MODULE 2

FOOTPRINTING

AND

RECONNAISSANCE

Date : 21.11.2025

Name : Mugdha Makarand Govilkar

Instructor : Satish Singh

mugdha govilkar

INDEX

mugdha govilkar

Target site – testfire.net

Target ip – 65.61.137.117

mugdha govilkar

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)

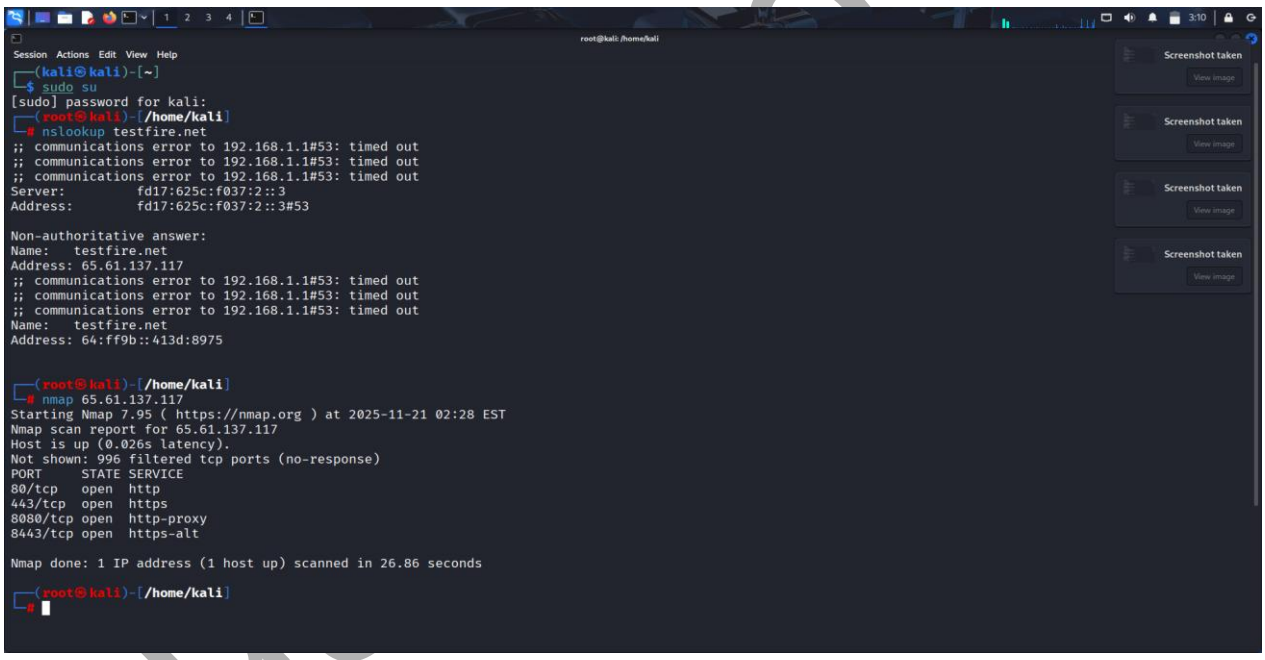
- **Stores text information in DNS, often used for:**
  - **SPF (email security)**
  - **DKIM**
  - **Google/Domain verifications**

