 9TR, United Kingdom
IPv4 autonomous systems	AS33070	DNS admin	hostmaster@akamai.com
IPv6 address	Not Present	Top Level Domain	Network entities (.net)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Enabled
Reverse DNS	Unknown		
IP delegation			

Fig.3.2 – shows target related information using netcraft.

- Hostnames matching testfire.net

source:www.testfire.net - Google Search | Research Tools | Netcraft | Hostnames matching testfire.net | +

searchdns.netcraft.com/?restriction=site+contains&host=testfire.net&position=limited

LEARN MORE REPORT FRAUD

Hostnames matching testfire.net

▶ Search with another pattern?

7 results

Rank	Site	First seen	Netblock	OS	Site Report
5580	testfire.net	April 2017	Rackspace Backbone Engineering	unknown	
20036	demo.testfire.net	August 2005	Rackspace Backbone Engineering	Windows Server 2008	
70502	www.testfire.net	April 2000	Rackspace Backbone Engineering	Windows Server 2008	
86122	altoro.testfire.net	August 2018	Rackspace Backbone Engineering	Windows Server 2008	

Fig.3.3 – shows target related information using netcraft.

4. Footprinting Using DNS dumpster (Web base tool):

A **DNS dumpster** Website is an online tool that helps you **find the IP address, DNS records, and server details** of a domain name.

How to use it: -search DNS dumpster on browser and open DNS dumpster website after opening website gives targeted domain.

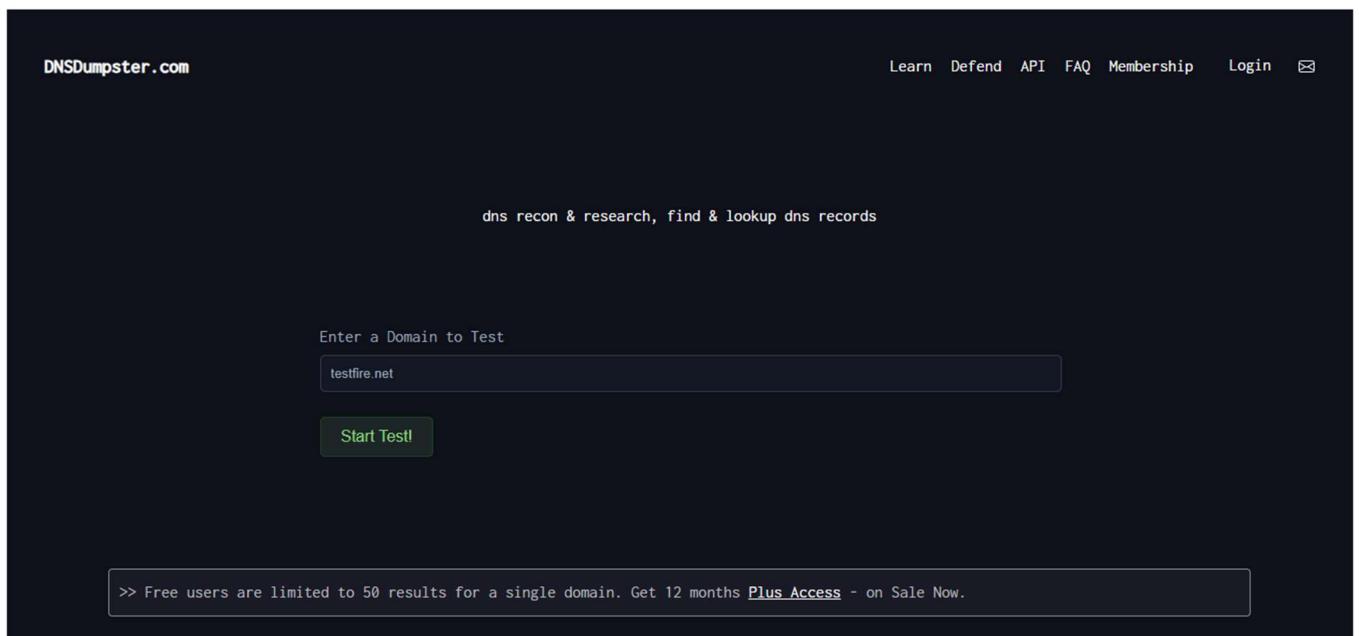


Fig.4.1 – shows DNS dumpster interface

- Shows geographical system location

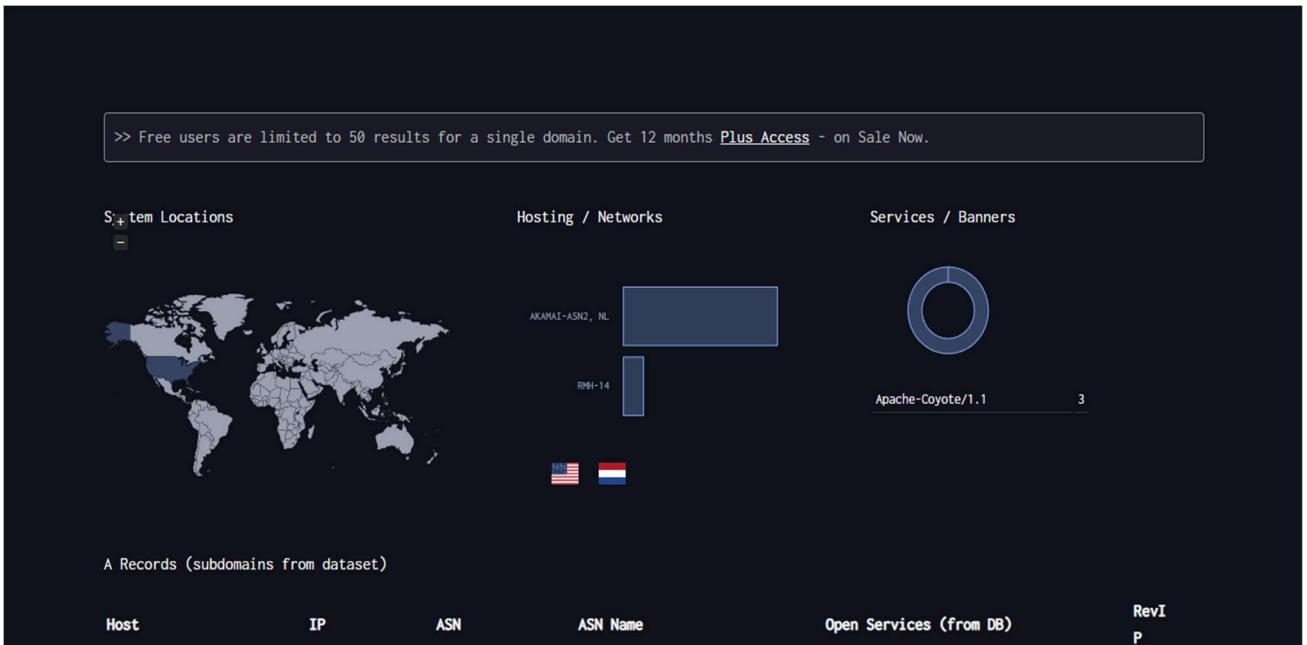


Fig.4.2 – shows target related geographical information.

