

MODULE 2

FOOTPRINTING

AND

RECONNAISSANCE

Date : 21.11.2025

Name : Mugdha Makarand Govilkar

Instructor : Satish Singh

INDEX

1. Footprinting via nslookup
2. Footprinting via whois
3. Footprinting via netcraft
4. Footprinting via whatweb
5. Footprinting via dns recon
6. Footprinting via dns zonetransfer
7. Footprinting via nmap
8. Footprinting via dns dumpster
9. Footprinting via shodan.io
10. Footprinting via sherlock
11. Footprinting via subfinder
12. Footprinting via network tracerouting
13. Footprinting via recon-ng
14. Additional tools :
 - 14.1. PentestGPT
 - 14.2. OSINT Framework
 - 14.3. NapaLM FTP Indexer

Target site – testfire.net

Target ip – 65.61.137.117

1 . Footprinting via nslookup:

1 . nslookup will convert domain name into ip and ip into its domain name.

2 . When you run an nslookup command, it provides the IP address associated with a domain name or the domain name linked to an IP through reverse DNS lookup.

3 . It also allows you to retrieve DNS records like A, AAAA, MX, NS, TXT, and SOA.

1 . A Record (Address Record)

- Maps a domain name to an IPv4 address.

Example: example.com → 192.168.1.10

2 . AAAA Record (Quad-A Record)

- Maps a domain name to an IPv6 address.

Example: example.com → 2400:bb00:1234::1

3 . MX Record (Mail Exchange Record)

- Specifies which mail server handles emails for the domain.

Example: mail.example.com receives all emails for example.com.

4 . NS Record (Name Server Record)

- Shows which authoritative DNS servers host the domain's DNS records.

Example: ns1.example.com, ns2.example.com

5 . TXT Record (Text Record)

- Stores text information in DNS, often used for:

- SPF (email security)
- DKIM
- Google/Domain verifications

6 . SOA Record (Start of Authority Record)

- Contains important information about the domain's DNS zone, such as:
 - Primary name server
 - Admin email
 - Serial number of DNS records
 - Refresh/expiry timingsOverall, it defines the authority and DNS zone control for the domain.

7 . Steps :

1. open kali linux.
2. run sudo su to gain root privilege.
3. run nslookup <target name> here testfire.net to get target ip.
4. here we get the ip address as 65.61.137.117
5. close kali linux.



```
root@kali:~/home/kali
(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali)~$ nslookup testfire.net
;; communications error to 192.168.1.1#53: timed out
;; communications error to 192.168.1.1#53: timed out
;; communications error to 192.168.1.1#53: timed out
Server:         fd17:625c:f037:2::3
Address:         fd17:625c:f037:2::3#53

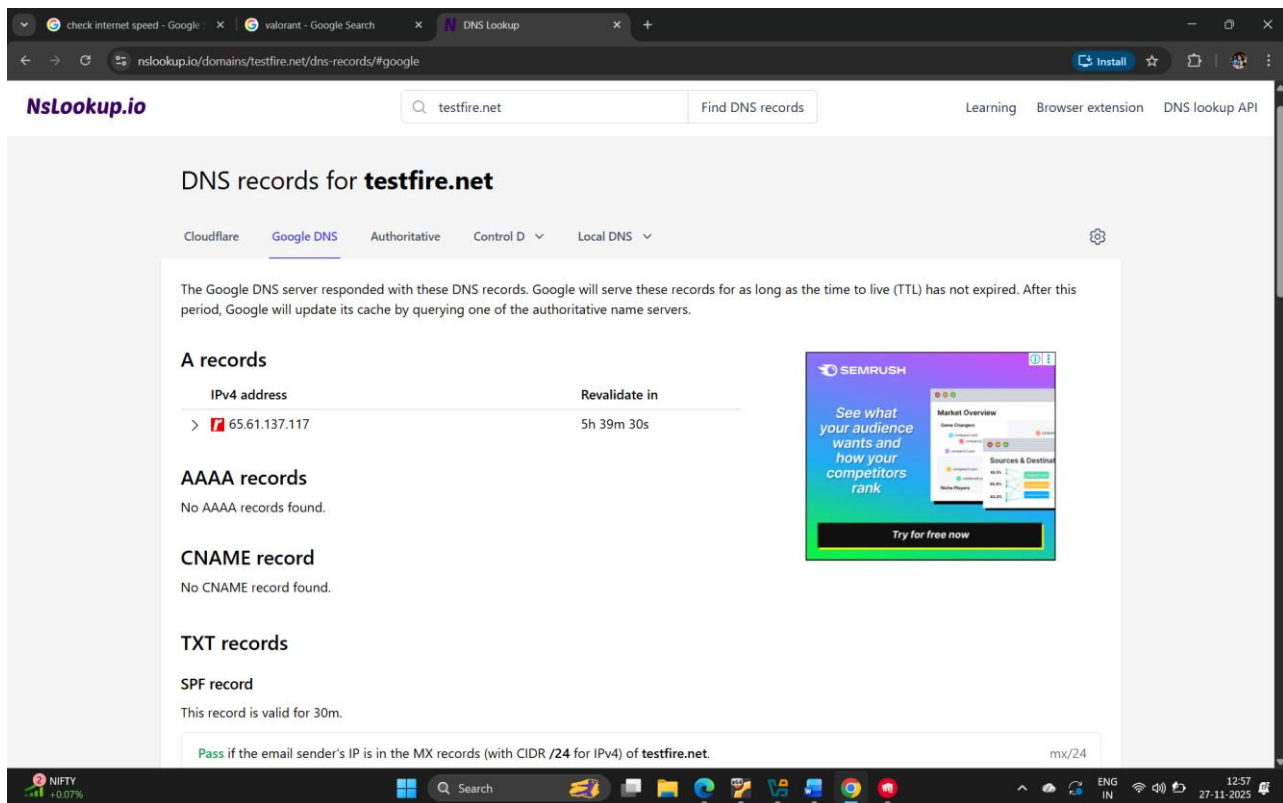
Non-authoritative answer:
Name:   testfire.net
Address: 65.61.137.117
;; communications error to 192.168.1.1#53: timed out
;; communications error to 192.168.1.1#53: timed out
;; communications error to 192.168.1.1#53: timed out
Name:   testfire.net
Address: 64:ff9b::413d:8975

(root@kali)~$ nmap 65.61.137.117
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 02:28 EST
Nmap scan report for 65.61.137.117
Host is up (0.026s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 26.86 seconds

(root@kali)~$
```

1.1



1.2

2 . Footprinting via whois :

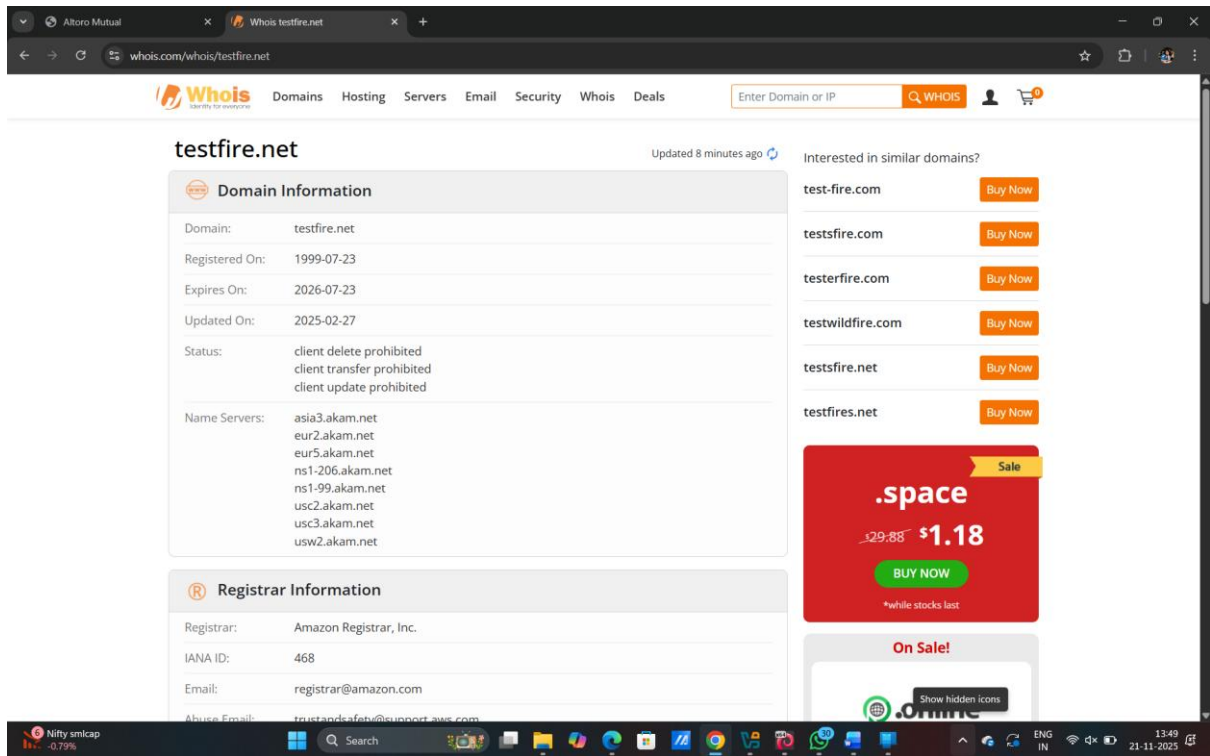
1 . whois is an important information-gathering tool used to retrieve details about a domain name or IP address, such as the owner, registrar, registration/expiry dates, contact information, and name servers.

2 . It helps in verifying domain ownership, identifying administrative contacts, investigating suspicious domains, and performing OSINT during cybersecurity assessments.

3 . Overall, WHOIS provides transparency and aids in troubleshooting, security analysis, and understanding the background of any domain.

4 . Steps :

1. open browser.
2. run whois.com then search testfire.net.
3. Result includes registration details,name servers,ip address,location.
4. Close browser.



3 . footprinting via netcraft:

1 . Netcraft helps stop these threats by detecting and blocking malicious websites. 2 . It also gives you detailed information about the target. it gives ipv4 address, Owner name, hosting country.