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.**

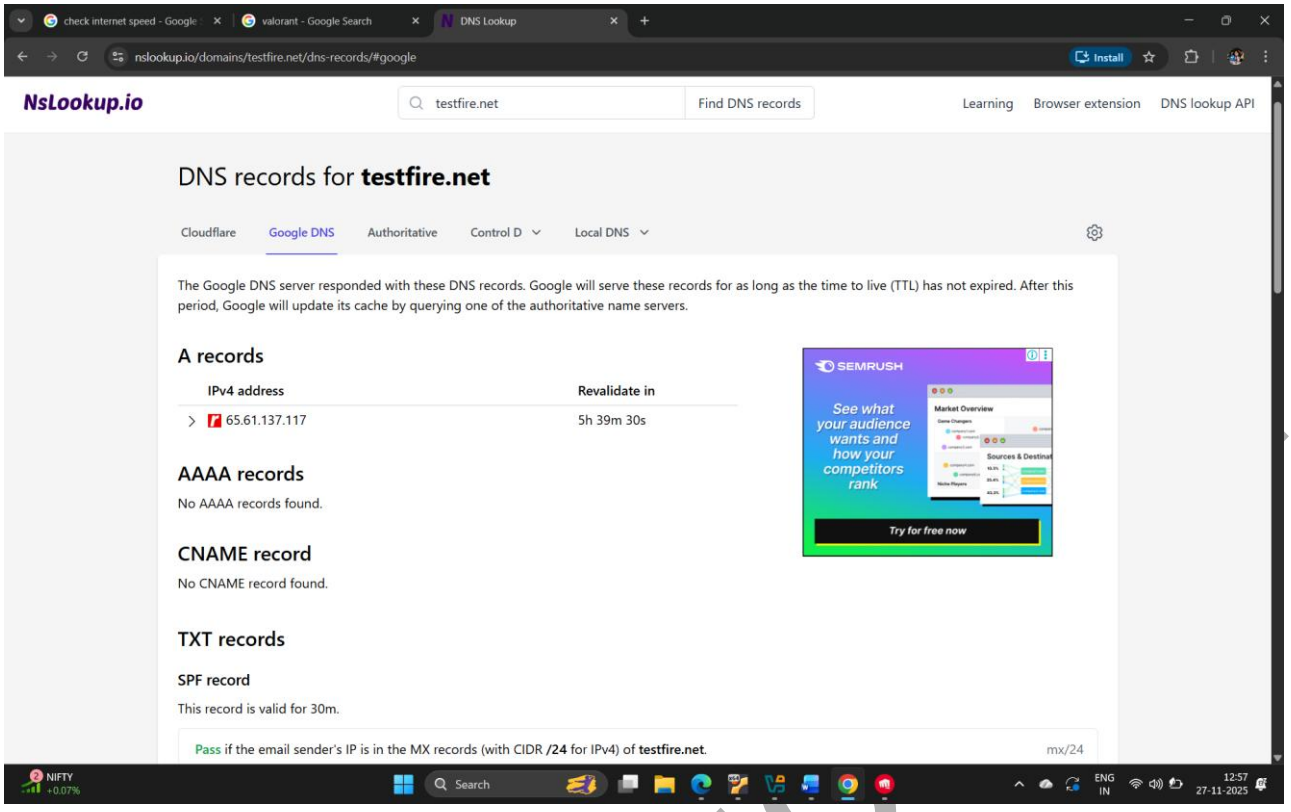
7 . Steps :

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.**



1.1

mukul vilkar



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.