- Graphical Representation shows DNS report and ip's

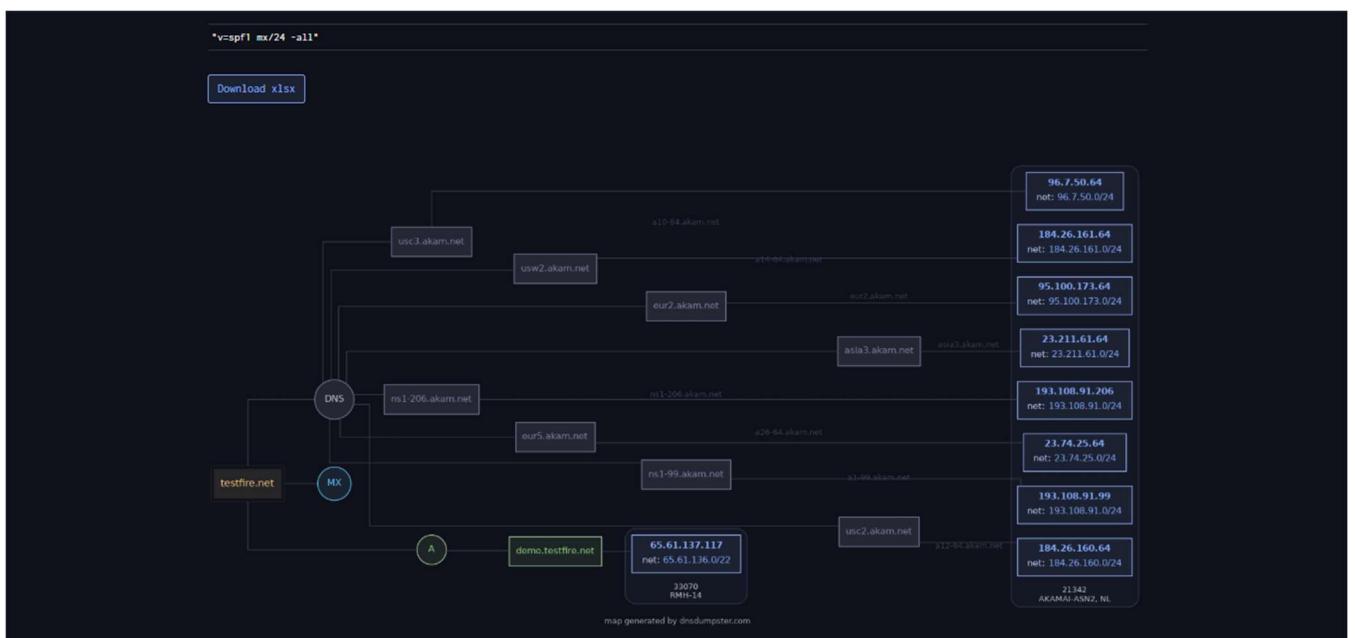


Fig.4.3 – shows graphical presentation of target

5. Footprinting Using Whois (Web base tool):

WHOIS Website is a **public online database** that provides detailed information about who owns a domain name or IP address.

How to use it: -Search Whois on browser and open Whois website after opening website gives targeted domain.



Frequently Asked Questions



Fig.5.1 – whois interface

- Here it finds some Domain information

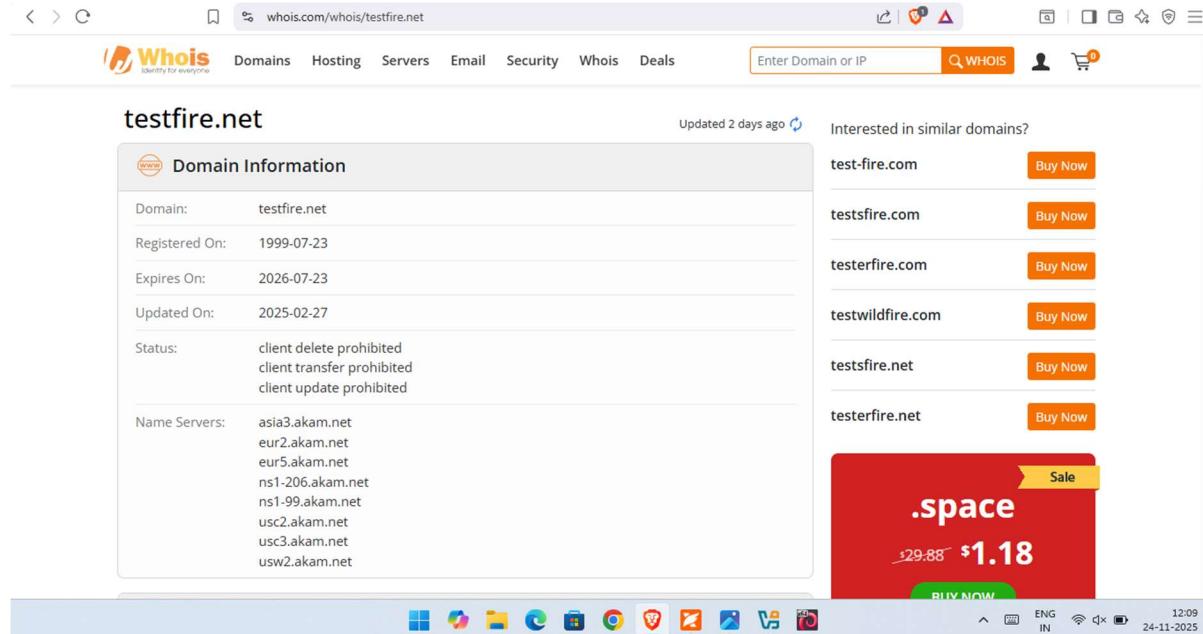


Fig.5.2 – shows target related information.

- Registrar Information and Registrant Contact

The screenshot shows a web browser displaying the Whois search results for the domain testfire.net. The main content area is divided into two sections: 'Registrar Information' and 'Registrant Contact'. Under 'Registrar Information', the details are as follows:

- Registrar: Amazon Registrar, Inc.
- IANA ID: 468
- Email: registrar@amazon.com
- Abuse Email: trustandsafety@support.aws.com
- Abuse Phone: +1.2024422253

Under 'Registrant Contact', the details are as follows:

- Name: On behalf of testfire.net owner
- Organization: Identity Protection Service
- Street: PO Box 786
- City: Hayes
- State: Middlesex
- Postal Code: UB3 9TR

On the right side of the page, there are promotional banners for '.UNO' domains and 'WORDPRESS HOSTING' at \$5.48/mo. The browser status bar at the bottom shows the URL <https://shop.whois.com/optimized-wordpress-hosting.php>, the date 24-11-2025, and system information like ENG IN.

Fig.5.3 – shows target more information

6.Footprinting Using DNS Lookup (Web base tool):

A **DNS Lookup Website** is an online tool that helps you **find the IP address, DNS records, and server details** of a domain name.

How to use it: -Search Nslookup on browser and open Nslookup website after opening website gives targeted domain.

The screenshot shows the nslookup.io website interface. At the top, there is a search bar with the domain 'testfire.net' and a button labeled 'Find DNS records'. Below the search bar, a message reads: 'Find all DNS records for a domain name using this online tool. For example, try [wikipedia.org](#) or [www.twitter.com](#) to view their DNS records.' A dark blue sidebar on the left contains the text 'By Nslookup.io', 'DNS for Developers', and 'Never be confused about DNS again.' The browser status bar at the bottom shows the URL <https://nslookup.io/>, the date 24-11-2025, and system information like ENG IN.

Fig.6.1- nslookup interface

▪ DNS Record Result

The screenshot shows the nslookup.io website interface. At the top, there's a navigation bar with links for 'Cloudflare', 'Google DNS', 'Authoritative', 'Control D', and 'Local DNS'. Below the navigation is a search bar with the query 'testfire.net' and a button 'Find DNS records'. To the right of the search bar are links for 'Learning', 'Browser extension', and 'DNS lookup API'. The main content area is titled 'DNS records for testfire.net'. It displays the following information:

- A records:** An IPv4 address listed as 65.61.137.117, with a 'Revalidate in' time of 24h.
- AAAA records:** No AAAA records found.
- CNAME record:** No CNAME record found.

On the right side of the main content area, there's a dark blue sidebar with the text 'By Nslookup.io' and 'DNS for Developers' followed by the tagline 'Never be confused about DNS again.'

Fig.6.2- shows dns record of target.