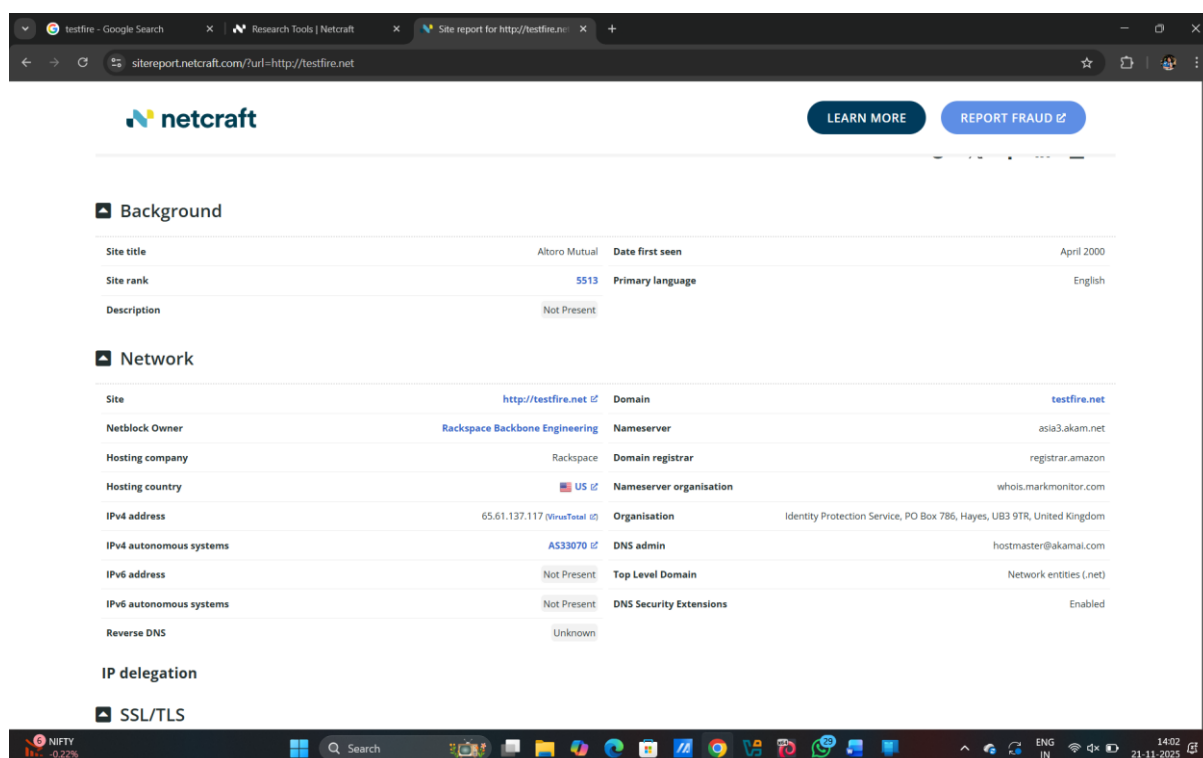
3 . Netcraft is used to gather detailed information about websites for security analysis, OSINT, and reconnaissance. It helps you find:

- Hosting details (where the website is hosted)
- Server technology (Apache, Nginx, IIS, etc.)
- Operating system
- SSL/TLS certificate details
- Domain history (previous owners, hosting changes)
- Site rank and traffic estimation
- Potential vulnerabilities or outdated software
- Cybersecurity professionals use Netcraft to understand a website's infrastructure, check for security risks, and track phishing or malicious domains.

4 . Steps :

1. open browser.

2. run netcraft.com then search testfire.net in the website's search bar.
3. in the result we get netblock owner,hosting company,hosting country,ipv4 address,ipv4 autonomous system.site rank,site title,name server,nameserver organisation,dns admin
4. close browser.



4 . footprinting via whatweb :

- 1 . Whatweb gives information about the services which are running on the target website.
- 2 . WhatWeb is a web reconnaissance tool used to identify technologies used by a website.
- 3 . It tells you what a website is built with by fingerprinting its components.

- For OSINT and reconnaissance
- To understand a website's technology stack
- To identify potential vulnerabilities (e.g., outdated versions)
- To gather information before a penetration test
- Quick tech fingerprinting for cybersecurity assessments

4 . Steps :

1. open kali linux.
2. run whatweb <http://testfire.net>
3. It gives result such as server name,cookies,country,HTTP server,ip,title,language.
4. Close kali linux.

```
root@kali: /home/kali
Session Actions Edit View Help
Address: fd17:625c:f037:2::3#53

Non-authoritative answer:
Name: testfire.net
Address: 65.61.137.117
;; communications error to 192.168.1.1#53: timed out
;; communications error to 192.168.1.1#53: timed out
;; communications error to 192.168.1.1#53: timed out
Name: testfire.net
Address: 64:ff9b::413d:8975

root@kali) - /home/kali
# nmap 65.61.137.117
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 02:28 EST
Nmap scan report for 65.61.137.117
Host is up (0.026s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 26.86 seconds

root@kali) - /home/kali
# whatweb http://testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STATES][US], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], IP[65.61.137.117], Java, Title[Altoro Mutual]

root@kali) - /home/kali
#
```

5 . footprinting using dnsrecon :

1 . dnsrecon is a powerful DNS enumeration tool used to gather detailed information about a domain's DNS infrastructure.

2 .It helps penetration testers and cybersecurity analysts collect DNS-related data for reconnaissance and security assessments.

3 . What DNSRecon is used for :

- **DNS Enumeration**
Collects records like A, AAAA, MX, NS, SOA, TXT, SRV, CNAME, PTR, etc.
- **Brute Forcing Subdomains**
Discovers hidden or unlisted subdomains.
- **Reverse Lookup**
Finds domains linked to an IP range.
- **Zone Transfer Testing**
Checks if DNS zone transfer (AXFR) is misconfigured, which can leak sensitive info.
- **Wildcard DNS Detection**
Identifies if wildcard entries are present.
- **Checking for DNS Misconfigurations**
Helps detect vulnerabilities in DNS setup.

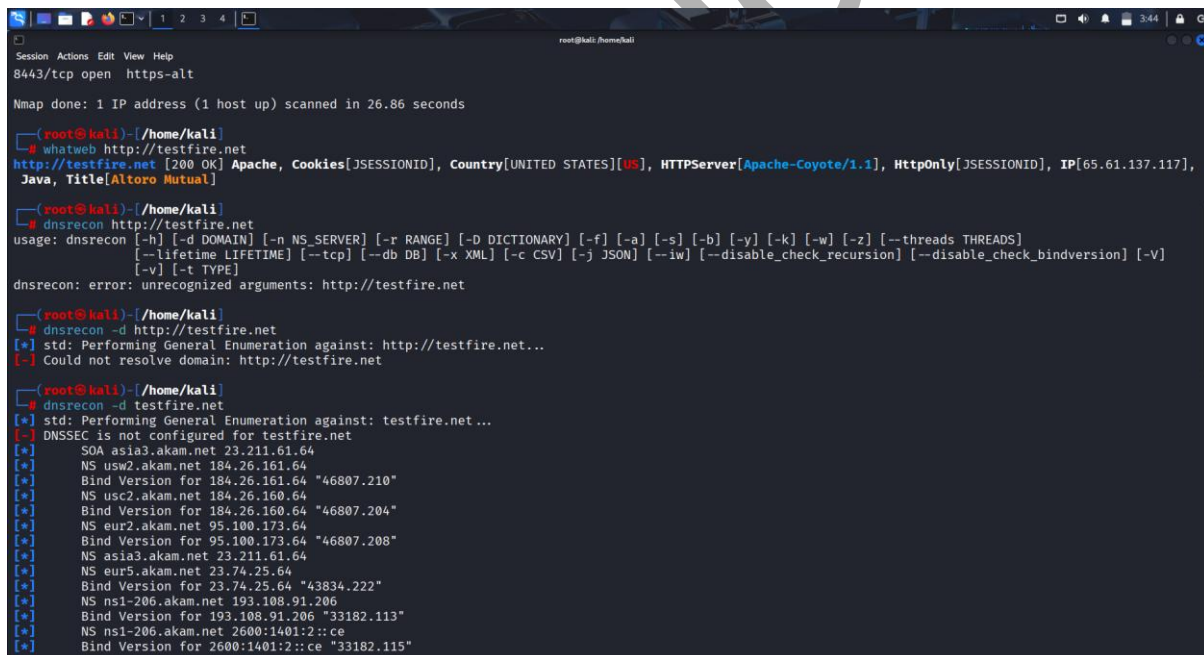
- **Gathering DNS Topology**
Helps understand how a domain is structured and managed.

4 . Why it is used :

- For reconnaissance in penetration testing
- To identify security weaknesses in DNS
- To discover subdomains and infrastructure
- To perform OSINT on a target domain

5 . Steps :

1. Open kali linux
2. run `dnsrecon -d http://testfire.net` in kali linux, -d flag is used to specify the target name
3. It gives result about A Record Domain resolves to 65.61.137.117, NS Records uses DNSMadeEasy name servers, SOA Shows-zone authority, serial number, and admin email
4. Close kali linux



```

root@kali:~/home/kali
Session Actions Edit View Help
8443/tcp open https-alt

Nmap done: 1 IP address (1 host up) scanned in 26.86 seconds

root@kali:~/home/kali
# whatweb http://testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STATES][US], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], IP[65.61.137.117], Java, Title[Altoro Mutual]

root@kali:~/home/kali
# dnsrecon http://testfire.net
usage: dnsrecon [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY] [-f] [-s] [-b] [-y] [-k] [-w] [-z] [--threads THREADS]
               [--lifetime LIFETIME] [--tcp] [--db DB] [-x XML] [-c CSV] [-j JSON] [--iw] [--disable_check_recursion] [--disable_check_bindversion] [-v]
               [-v] [-t TYPE]
dnsrecon: error: unrecognized arguments: http://testfire.net

root@kali:~/home/kali
# dnsrecon -d http://testfire.net
[*] std: Performing General Enumeration against: http://testfire.net...
[-] Could not resolve domain: http://testfire.net

root@kali:~/home/kali
# dnsrecon -d testfire.net
[*] std: Performing General Enumeration against: testfire.net...
[-] DNSSEC is not configured for testfire.net
[*] SOA asia3.akam.net 23.211.61.64
[*] NS usw2.akam.net 184.26.161.64
[*] Bind Version for 184.26.161.64 "46807.210"
[*] NS usc2.akam.net 184.26.160.64
[*] Bind Version for 184.26.160.64 "46807.204"
[*] NS eur2.akam.net 95.100.173.64
[*] Bind Version for 95.100.173.64 "46807.208"
[*] NS asia3.akam.net 23.211.61.64
[*] NS eur5.akam.net 23.74.25.64
[*] Bind Version for 23.74.25.64 "43834.222"
[*] NS ns1-206.akam.net 193.108.91.206
[*] Bind Version for 193.108.91.206 "33182.113"
[*] NS ns1-206.akam.net 2600:1401:2::ce
[*] Bind Version for 2600:1401:2::ce "33182.115"

```

6 . footprinting via dns zonetransfer:

1 . dns zonetransfer allows you to pull down all the dns records of a domain its typically meant for dns server to replicate data but when misconfured it can be used to steal a domains entire DNS record.