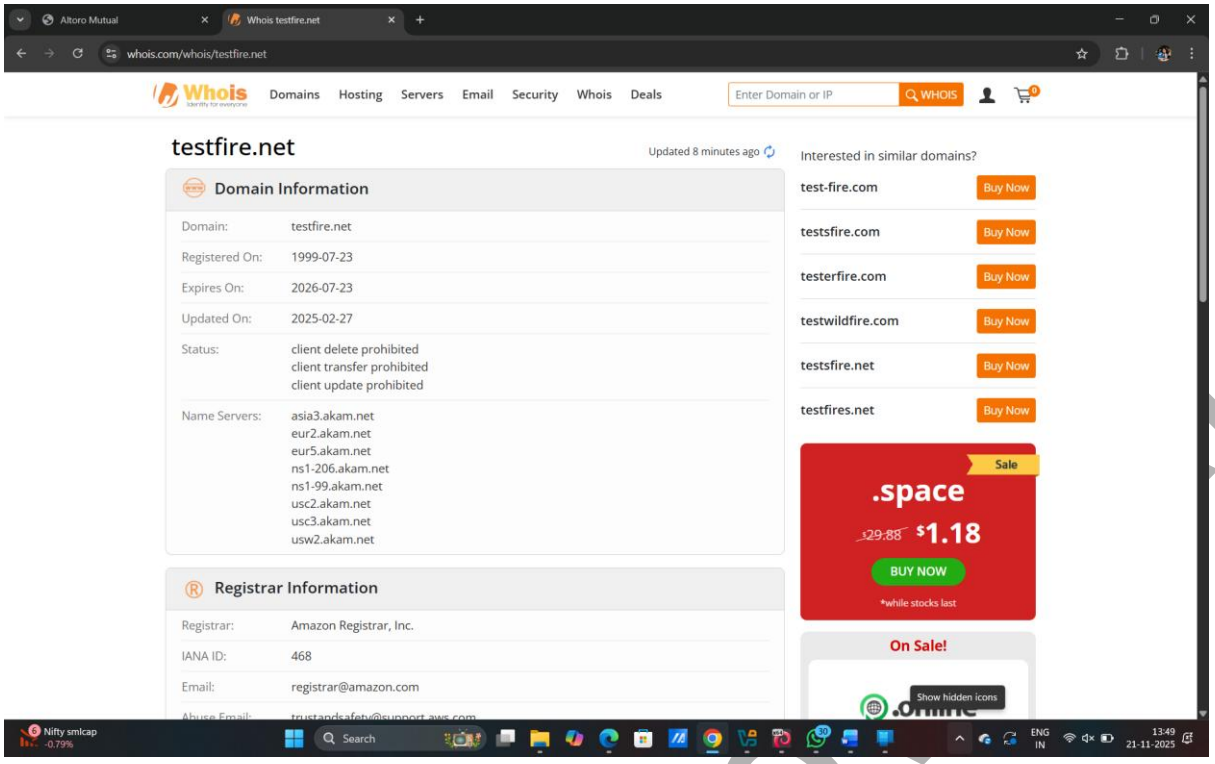
2 . It helps in verifying domain ownership, identifying administrative contacts, investigating suspicious domains, and performing OSINT during cybersecurity assessments.

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.**

mugdha go



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:**

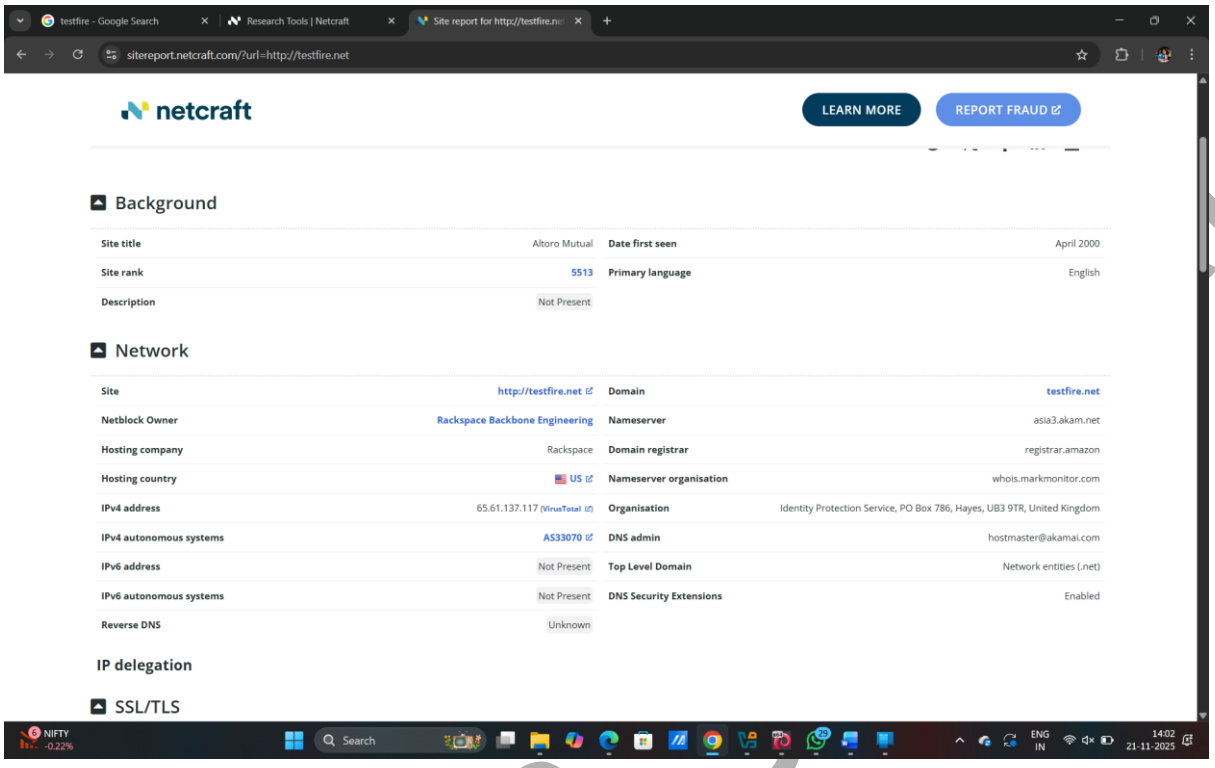
- **Hosting details (where the website is hosted)**
- **Server technology (Apache, Nginx, IIS, etc.)**
- **Operating system**
- **SSL/TLS certificate details**
- **Domain history (previous owners, hosting changes)**
- **Site rank and traffic estimation**
- **Potential vulnerabilities or outdated software**
- **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.**