▪ Ns Records/ MX records

The screenshot shows the nslookup.io website interface, similar to Fig.6.2 but with different results. The main content area is titled 'NS records' and lists several name servers:

Name server	Revalidate in
usw2.akam.net.	24h
usc3.akam.net.	24h
ns1-99.akam.net.	24h
eur2.akam.net.	24h
eur5.akam.net.	24h
asia3.akam.net.	24h
ns1-206.akam.net.	24h
usc2.akam.net.	24h

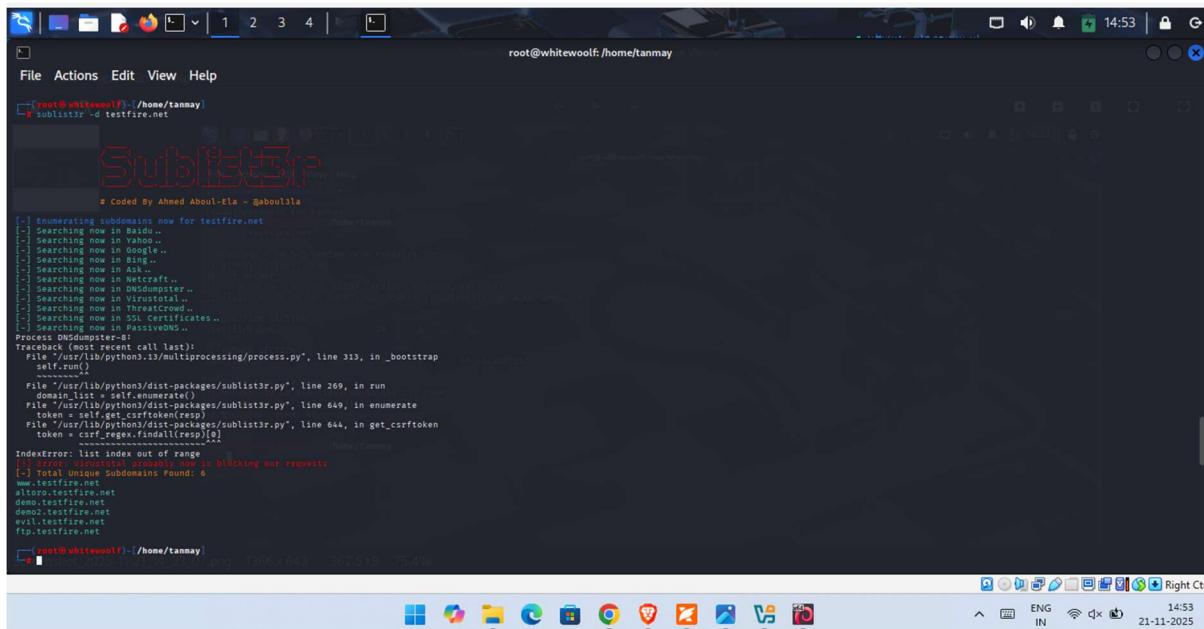
Below the NS records, there's a section for 'MX records' which states 'No mail servers found.' There's also a 'Other records' section with a dropdown menu currently set to 'SOA'.

Fig.6.3- shows ns records of target.

7. Footprinting Using Sublister CLI Tool: -

How to use it: - Open Kali Linux and run Terminal.

Command- sublist3r -d testfire.net using this command, we get sub domains. Here **-d** use to put domain in command line.



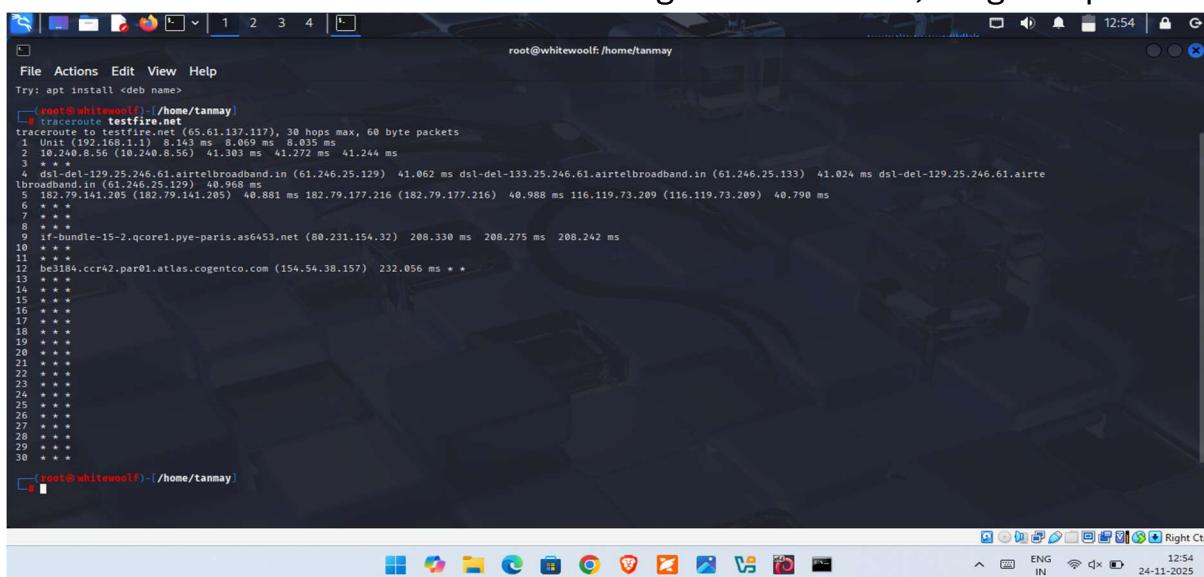
```
[root@whitewoolf ~]# ./sublist3r -d testfire.net
[!] Enumerating subdomains now for testfire.net
[!] Searching now in Yahoo...
[!] Searching now in Google...
[!] Searching now in Bing...
[!] Searching now in DuckDuckGo...
[!] Searching now in Netcraft...
[!] Searching now in DNSdumpster...
[!] Searching now in Shodan...
[!] Searching now in Threatcrowd...
[!] Searching now in SSL Certificates...
[!] Searching now in Whois...
Process DNSdumpster-B:
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 313, in _bootstrap
    self.run()
  File "----"
  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
    resp = self._request(url)
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in _request
    token = csrf_regex.findall(resp)[0]
IndexError: list index out of range
Error: VirusTotal actually now is blocking our requests
[!] Total Unique Subdomains Found: 6
www.testfire.net
altcoro.testfire.net
demo.testfire.net
demopage.testfire.net
exit.testfire.net
ftp.testfire.net
[root@whitewoolf ~]
```

Fig.7.1- shows sub domain using sublist3r.

8. Footprinting Using Traceroute CLI Tool: -

How to use it: - Open Kali Linux and run Terminal.

Command- traceroute testfire.net using this command, we get hopes.



```
[root@whitewoolf ~]# traceroute testfire.net
traceroute to testfire.net (65.61.137.117), 30 hops max, 60 byte packets
1 Unit (192.168.1.1) 8.143 ms 8.069 ms 8.035 ms
2 10.240.8.56 (10.240.8.56) 41.303 ms 41.272 ms 41.244 ms
3 *
4 dsl-del-129.25.246.61.airtelbroadband.in (61.246.25.129) 41.062 ms dsl-del-133.25.246.61.airtelbroadband.in (61.246.25.133) 41.024 ms dsl-del-129.25.246.61.airtelbroadband.in (61.246.25.129) 40.968 ms
5 182.79.141.205 (182.79.141.205) 40.881 ms 182.79.177.216 (182.79.177.216) 40.988 ms 116.119.73.209 (116.119.73.209) 40.790 ms
6 *
7 *
8 if-brbundle-15-2.qcore1.pye-paris.as6453.net (80.231.154.32) 208.330 ms 208.275 ms 208.242 ms
9 *
10 *
11 be3184.ccr42.par01.atlas.cogentco.com (154.54.38.157) 232.056 ms * *
12 *
13 *
14 *
15 *
16 *
17 *
18 *
19 *
20 *
21 *
22 *
23 *
24 *
25 *
26 *
27 *
28 *
29 *
30 *

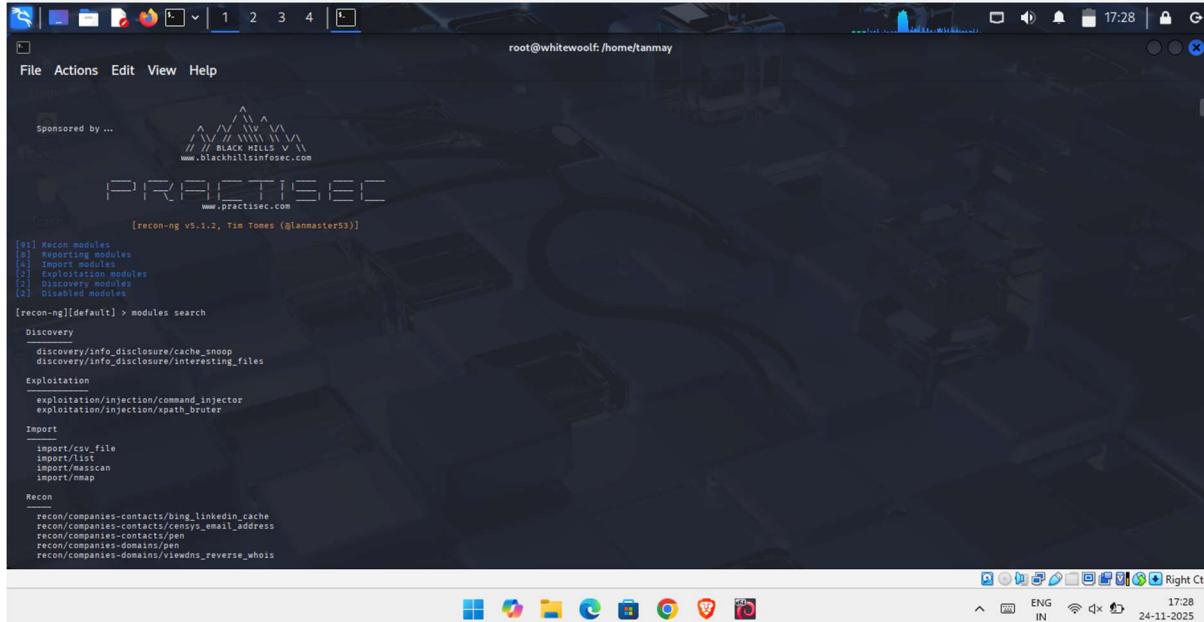
[root@whitewoolf ~]
```