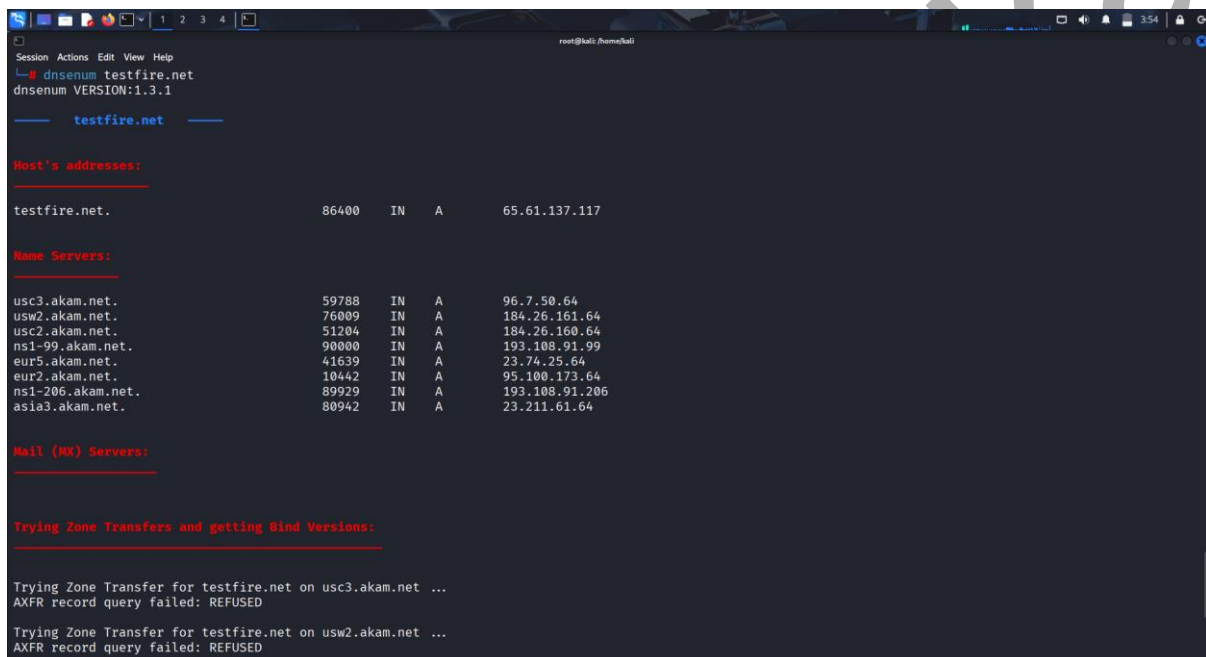
2 . DNS zone transfer is the process of copying DNS zone data from a primary (authoritative) server to secondary servers for redundancy and fault tolerance. This allows secondary servers to

serve DNS requests if the primary server becomes unavailable and ensures that the data is synchronized across the server infrastructure

3 . here we use dnsenum tool.

4 . Steps :

1. Open kali linux
2. Run dnsenum testfire.net
3. It gives result about host addresses,name servers,tries zone transfer but here result is query failed it means it is secure.
4. Close kali linux.



```
root@kali: /home/kali
Session Actions Edit View Help
└─ # dnsenum testfire.net
dnsenum VERSION:1.3.1

┌─── testfire.net ───┐

Host's addresses:

testfire.net.                86400    IN      A       65.61.137.117

Name Servers:

usc3.akam.net.               59788    IN      A       96.7.50.64
usw2.akam.net.               76009    IN      A       184.26.161.64
usc2.akam.net.               51204    IN      A       184.26.160.64
ns1-99.akam.net.             90000    IN      A       193.108.91.99
eur5.akam.net.               41639    IN      A       23.74.25.64
eur2.akam.net.               10442    IN      A       95.100.173.64
ns1-206.akam.net.            89929    IN      A       193.108.91.206
asia3.akam.net.              80942    IN      A       23.211.61.64

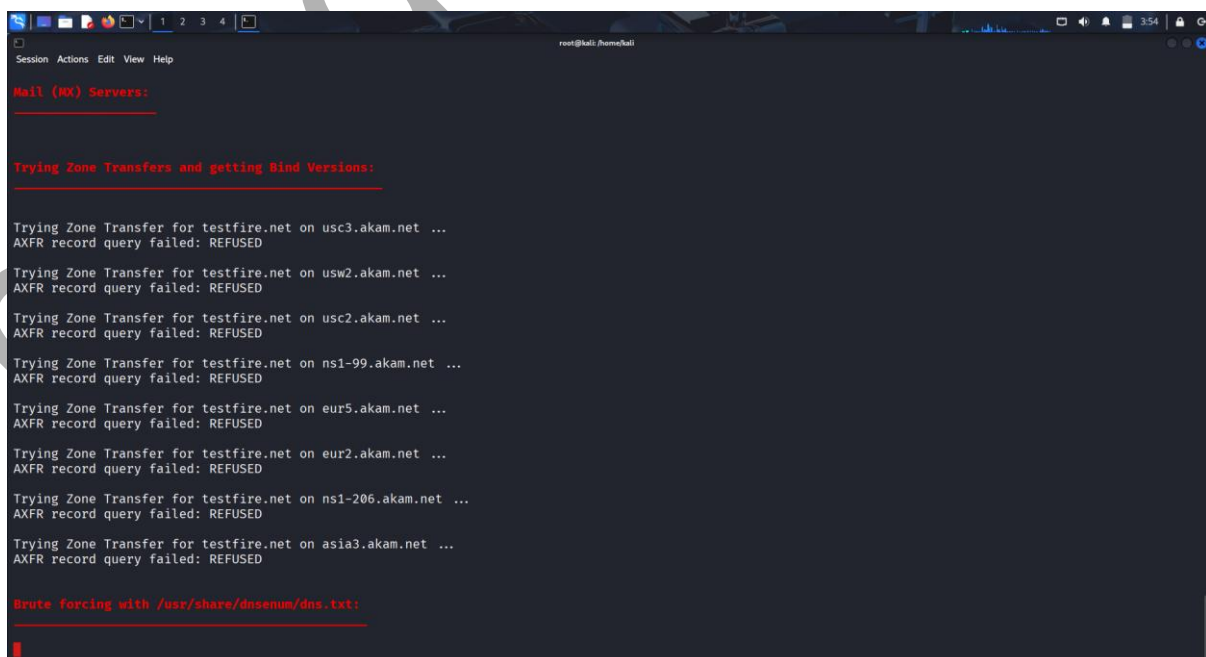
Mail (MX) Servers:

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for testfire.net on usc3.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for testfire.net on usw2.akam.net ...
AXFR record query failed: REFUSED
```

1.1



```
Mail (MX) Servers:

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for testfire.net on usc3.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for testfire.net on usw2.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for testfire.net on usc2.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for testfire.net on ns1-99.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for testfire.net on eur5.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for testfire.net on eur2.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for testfire.net on ns1-206.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for testfire.net on asia3.akam.net ...
AXFR record query failed: REFUSED

Brute forcing with /usr/share/dnsenum/dns.txt:
```

1.2

7 . footprinting via nmap :

1 . nmap means network mapping which gives information about open,filtered and closed ports about the target .

2 . it actively footprints the target.

3 . nmap is a powerful network scanning tool used to discover hosts, services, and vulnerabilities in a network.

4 . Host Discovery

Identifies which devices are active on a network.

(Eg: online/offline systems)

5 . Port Scanning

Finds open, closed, or filtered ports on a target.

(Eg: 80, 443, 22, 3389, etc.)

6 . Service & Version Detection

Detects which services are running and their versions.

(Eg: Apache 2.4.6, SSH 7.9)

7 . Operating System Detection

Identifies the OS of the target system.

(Eg: Linux, Windows, FreeBSD)

8 . Vulnerability Scanning (with NSE)

Nmap Scripting Engine (NSE) can check for:

- **Weak passwords**
- **Misconfigurations**
- **Known vulnerabilities**
- **Dangerous services**

9 . Network Mapping

Gives a clear structure of network layout.

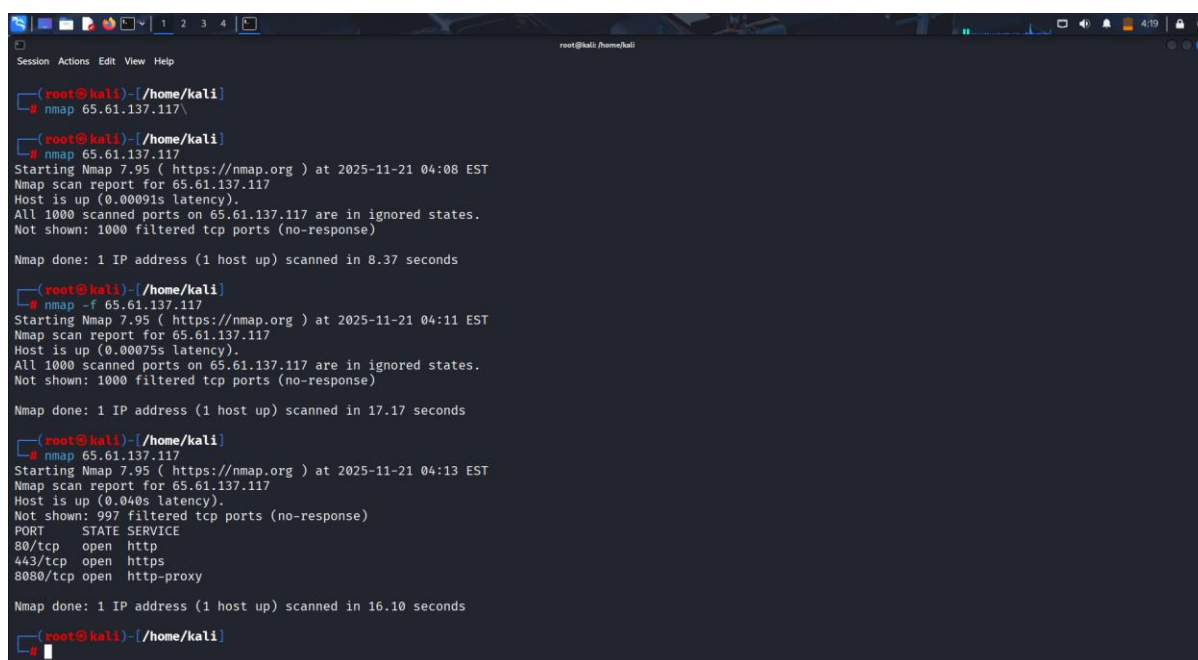
10 . Firewall & Security Testing

Helps identify firewall rules and packet filtering.