muggha go

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 brower.



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.

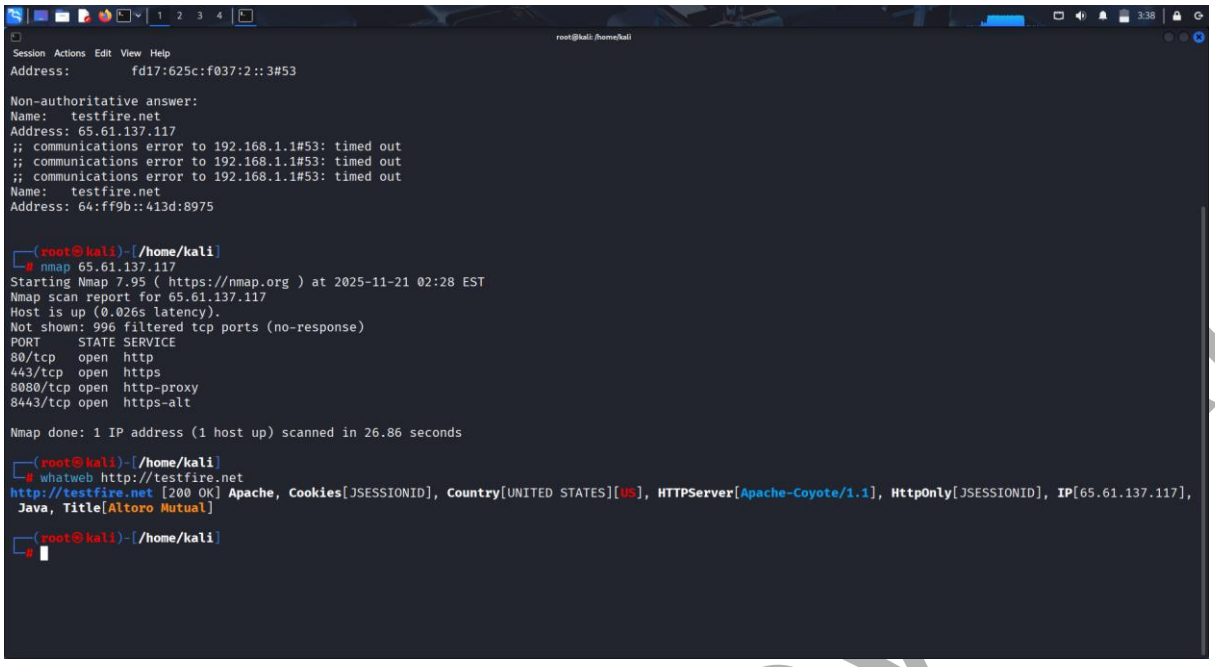
3 . It tells you what a website is built with by fingerprinting its components.