Fig.8.1- shows in between hopes

9. Footprinting Using recon-ng CLI Tool: -

How to use it: - Open Kali Linux and run Terminal.

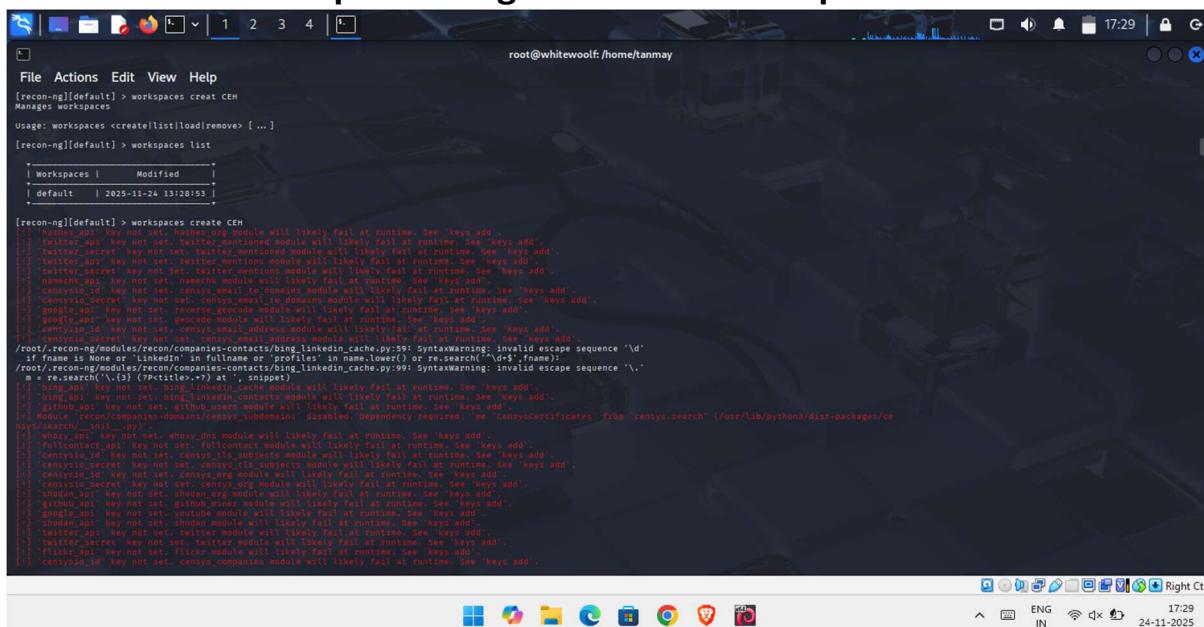
Command- recon-ng using this command tool get start. As shown below-



```
[recon-ng] > 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
import/masscan
import/map
Recon
recon/companies-contacts/bing_linkedin_cache
recon/companies-contacts/censys_email_address
recon/companies-contacts/pdn
recon/companies-domains/pen
recon/companies-domains/viewdns_reverse_whois
```

Fig.9.1- Starting of tool

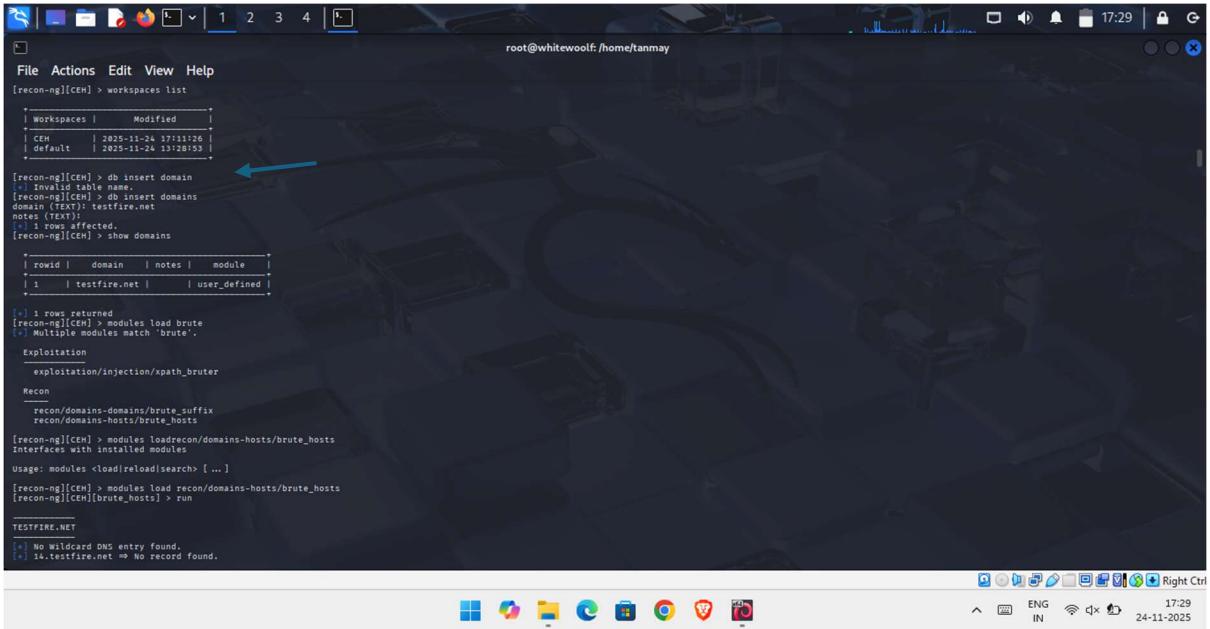
▪ Create Workspace using command- workspace create CEH



```
[recon-ng] > workspaces create CEH
[recon-ng] > workspaces list
[recon-ng] > workspaces create CEH
[recon-ng] >
```

Fig.9.2- Creating work space.