10 .Steps :

- 1. Open kali linux.**
- 2. Run nmap <ip> 65.61.137.117**

3. It gives result about host's condition like open,close,filtered,unfiltered.up,down.
4. Close kali linux.



```
root@kali: /home/kali
root@kali)~# nmap 65.61.137.117
root@kali)~# nmap 65.61.137.117
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 04:08 EST
Nmap scan report for 65.61.137.117
Host is up (0.00091s latency).
All 1000 scanned ports on 65.61.137.117 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 8.37 seconds
root@kali)~# nmap -f 65.61.137.117
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 04:11 EST
Nmap scan report for 65.61.137.117
Host is up (0.00075s latency).
All 1000 scanned ports on 65.61.137.117 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 17.17 seconds
root@kali)~# nmap 65.61.137.117
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 04:13 EST
Nmap scan report for 65.61.137.117
Host is up (0.040s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
Nmap done: 1 IP address (1 host up) scanned in 16.10 seconds
root@kali)~#
```

8 . footprinting via dnsdumpster :

- 1 . it is a web-based tool used for DNS recon and mapping an organization's public digital footprint.
- 2 . It gathers publicly available DNS information
- 3 . DNSdumpster is an online DNS recon tool used to gather information about a domain's DNS infrastructure and discover its subdomains.
- 4 . What DNSdumpster is used for:

1. Subdomain Discovery

Finds publicly visible subdomains of a target domain.

2. DNS Records Enumeration

Shows important DNS records like:

- A
- MX
- NS
- TXT
- SOA

- **CNAME**

3. Mapping Infrastructure

Provides a visual network map showing:

- **Subdomains**
- **Hostnames**
- **IP addresses**
- **Associated services**

4. Identifying Hosting Providers

Shows where websites or services are hosted (cloud, on-premises, CDN, etc.)

5. Finding Potential Attack Surface

Subdomains may expose:

- **Login portals**
- **Admin panels**
- **Development servers**
- **Test/staging environments**

Useful for penetration testing and OSINT.

6. Checking DNS Configurations

Helps identify misconfigurations or outdated DNS entries.

7 . Steps :

- 1. Open browser**
- 2. Run dnsdumpster in search bar,then run target site name testfire.net in the dnsdumpster's search bar**
- 3. It gives result about A record,MX record,NS record,open services,ip**
- 4. Close the browser.**

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
demo.testfire.net	65.61.137.117	ASN 33070 65.61.136.0/22	RMI-14 United States	Http: Apache-Coyote/1.1 title: Altoro Mutual tech: Apache Tomcat Java Https: Apache-Coyote/1.1 title: Altoro Mutual on demo.testfire.net Https: Apache-Coyote/1.1 title: Altoro Mutual tech: Apache Tomcat Java	22

MX Records					
NS Records					
usw2.akam.net	184.26.161.64 a14-64.akam.net	ASN 21342 184.26.161.0/24	AKAMAI-ASN2, NL United States		
usc2.akam.net	184.26.160.64 a12-64.akam.net	ASN 21342 184.26.160.0/24	AKAMAI-ASN2, NL United States		
eur5.akam.net	23.74.25.64 a20-64.akam.net	ASN 21342 23.74.25.0/24	AKAMAI-ASN2, NL United States		
usc3.akam.net	96.7.50.64 a10-64.akam.net	ASN 21342 96.7.50.0/24	AKAMAI-ASN2, NL United States		
ns1-206.akam.net	193.108.91.206 ns1-206.akam.net	ASN 21342	AKAMAI-ASN2, NL		

1.1

NS Records					
usw2.akam.net	184.26.161.64 a14-64.akam.net	ASN 21342 184.26.161.0/24	AKAMAI-ASN2, NL United States		
usc2.akam.net	184.26.160.64 a12-64.akam.net	ASN 21342 184.26.160.0/24	AKAMAI-ASN2, NL United States		
eur5.akam.net	23.74.25.64 a20-64.akam.net	ASN 21342 23.74.25.0/24	AKAMAI-ASN2, NL United States		
usc3.akam.net	96.7.50.64 a10-64.akam.net	ASN 21342 96.7.50.0/24	AKAMAI-ASN2, NL United States		
ns1-206.akam.net	193.108.91.206 ns1-206.akam.net	ASN 21342	AKAMAI-ASN2, NL The Netherlands		
ns1-99.akam.net	193.108.91.99 a1-99.akam.net	ASN 21342 193.108.91.0/24	AKAMAI-ASN2, NL The Netherlands		
eur2.akam.net	95.100.173.64 eur2.akam.net	ASN 21342 95.100.173.0/24	AKAMAI-ASN2, NL The Netherlands		
asia3.akam.net	23.211.61.64 asia3.akam.net	ASN 21342 23.211.61.0/24	AKAMAI-ASN2, NL United States		

TXT Records	
\"v=spf1 mx/24 -all\"	

Download xlsx

1.2

9 . footprinting via shodan.io:

1 . Shodan is a search engine for Internet-connected devices.

2 . Unlike Google (which searches websites), Shodan scans the entire internet and shows devices and services that are publicly accessible

3 . uses :

1. Discovering Exposed Devices

Finds devices connected to the internet like:

- **Cameras**
- **Routers**
- **Servers**
- **Databases**
- **SCADA/ICS systems**
- **IoT devices**

2. Finding Open Ports & Services

Shows which ports are open and what services are running.

3. Vulnerability Detection

Identifies systems vulnerable to:

- **CVEs**
- **Weak configurations**
- **Outdated software**

4. Checking Security Exposure

Used to see if your organization has:

- **Misconfigured servers**
- **Open ports**
- **Leaked services**
- **Unsafe IoT devices**

5. Gathering Technical Information

Provides details like:

- **OS**
- **Web server versions**
- **SSL certificates**

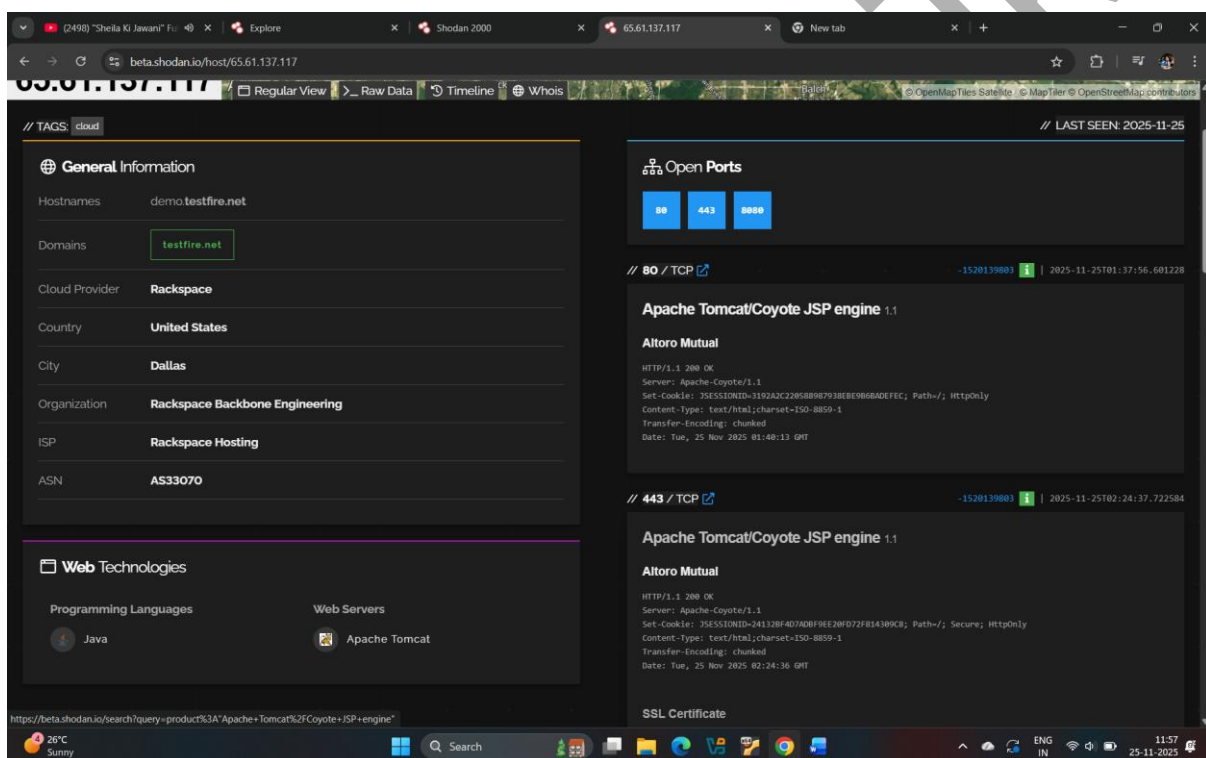
- Banners

6. OSINT & Reconnaissance

Used heavily in penetration testing to gather info before attacks.

7 Steps :

1. Open browser
2. Run shodan.io
3. Run testfire.net in shodan.io's search bar
4. It gives result about website technology, open port, web server, country, city, organisation
5. Close browser.



10 . footprinting via sherlock:

1 . Sherlock is an open-source tool used to find usernames across social media platforms and websites.

2 . You give a username, and Sherlock checks hundreds of platforms (Facebook, Instagram, Twitter, GitHub, LinkedIn, TikTok, gaming sites, forums, etc.) to see if that username exists or is registered there.