- 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,iptitle,language.
4. Close kali linux.

mugdha



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.

mugdha gov

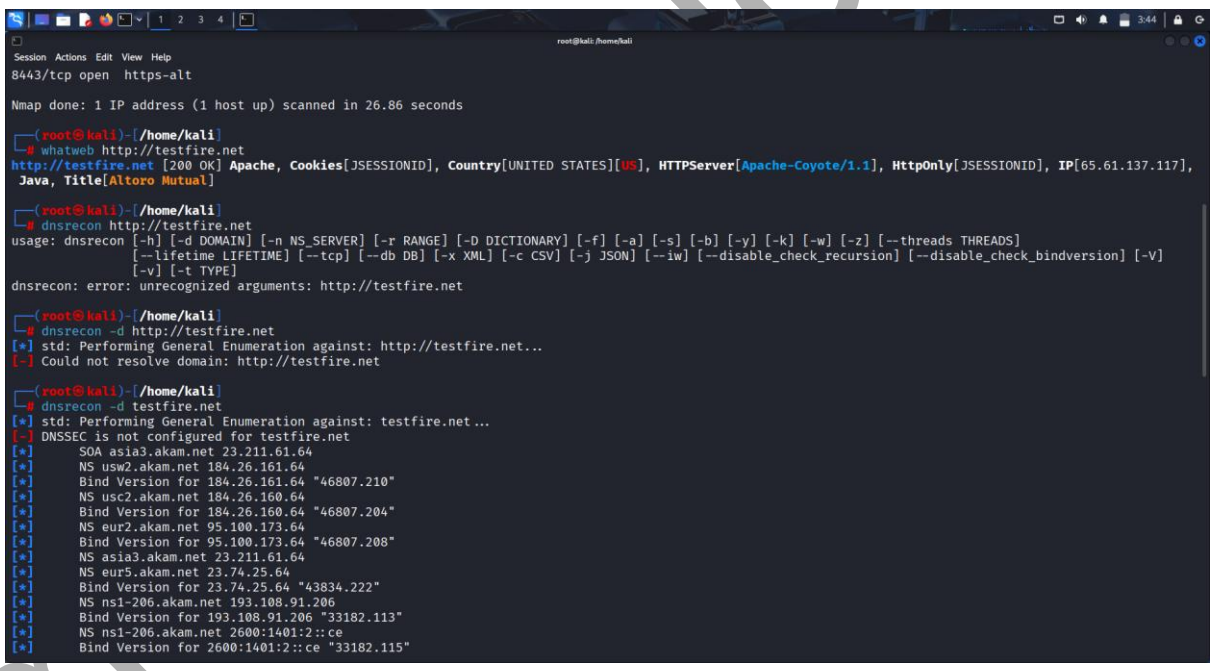
- **Gathering DNS Topology**
  Helps understand how a domain is structured and managed.

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,SOAShows-zone authority, serial number, and admin email**
4. **Close kali linux**



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.

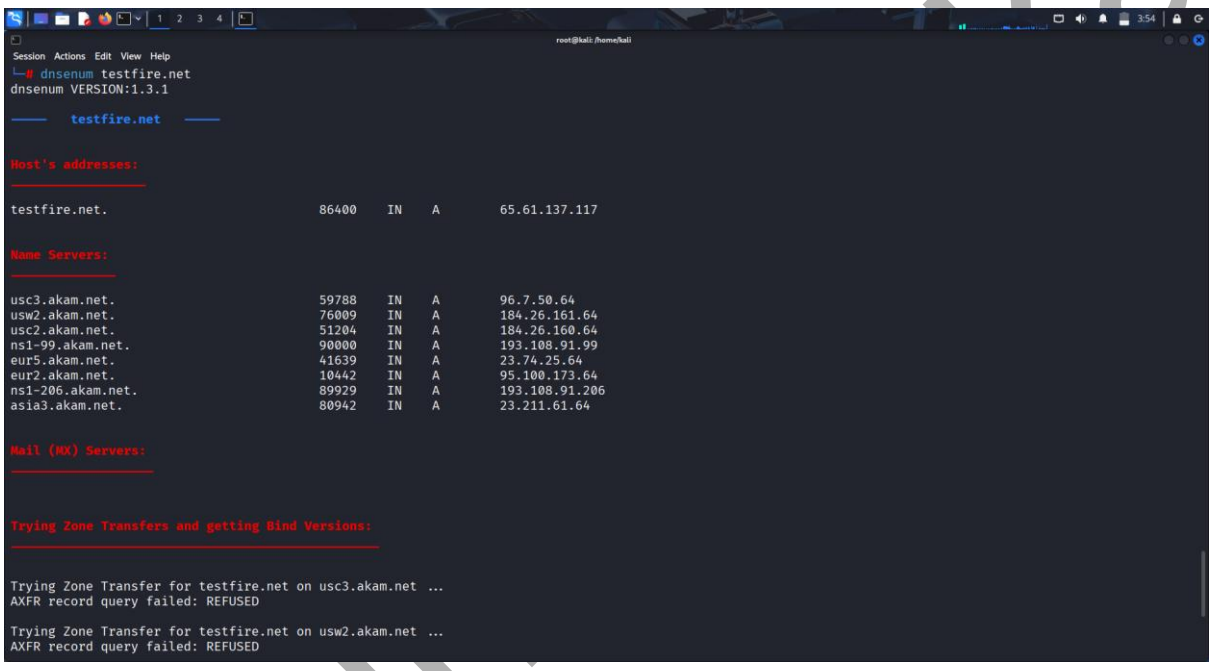
2 . DNS zone transfer is the process of copying DNS zone data from a primary (authoritative) server to secondary servers for redundancy and fault tolerance. This allows secondary servers to