- To check work space is created or not **Command – workspace list**



```

root@whitewoolf:/home/tanmay
[recon-ng][CEH] > workspaces list
| workspaces | Modified |
| CEM | 2025-11-24 17:11:26 |
| default | 2025-11-24 13:28:53 |

[recon-ng][CEH] > db insert domain
[recon-ng][CEH] > db insert domains
domain (TEXT): testfire.net
notes()
| 1 rows affected.

[recon-ng][CEH] > show domains

| rowid | domain | notes | module |
| -1 | testfire.net | user_defined |

| 1 rows returned.

[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.

Exploitation
exploitation/injection/xpath_bruter
Recon
recon/domains-domains/brute_SUFFIX
recon/domains-hosts/brute_HOSTS

[recon-ng][CEH] > modules loadrecon/domains-hosts/brute_HOSTS
Interfaces with installed modules
Usage: modules <load|reload|search> [ ... ]

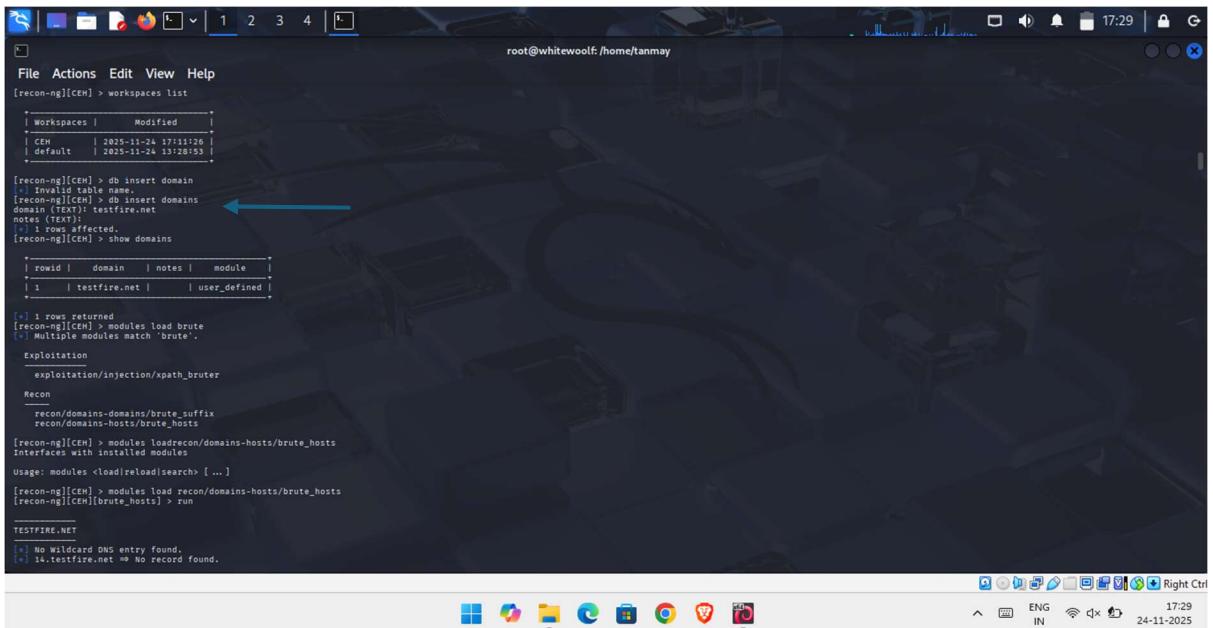
[recon-ng][CEH]> modules load recon/domains-hosts/brute_HOSTS
[recon-ng][CEH]> [brute_HOSTS]> run

TESTFIRE.NET
[*] No Wildcard DNS entry found.
[*] 14.testfire.net => No record found.

```

Fig.9.3- shows work list

- To insert Domain in workspace **Command- db insert domains** and press **enter** after pressing enter insert domain and press **enter**.



```

root@whitewoolf:/home/tanmay
[recon-ng][CEH] > workspaces list
| workspaces | Modified |
| CEM | 2025-11-24 17:11:26 |
| default | 2025-11-24 13:28:53 |

[recon-ng][CEH] > db insert domain
[recon-ng][CEH] > db insert domains
domain (TEXT): testfire.net
notes()
| 1 rows affected.

[recon-ng][CEH] > show domains

| rowid | domain | notes | module |
| -1 | testfire.net | user_defined |

| 1 rows returned.

[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.

Exploitation
exploitation/injection/xpath_bruter
Recon
recon/domains-domains/brute_SUFFIX
recon/domains-hosts/brute_HOSTS

[recon-ng][CEH] > modules loadrecon/domains-hosts/brute_HOSTS
Interfaces with installed modules
Usage: modules <load|reload|search> [ ... ]

[recon-ng][CEH]> modules load recon/domains-hosts/brute_HOSTS
[recon-ng][CEH]> [brute_HOSTS]> run

TESTFIRE.NET
[*] No Wildcard DNS entry found.
[*] 14.testfire.net => No record found.

```

Fig.9.4- Adding target in database.

- To check domain is created in workspace or not **Command-Show domains**

```
[recon-ng][cEH] > workspaces list
[recon-ng][cEH] > db insert domain
    Invalid table name.
[recon-ng][cEH] > db insert domains
domains (TEXT); testfire.net
notes (TEXT);
+: 1 rows affected.
[recon-ng][cEH] > show domains
[recon-ng][cEH] >
[recon-ng][cEH] > modules load brute
+: Multiple modules match 'brute'.
Exploitation
exploitation/injection/xpath_bruter
Recon
recon/domains-domains/brute_SUFFIX
recon/domains-hosts/brute_HOSTS
[recon-ng][cEH] > modules load recon/domains-hosts/brute_HOSTS
Interfaces with installed modules
Usage: modules load/reload/search [ ... ]
[recon-ng][cEH] > modules load recon/domains-hosts/brute_HOSTS
[recon-ng][cEH][brute_HOSTS] > run

TESTFIRE.NET
+: No Wildcard DNS entry found.
14.testfire.net => No record found.
```

Fig.9.5- shows added list of domains.

- Then Load module **Command- modules load brute**

```
[recon-ng][CEH] > workspaces list
[recon-ng][CEH] > db insert domain
[*] Invalid table name.
[recon-ng][CEH] > db insert domains
domains: testfire.net
notes (TEXT):
[*] 1 rows affected.
[recon-ng][CEH] > show domains
[recon-ng][CEH] >
[*] 1 rows returned
[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.
Exploitation
exploitation/injection/xpath_buzzer
Recon
recon/domains-domains/brute_SUFFIX
recon/domains-hosts/brute_HOSTS

[recon-ng][CEH] > modules load recon/domains-hosts/brute_HOSTS
Interfaces with installed modules

Usage: modules <load|reload>[search] [ ... ]
[recon-ng][CEH] > modules load recon/domains-hosts/brute_HOSTS
[recon-ng][CEH][brute_HOSTS] > run

TESTFIRE.NET
[*] No Wildcard DNS entry found.
[*] 14.testfire.net => No record found.
```

Fig.9.6- Selecting recon.

- Then recon model load

Command- modules load recon/domain-hosts/brute_hosts and press **enter**.

For work this command give **Command- Run**.

```

root@whitewoolf:/home/tanmay
[recon-ng][CEH] > workspaces list
[recon-ng][CEH] > db insert domain
[*] Invalid table name.
[recon-ng][CEH] > db insert domains
domains > testfire.net
notes (TEXT):
[*] 1 rows affected.
[recon-ng][CEH] > show domains
[*] 1 rows returned
[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.
Exploitation
  exploitation/injection/xpath_bruter
Recon
  recon/domains-domains/brute_SUFFIX
  recon/domains-hosts/brute_HOSTS
[recon-ng][CEH] > modules load recon/domains-hosts/brute_HOSTS
Interfaces with installed modules
Usage: modules <load|reload|search> [ ... ]
[recon-ng][CEH] > modules load recon/domains-hosts/brute_HOSTS
[recon-ng][CEH]> run
TESTFIRE.NET
[*] No Wildcard DNS entry found.
[*] 14.testfire.net => No record found.

```

Fig.9.7- Running recon.

- After running above commands, it shows hosts as result for seeing that hosts.