3 . Steps :

1. Open kali linux

2. Run sherlock <name of site, person name> here aniketpagare
3. It checks the username on all the sites where it was registered.
4. Close kali linux.

```

root@kali: /home/mugdha # sherlock aniketpagare
Update available! 0.15.0 -> 0.16.0
https://github.com/sherlock-project/sherlock/releases/tag/v0.16.0
[*] Checking username aniketpagare on:

[*] Academia.edu: https://independent.academia.edu/aniketpagare
[*] AllMyLinks: https://allmylinks.com/aniketpagare
[*] Archive.org: https://archive.org/details/aniketpagare
[*] Behance: https://www.behance.net/aniketpagare
[*] Chess: https://www.chess.com/member/aniketpagare
[*] Coders Rank: https://profile.codersrank.io/user/aniketpagare/
[*] Discord: https://discord.com
[*] Envato Forum: https://forums.envato.com/u/aniketpagare
[*] Flipboard: https://flipboard.com/@aniketpagare
[*] Freelancer: https://www.freelancer.com/u/aniketpagare
[*] Gnome VCS: https://gitlab.gnome.org/aniketpagare
[*] GitHub: https://www.github.com/aniketpagare
[*] Gumroad: https://www.gumroad.com/aniketpagare
[*] HackenProof (hackers): https://hackenproof.com/hackers/aniketpagare
[*] LibraryThing: https://www.librarything.com/profile/aniketpagare
[*] NationStates: https://nationstates.net/nation-aniketpagare
[*] NationStates Region: https://nationstates.net/region-aniketpagare
[*] Patched: https://patched.sh/user/aniketpagare
[*] SlideShare: https://slideshare.net/aniketpagare
[*] Smule: https://www.smule.com/aniketpagare
[*] Snapchat: https://www.snapchat.com/add/aniketpagare
[*] Solica: https://solica.com/aniketpagare
[*] Spotify: https://open.spotify.com/user/aniketpagare
[*] TradingView: https://www.tradingview.com/u/aniketpagare/
[*] Trello: https://trello.com/aniketpagare
[*] Typeracer: https://data.typeracer.com/pit/profile?user-aniketpagare
[*] VSCO: https://vscocdn.com/aniketpagare
[*] Wattpad: https://www.wattpad.com/user/aniketpagare
[*] Weblate: https://hosted.weblate.org/user/aniketpagare/
[*] YandexMusic: https://music.yandex/users/aniketpagare/playlists
[*] Dailymotion: https://www.dailymotion.com/user/aniketpagare
[*] Mashedin: https://mashedin.cloud/aniketpagare
[*] PkgPU: https://php.ru/forum/members/username-aniketpagare
[*] Pinterest: https://www.pinterest.com/aniketpagare/
[*] Vaidhok: https://www.vaidhok.ru/user/aniketpagare
[*] BabyRu: https://www.baby.ru/u/aniketpagare

[*] Search completed with 36 results
root@kali: /home/mugdha #

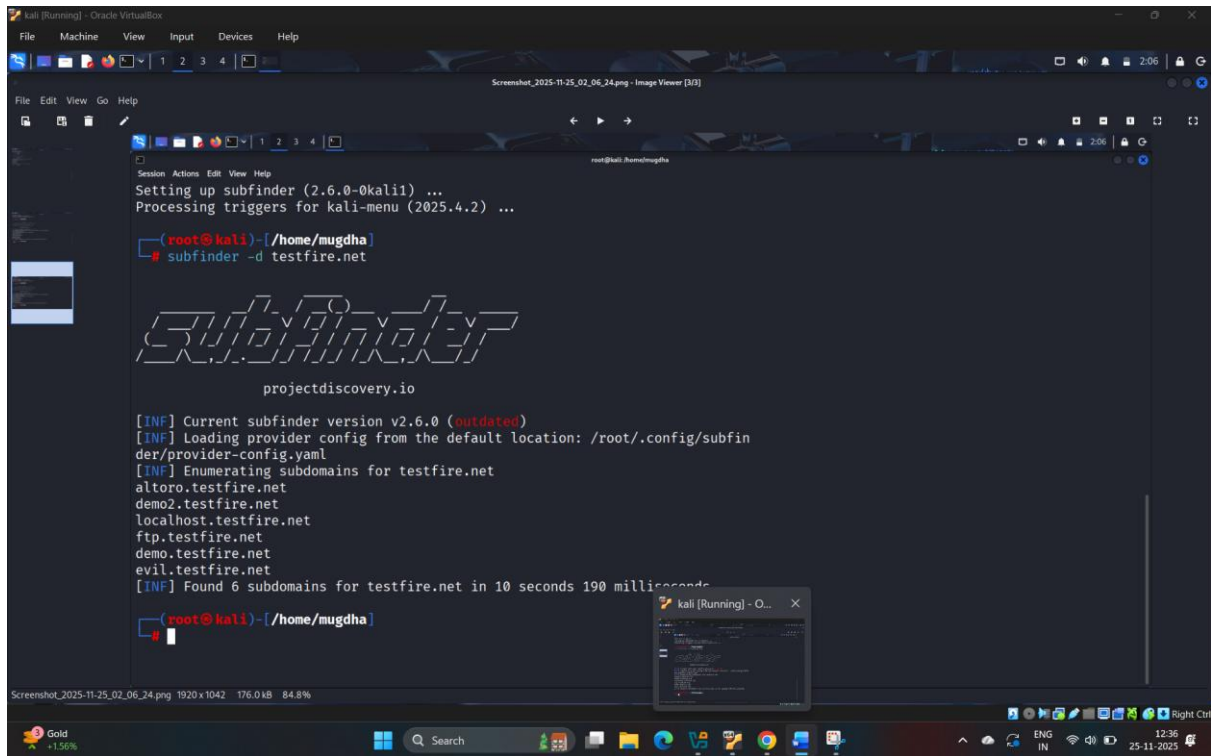
```

11 . subfinder:

- 1 . Subfinder is a popular OSINT and recon tool used in cyber security to find subdomains of a target domain.
- 2 . It is developed by ProjectDiscovery and is widely used during penetration testing, bug bounty hunting, and attack surface mapping

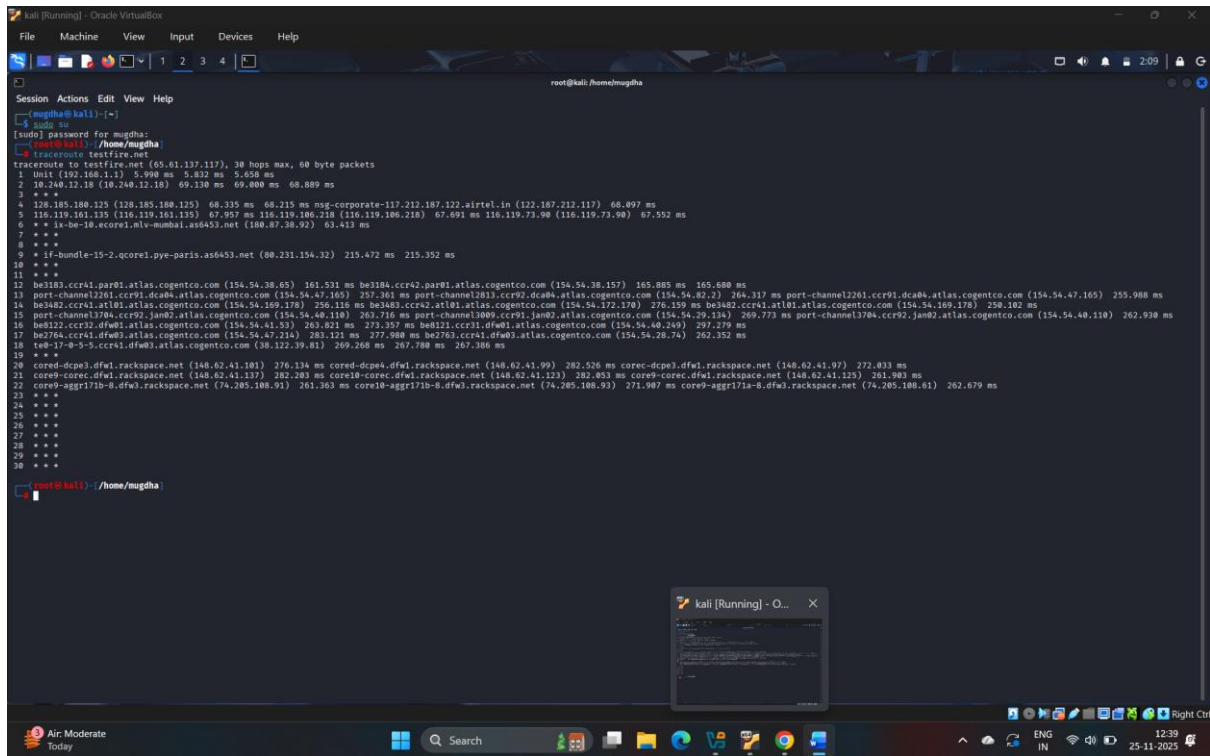
3 . Steps :

1. Open kali linux
2. Run subfinder -d testfire.net
3. It gives result about subdomain here
altoro.testfire.net,demo2.testfire.net,localhost.testfire.net,ftp.testfire.net,demo.testfire.net,evil.testfire.net.
4. Close kali linux.



12 . footprinting via network tracerouting:

- 1 . Network tracerouting is used to trace the path (hops) a packet takes to reach a destination (website or IP).
- 2 . It helps in network troubleshooting, OSINT, pentesting, and mapping network infrastructure.
- 3 . * means no response received from that hop
- 4 . Steps :
 1. Open kali linux.
 2. Run `tracert testfire.net`
 3. It gives information about the path testfire.net's packets uses to reach destination.
 4. Close kali linux.



```
kali [Running] - O...
root@kali: /home/mugdha
Session Actions Edit View Help
root@kali: /home/mugdha
root@kali:~# sudo su
[sudo] password for mugdha:
root@kali:~# tracert testfire.net
Traceroute to testfire.net (65.61.137.117), 30 hops max, 60 byte packets
 1  * * *
 2  10.240.12.18 (10.240.12.18) 69.130 ms 69.000 ms 68.889 ms
 3  * * *
 4  128.185.180.125 (128.185.180.125) 68.335 ms 68.215 ms msg-corporate-117-212-187-122.airtel.in (122.187.212.117) 68.097 ms
 5  116.119.161.135 (116.119.161.135) 67.957 ms 116.119.186.218 (116.119.186.218) 67.691 ms 116.119.73.90 (116.119.73.90) 67.352 ms
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  be3183.ccr01.par01.atlas.cogentco.com (154.54.38.65) 161.531 ms be3184.ccr42.par01.atlas.cogentco.com (154.54.38.157) 165.885 ms 165.680 ms
13  port-channel2261.ccr91.dca04.atlas.cogentco.com (154.54.47.165) 257.361 ms port-channel2813.ccr92.dca04.atlas.cogentco.com (154.54.82.2) 264.317 ms port-channel2261.ccr91.dca04.atlas.cogentco.com (154.54.47.165) 255.988 ms
14  be3482.ccr01.atl01.atlas.cogentco.com (154.54.169.178) 256.116 ms be3483.ccr42.atl01.atlas.cogentco.com (154.54.172.170) 276.159 ms be3482.ccr01.atl01.atlas.cogentco.com (154.54.169.178) 250.102 ms
15  port-channel3784.ccr92.jam02.atlas.cogentco.com (154.54.40.110) 263.716 ms port-channel3809.ccr91.jam02.atlas.cogentco.com (154.54.29.134) 269.773 ms port-channel3784.ccr92.jam02.atlas.cogentco.com (154.54.40.110) 262.930 ms