Command-Show host

```

root@whitewoolf:/home/tanmay
[recon-ng][CEH] > show hosts
[*] total (7 new) hosts found.
[recon-ng][CEH][brute_HOSTS] > show
Shows various framework items
Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>
[recon-ng][CEH][brute_HOSTS] > show host
Shows various framework items
Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>
[recon-ng][CEH][brute_HOSTS] > show hosts
[*] 7 rows returned
[recon-ng][CEH][brute_HOSTS] > back
[recon-ng][CEH] > module load exploitation/injection/xpath_BRUTER
[*] Invalid command - module load exploitation/injection/xpath_BRUTER.
[recon-ng][CEH] > module load exploitation/injection/xpath_BRUTER
[recon-ng][CEH][xpath_BRUTER] > run
[*] value required for the 'BASE_URL' option.

SUMMARY
[*] 1 total (3 new) domains found.
[recon-ng][CEH][xpath_BRUTER] > show domain
Shows various framework items
Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>
[recon-ng][CEH][xpath_BRUTER] > show domains
[*] 1 rows returned

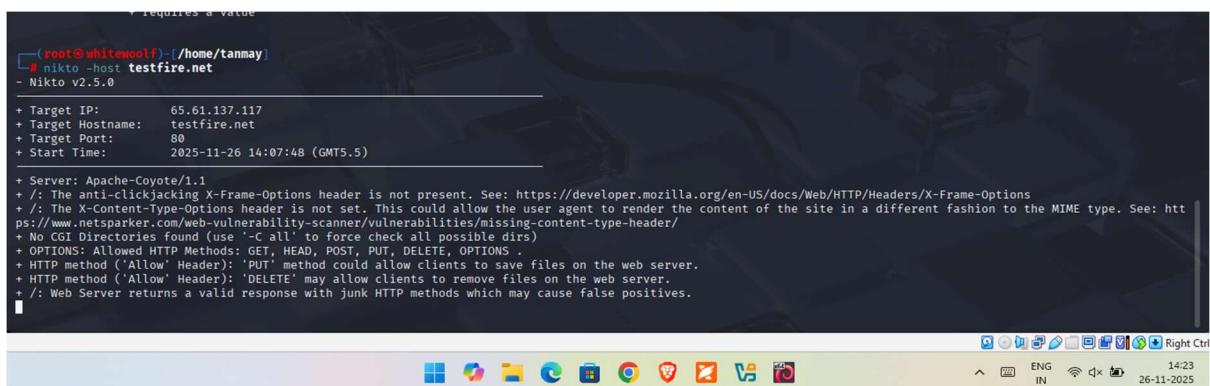
```

Fig.9.8- Showing subdomain.

10. Footprinting Using Nikto CLI Tool: -

How to use it: - Open Kali Linux and run Terminal.

Command- nikto -host testfire.net



```
+ requires a value
(root@whitewolf:~/home/tanmay]
└─# nikto -host testfire.net
- Nikto v2.5.0

+ Target IP:      65.61.137.117
+ Target Hostname: testfire.net
+ Target Port:    80
+ Start Time:    2025-11-26 14:07:48 (GMT5.5)

+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.

[...]
```

Fig.10.1- Running nikto tool.

11. Footprinting Using NAPALM FTP indexer (web base tool): -

How to use it: - Open any browser and search napalm ftp indexer. After searching in browser open first website shown after that give domain name to search for ex.microsoft using this tool we get all the words related data.

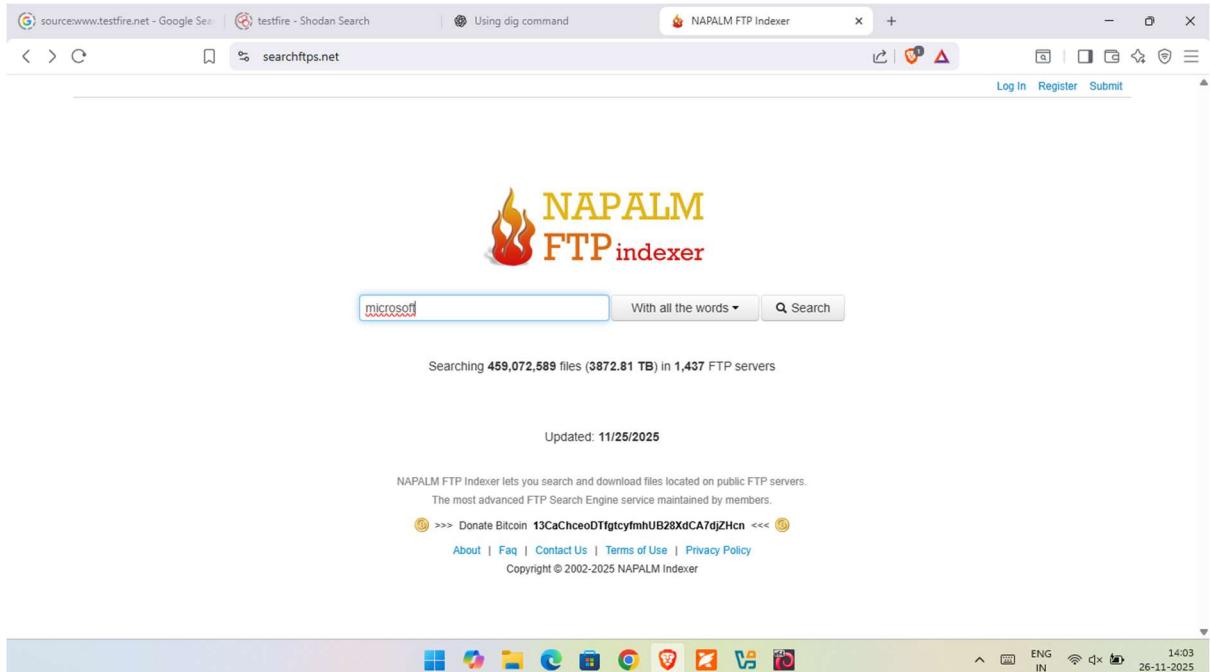


Fig.11.1- NAPALM interface.

- Result

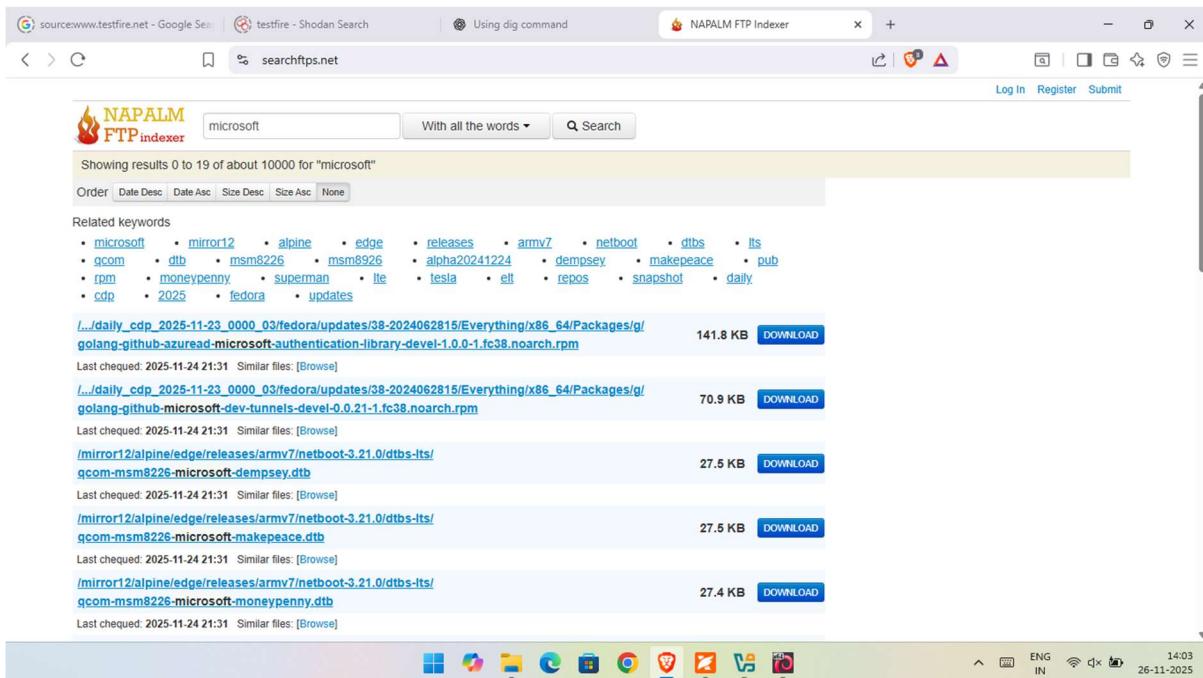


Fig.11.2- Showing Result.

12. Footprinting Using OSINT Framework (web base tool): -

How to use it: - Open any browser and search osint framework. After searching in browser open first website.

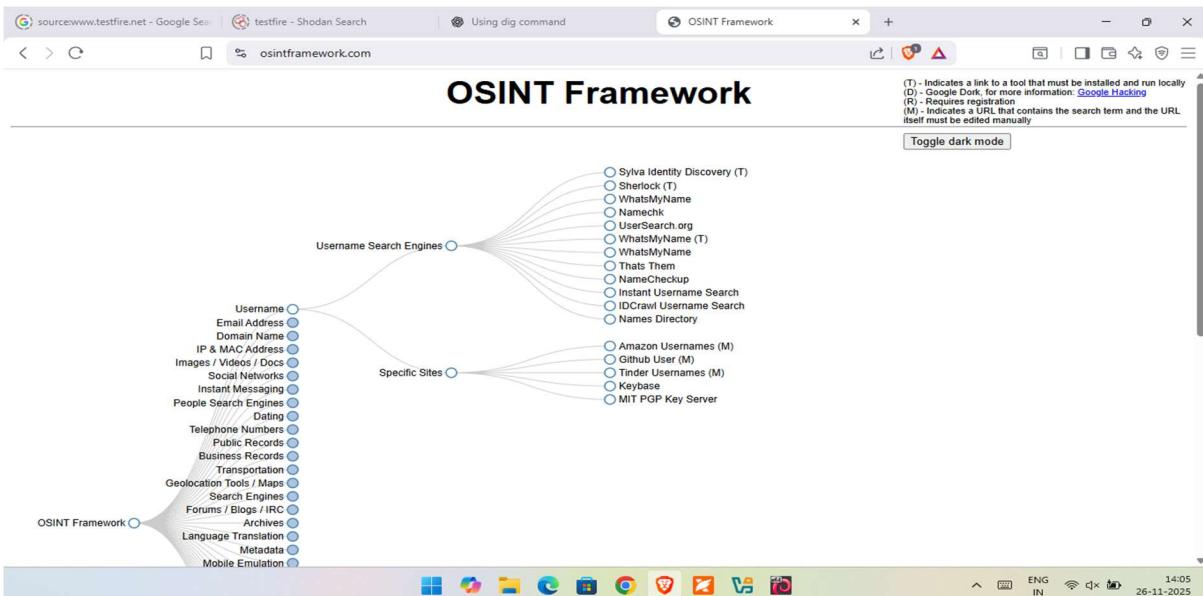


Fig.12.1- Interface of OSINT.

- Deep Result

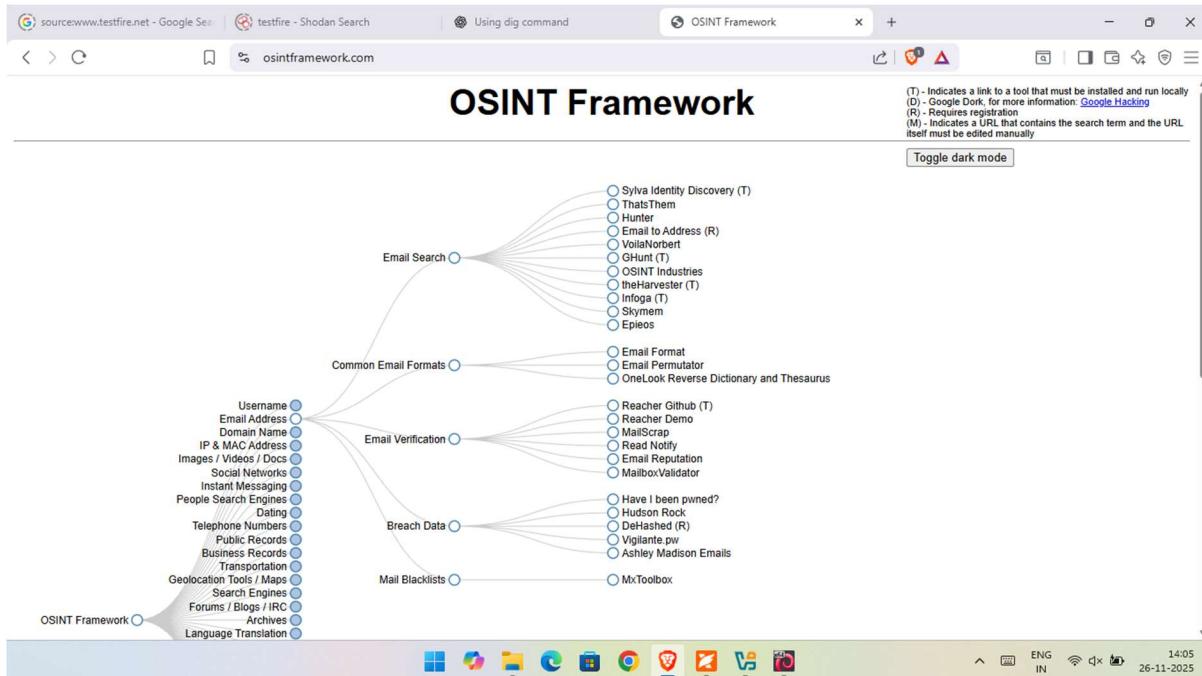


Fig.12.2 – Shows email OSINT.

- Results

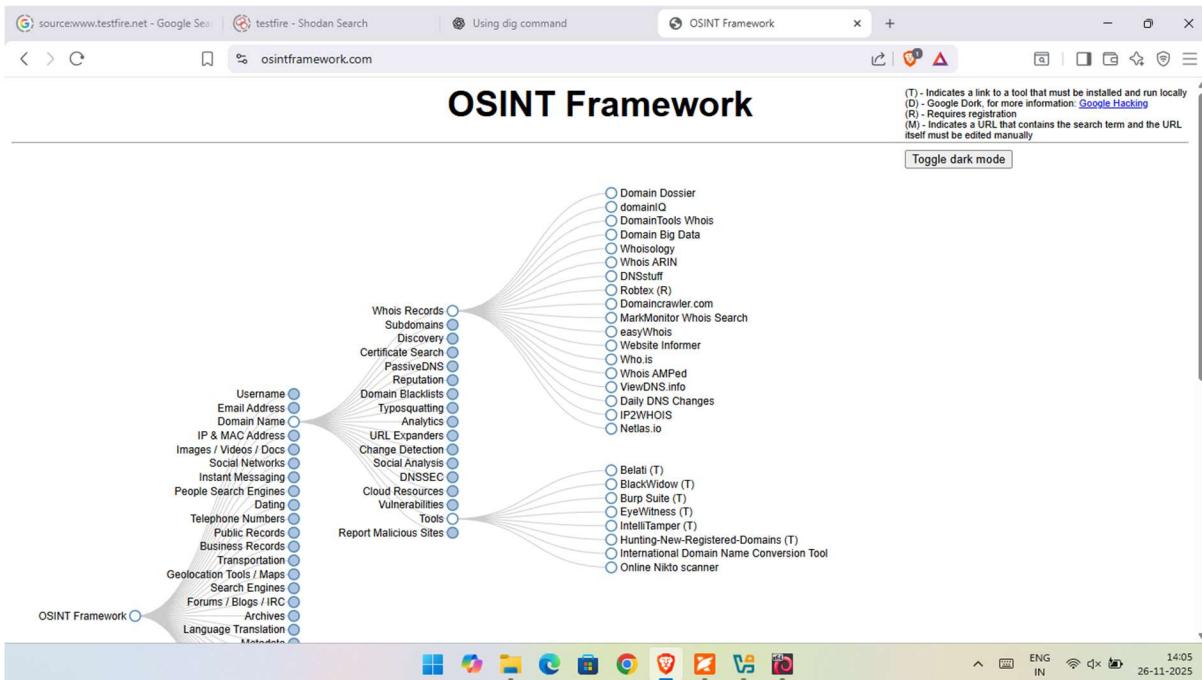


Fig.12.3- shows OSINT.

13. Footprinting Using email spider (software base tool): -

How to use it: - open the tool and in URL box give the URL of target and click on start button.