16  be8122.ccr32.dfw01.atlas.cogentco.com (154.54.41.53) 263.821 ms 273.357 ms be8121.ccr31.dfw01.atlas.cogentco.com (154.54.40.749) 297.279 ms
17  be2764.ccr01.dfw03.atlas.cogentco.com (154.54.47.214) 283.121 ms 277.988 ms be2763.ccr31.dfw03.atlas.cogentco.com (154.54.28.74) 262.352 ms
18  te0-17-0-5.ccr01.dfw03.atlas.cogentco.com (38.122.39.81) 269.268 ms 267.780 ms 267.386 ms
19  * * *
20  core0-dcp3.dfw1.rackspace.net (148.62.41.101) 276.134 ms core0-dcp4.dfw1.rackspace.net (148.62.41.99) 282.526 ms core0-dcp3.dfw1.rackspace.net (148.62.41.07) 272.833 ms
21  core9-corec.dfw1.rackspace.net (148.62.41.137) 282.283 ms core10-corec.dfw1.rackspace.net (148.62.41.123) 282.853 ms core9-corec.dfw1.rackspace.net (148.62.41.125) 261.983 ms
22  core9-aggr171b-0.dfw0.rackspace.net (74.205.180.91) 261.363 ms core10-aggr171b-0.dfw0.rackspace.net (74.205.180.92) 271.907 ms core9-aggr171a-0.dfw0.rackspace.net (74.205.180.61) 262.679 ms
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

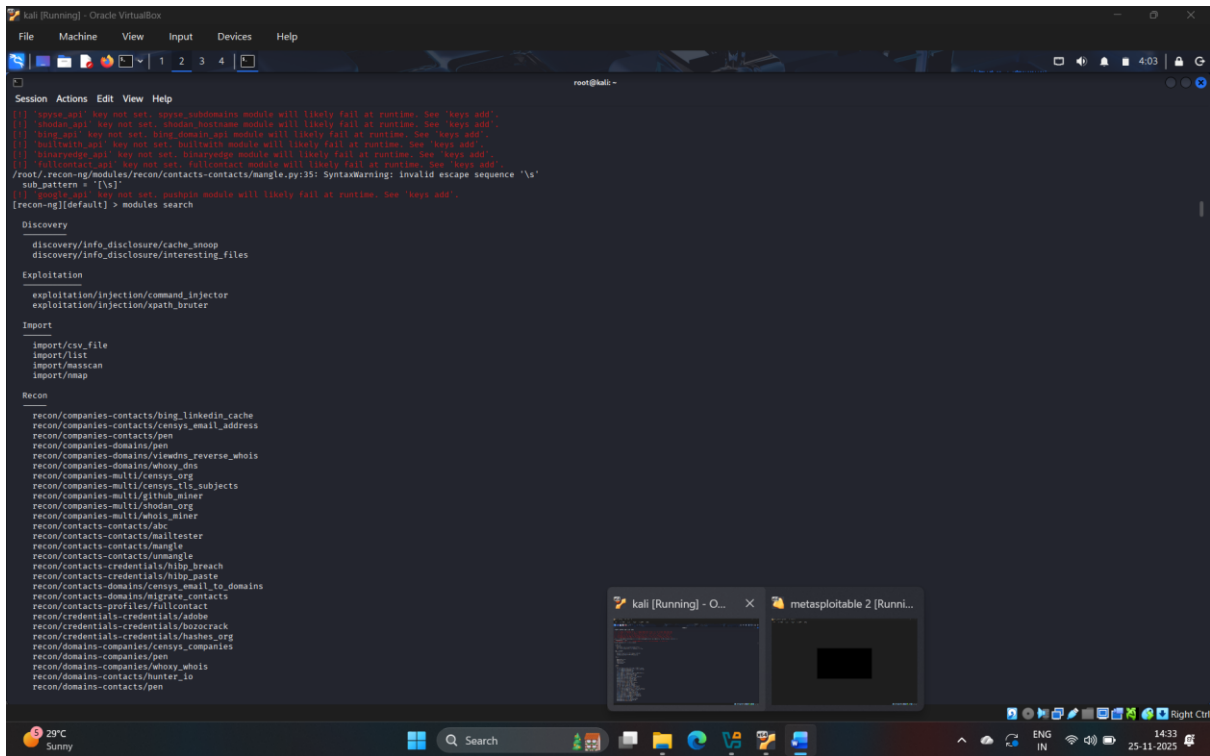
13 . recon-ng:

1 . It is used to gather information about targets such as domains, companies, people, IP addresses, emails, and social media profiles.

2 . In Recon-ng, the "record not found" message means that the module you are running did not find any relevant information for the given target during its execution.

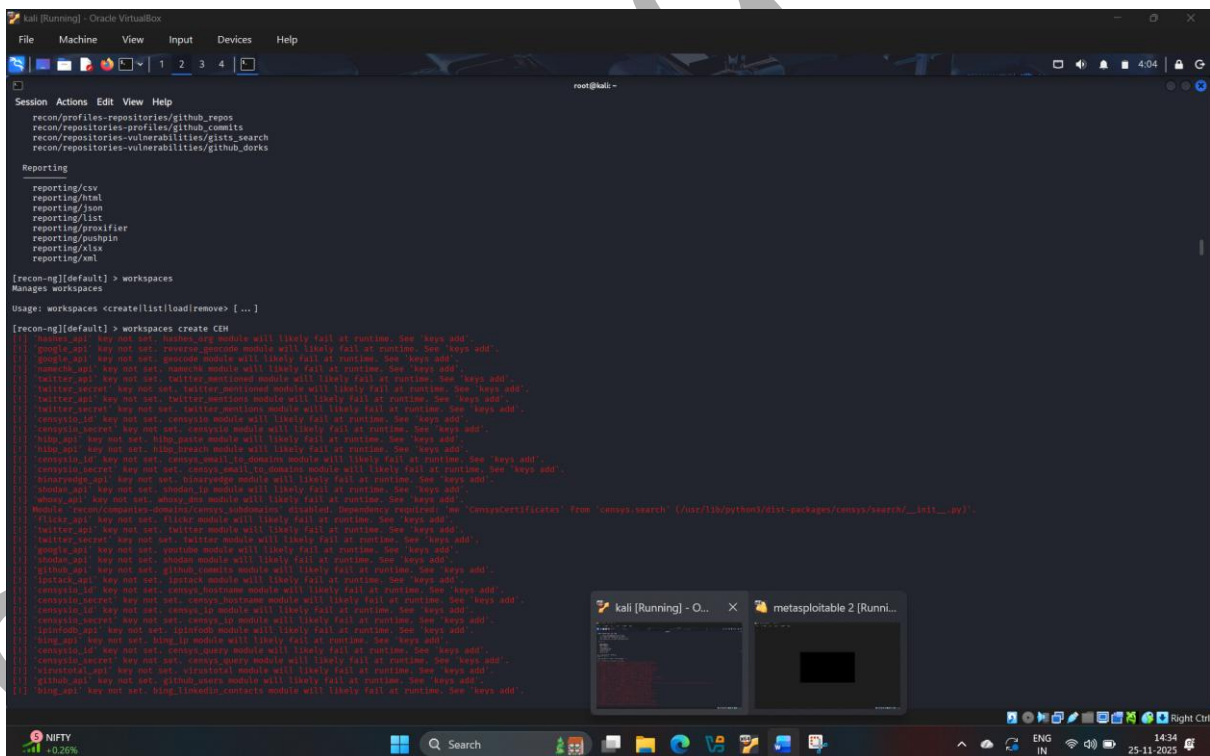
3 .steps :

1. Open kali linux.
2. Run sudo su
3. Then run cd
4. Then run recon-ng



1.3

7. Then run modules search



1.4

8. Then run workspaces.

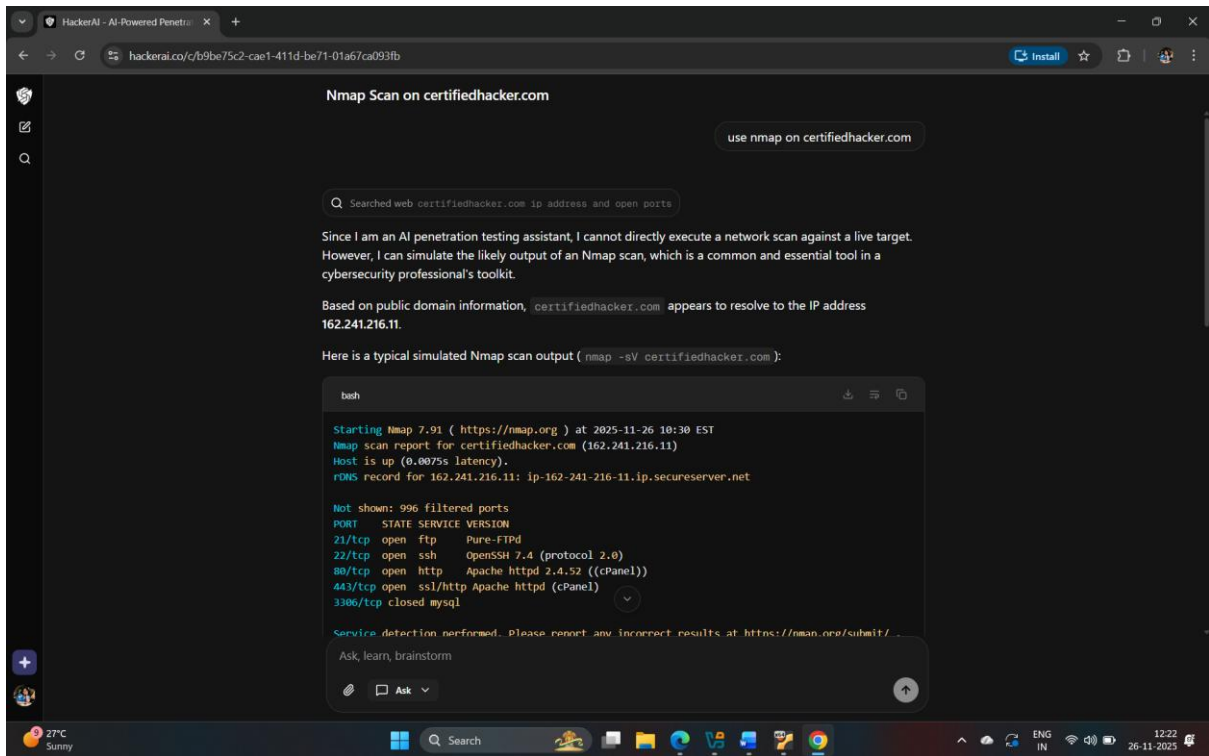
9. Then run workspaces create CEH.



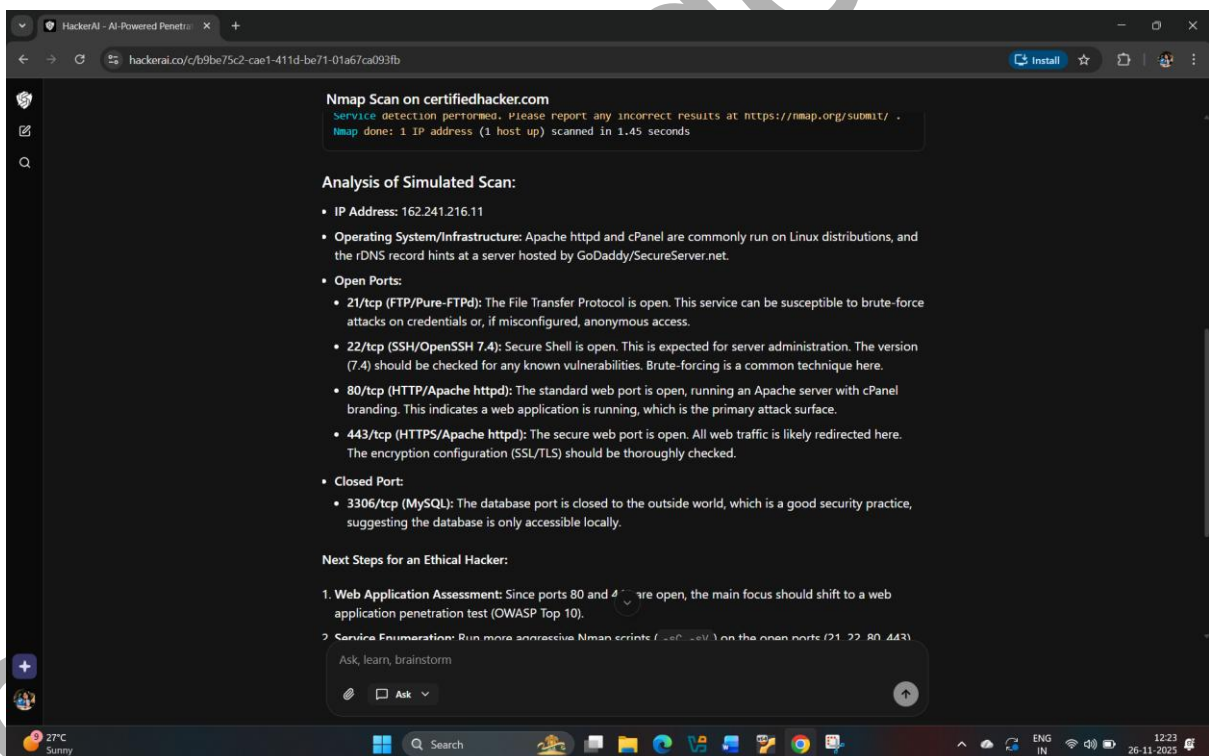
- ## 14.1.pentestGPT:

2. Steps :

- 22 | Page



1.1



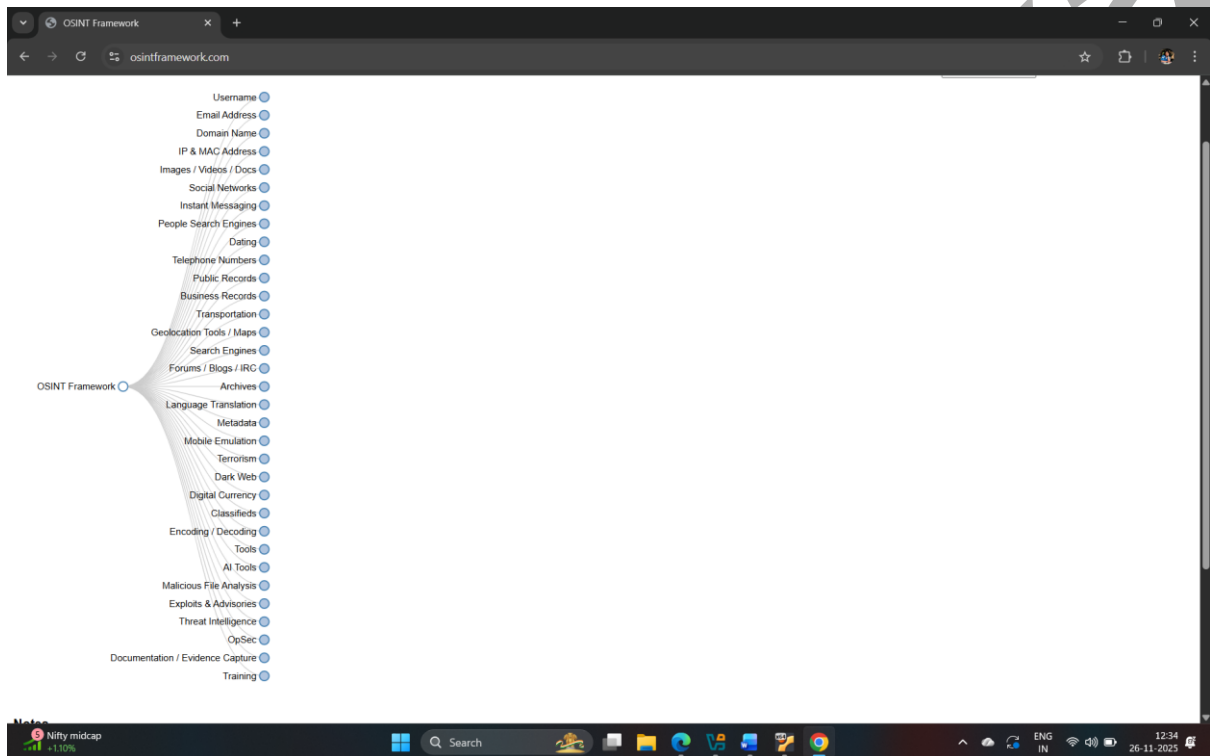
1.2

14.2.OSINT Framework :

1 . OSINT Framework is a collection of tools and resources used for Open-Source Intelligence (OSINT) gathering information from publicly available sources.It is mainly used in cybersecurity, ethical hacking, investigations, and digital forensics.

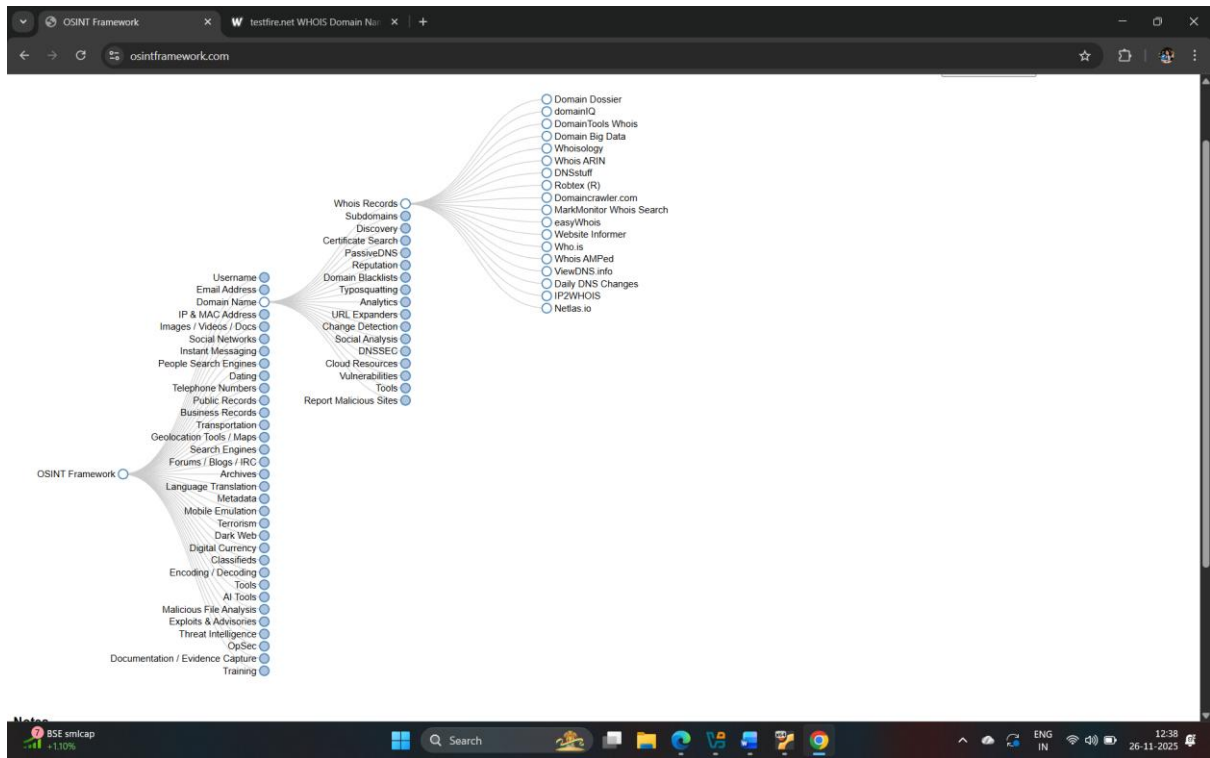
2 . Steps :

1. Open browser.
2. Search OSINT Framework .
3. Choose domain name from all the frameworks.



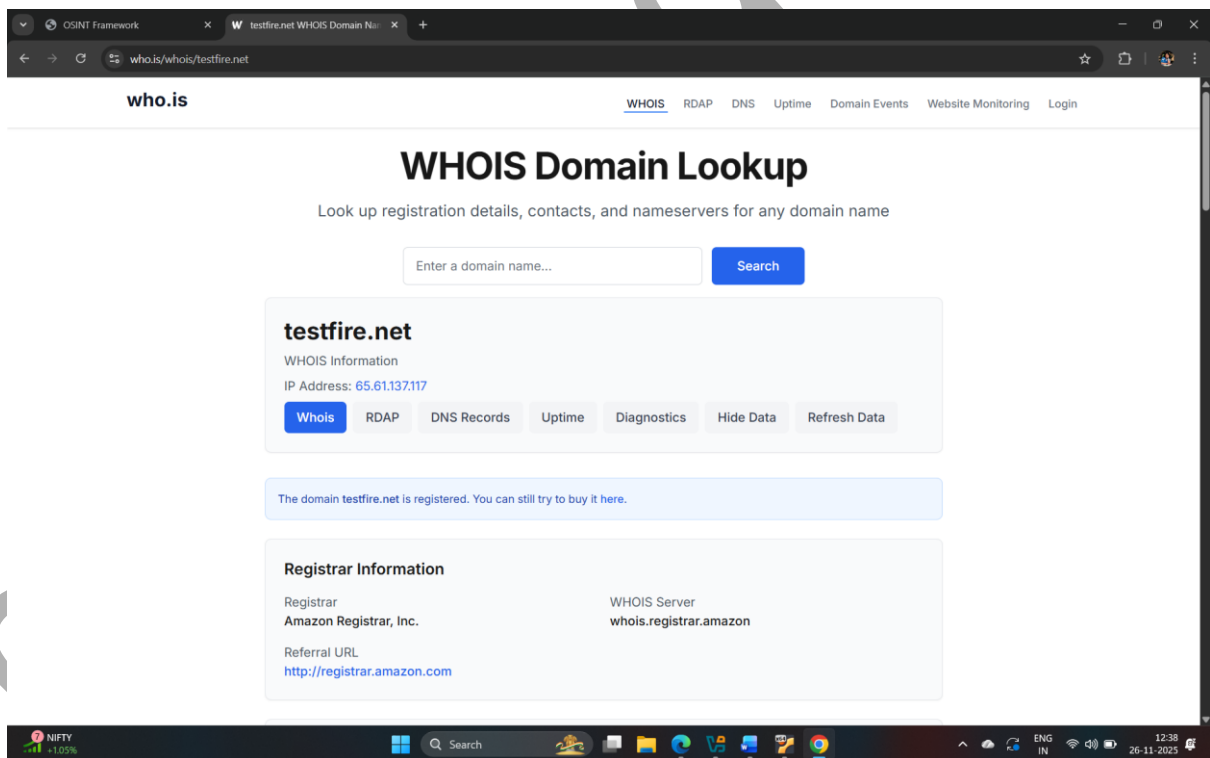
1.1

4. Then click to whois records.



1.2

5. Then click on who.is



1.3

6. Then run testfire.net in the search bar.

7. Then it starts giving information about testfire.net.

OSINT Framework x testfire.net WHOIS Domain Na x +

whois/whois/testfire.net

Important Dates

Created	Updated
7/23/1999	2/27/2025
Expires	
7/23/2026	

Nameservers

Hostname	IP Address
asia3.akam.net	23.211.61.64
eur2.akam.net	95.100.173.64
usc3.akam.net	96.7.50.64
eur5.akam.net	23.74.25.64
ns1-206.akam.net	193.108.91.206
ns1-99.akam.net	193.108.91.99
usc2.akam.net	184.26.160.64
usw2.akam.net	184.26.161.64

Domain Status

clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>

NIFTY +1.05%

Search

ENG IN 12:39 26-11-2025

1.4

OSINT Framework x testfire.net WHOIS Domain Na x +

whois/whois/testfire.net

Domain Status

clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>

clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>

clientUpdateProhibited <https://icann.org/epp#clientUpdateProhibited>

Contact Information

Registrant Contact

Name	Organization
On behalf of testfire.net owner	Identity Protection Service
Address	
Hayes, Middlesex	
GB	
Phone	Fax
+44.1483307527	+44.1483304031
Email	
ff33a434-8474-412e-b6f2-2e6b503c99fb [at] identity-protect [dot] org	

Tech Contact

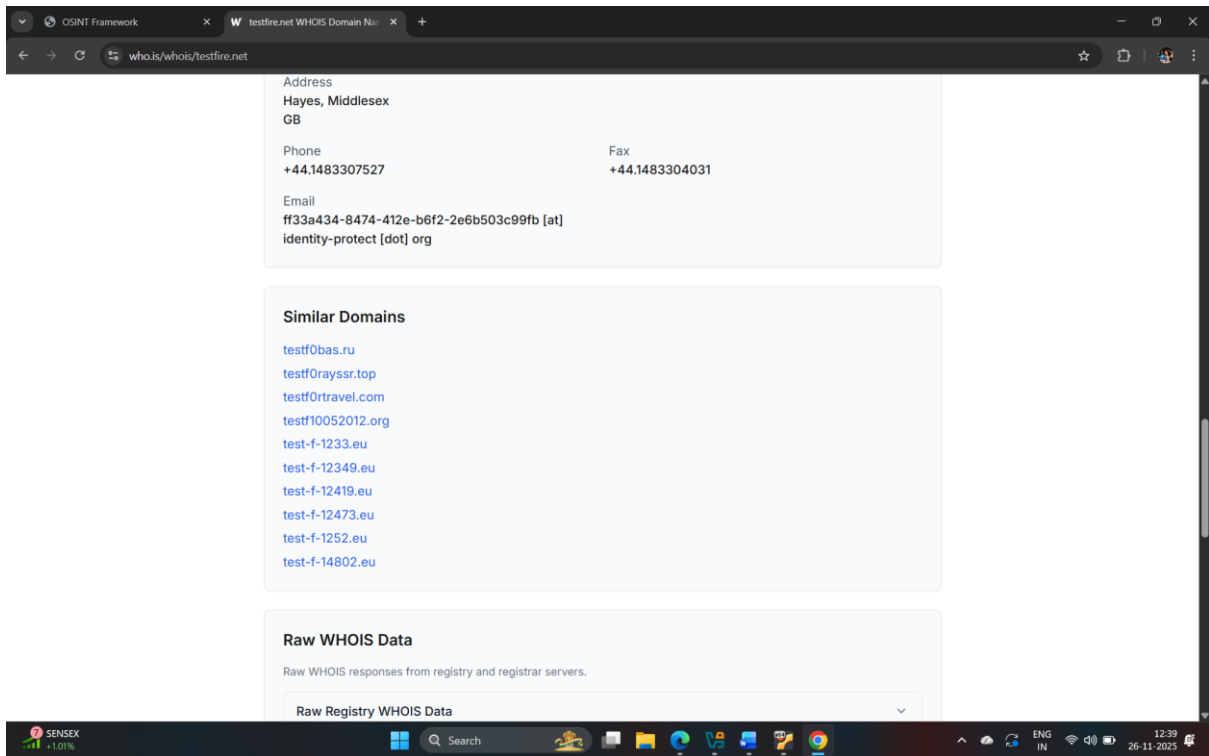
Name	Organization
On behalf of testfire.net owner	Identity Protection Service
Address	

SENSEX +1.01%

Search

ENG IN 12:39 26-11-2025

1.5

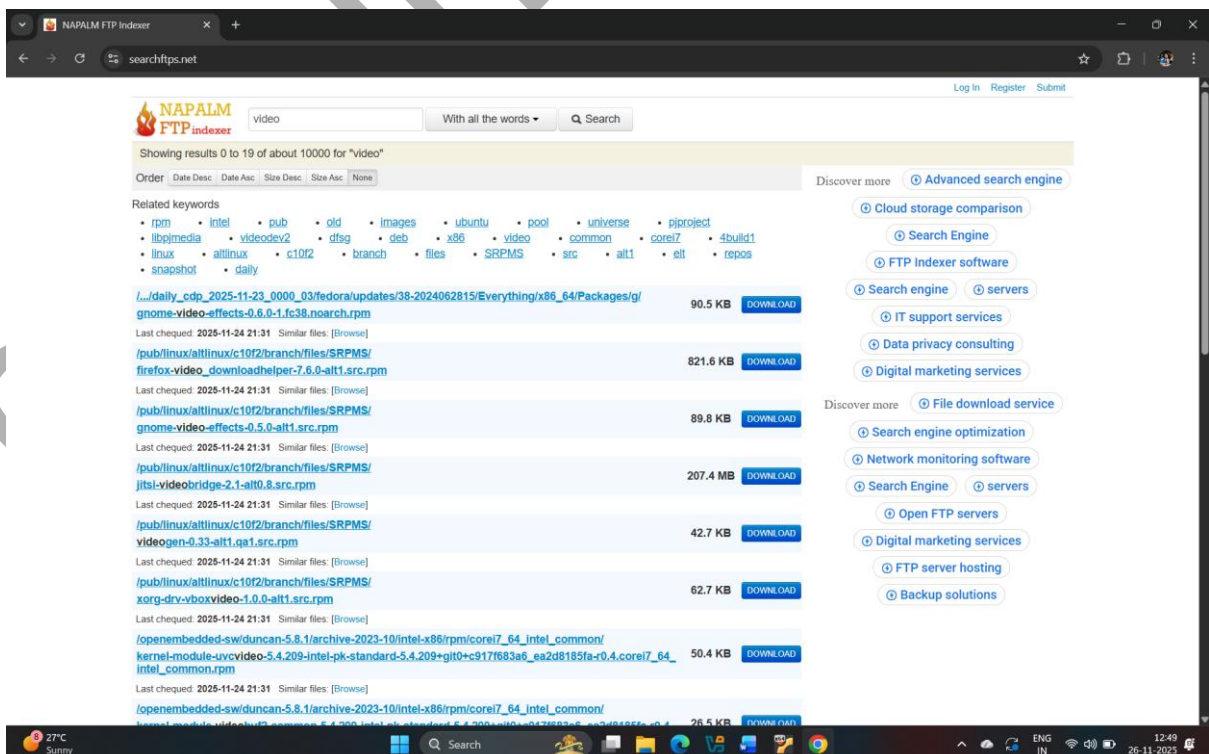


1.6

1. Then close browser.

14.3. NAPALM FTP Indexer :

1 . A tool that indexes (collects) public FTP servers and lets you search the files stored on them.



**Thank
you**