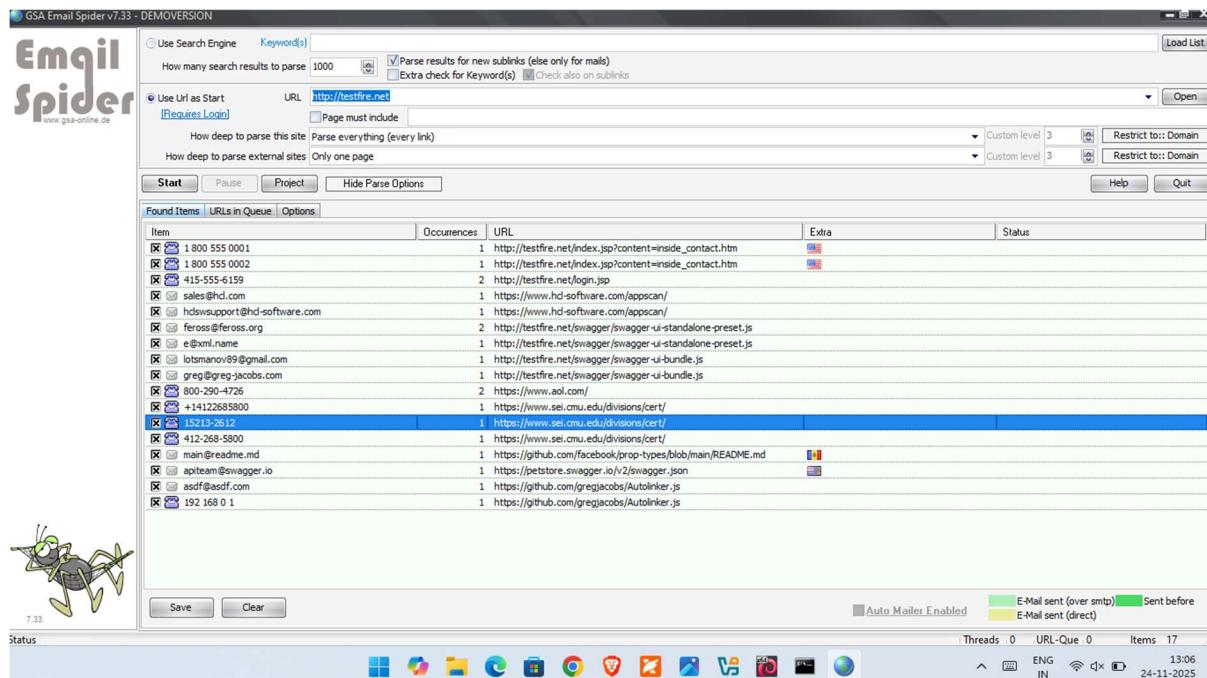


Fig.13.1- shows Email spider result.

14. Footprinting Using dig (CLI base tool): -

How to use it: - Open Kali Linux and run Terminal.

Command – dig ns certifiedhacker.com here **ns** use for find ns records.

The screenshot shows a terminal window on a Kali Linux desktop. The terminal prompt is "(root@whitewoolf-[/home/tanmay])". The user has run the command "# dig ns certifiedhacker.com". The terminal output shows the following DNS query results:

```
; <>> DiG 9.20.9-1-Debian <>> ns certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 42587
;; 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      ns1.bluehost.com.
certifiedhacker.com.    86400   IN      NS      ns2.bluehost.com.

;; Query time: 308 msec
;; SERVER: 192.168.202.184#53(192.168.202.184) (UDP)
;; WHEN: Thu Nov 27 12:08:07 IST 2025
;; MSG SIZE  rcvd: 93
```

Fig.14.1- Shows ns records.

- here using NS record transferring zone. If transfer is successful then zone transfer is completed and if that failed means dns is stopping to transfer.

```

root@whitewolf: /home/tanmay
# dig @ns1.bluehost.com certifiedhacker.com axfr
; <>> DiG 9.20.9-1-Debian <>> @ns1.bluehost.com certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
;; Transfer failed.

root@whitewolf: /home/tanmay
# dig @ns2.bluehost.com. certifiedhacker.com

; <>> DiG 9.20.9-1-Debian <>> @ns2.bluehost.com. certifiedhacker.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 23234
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;certifiedhacker.com. IN A

;; ANSWER SECTION:

```

Fig.14.2- Shows Zone transfer result.

15. Footprinting Using dnsenum (CLI base tool): -

How to use it: - Open Kali Linux and run Terminal.

Command – dnsenum -enum certifiedhacker.com it is automated tool that using this command automatically transfer the zone.

```

dnsenum VERSION:1.3.1
certifiedhacker.com

Host's addresses:
certifiedhacker.com. 14400 IN A 162.241.216.11

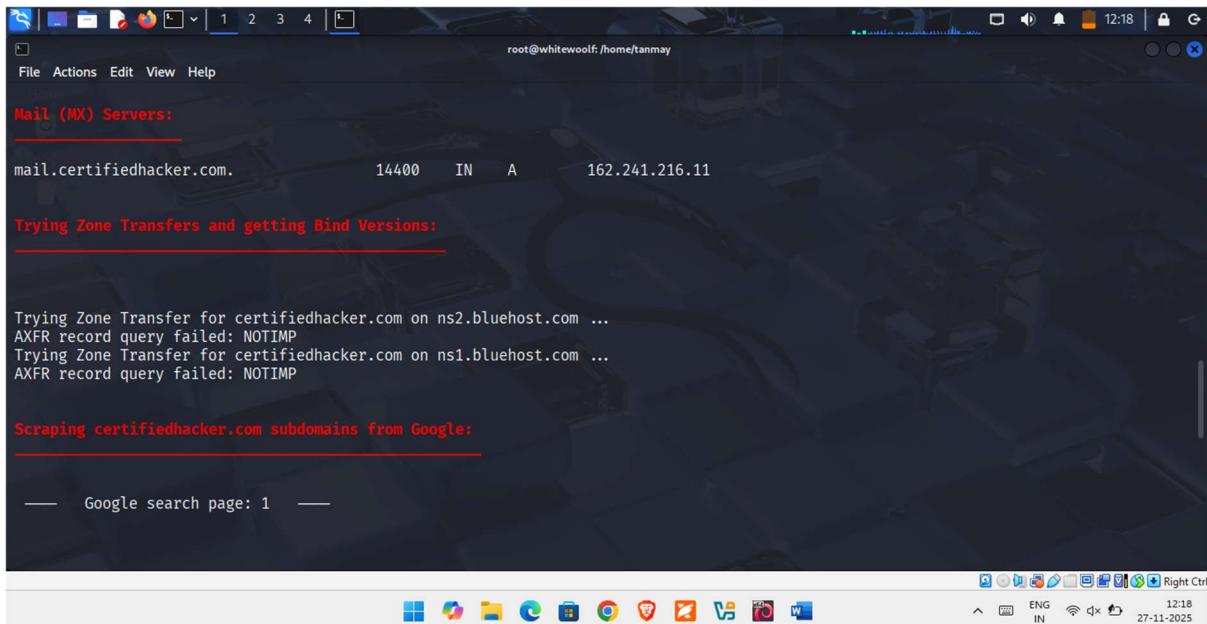
Name Servers:
ns1.bluehost.com. 2863 IN A 162.159.24.80
ns2.bluehost.com. 2863 IN A 162.159.25.175

Mail (MX) Servers:

```

Fig.15.1- Shows NS record result.

- here it started to zone transfer



The screenshot shows a terminal window on a Linux desktop environment. The terminal output is as follows:

```

root@whitewolf:/home/tanmay
File Actions Edit View Help
Mail (MX) Servers:
mail.certifiedhacker.com.      14400    IN   A      162.241.216.11

Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for certifiedhacker.com on ns2.bluehost.com ...
AXFR record query failed: NOTIMP
Trying Zone Transfer for certifiedhacker.com on ns1.bluehost.com ...
AXFR record query failed: NOTIMP

Scraping certifiedhacker.com subdomains from Google:
— Google search page: 1 —

```

The desktop taskbar at the bottom shows various application icons, and the system tray indicates the date and time as 27-11-2025.

Fig. 15.2- Shows Zone transfer result.

16. Objective

- To gather publicly available information about a target system or organization.
- To identify domains, IP addresses, network structure, and technologies used.
- To discover potential vulnerabilities, entry points, and weak security areas.
- To understand the target's attack surface before performing deeper testing.
- To support planning for scanning and penetration testing with accurate information.