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

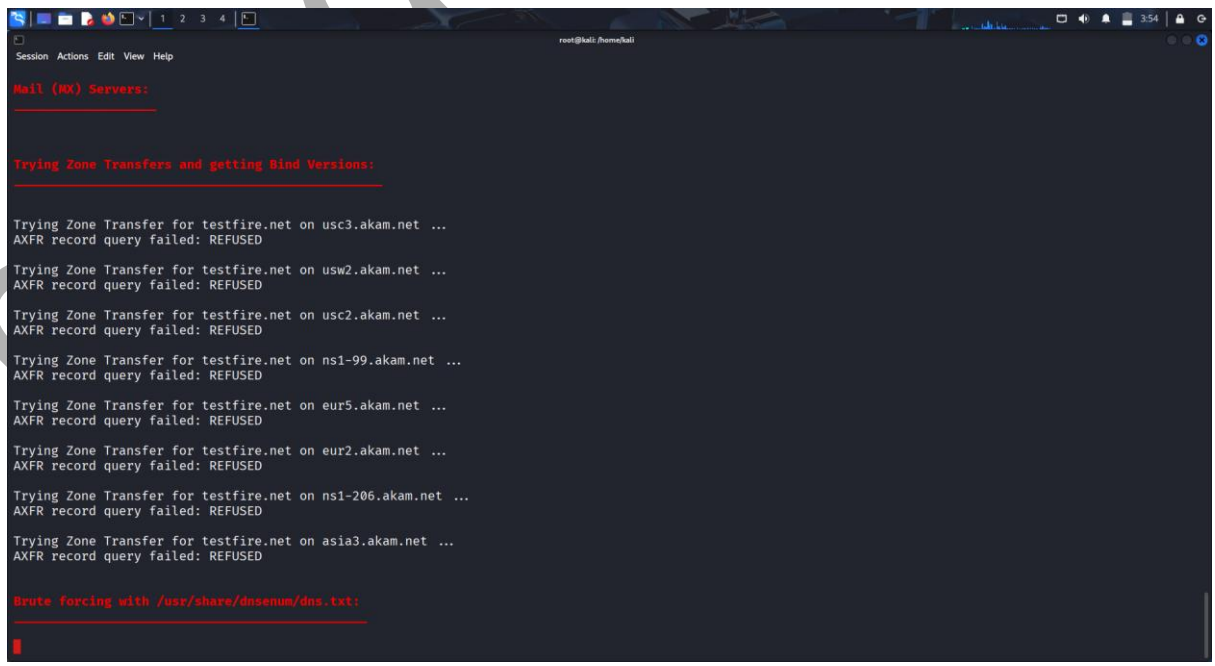
3 . here we use dnsenum tool.

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.**



1.1



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

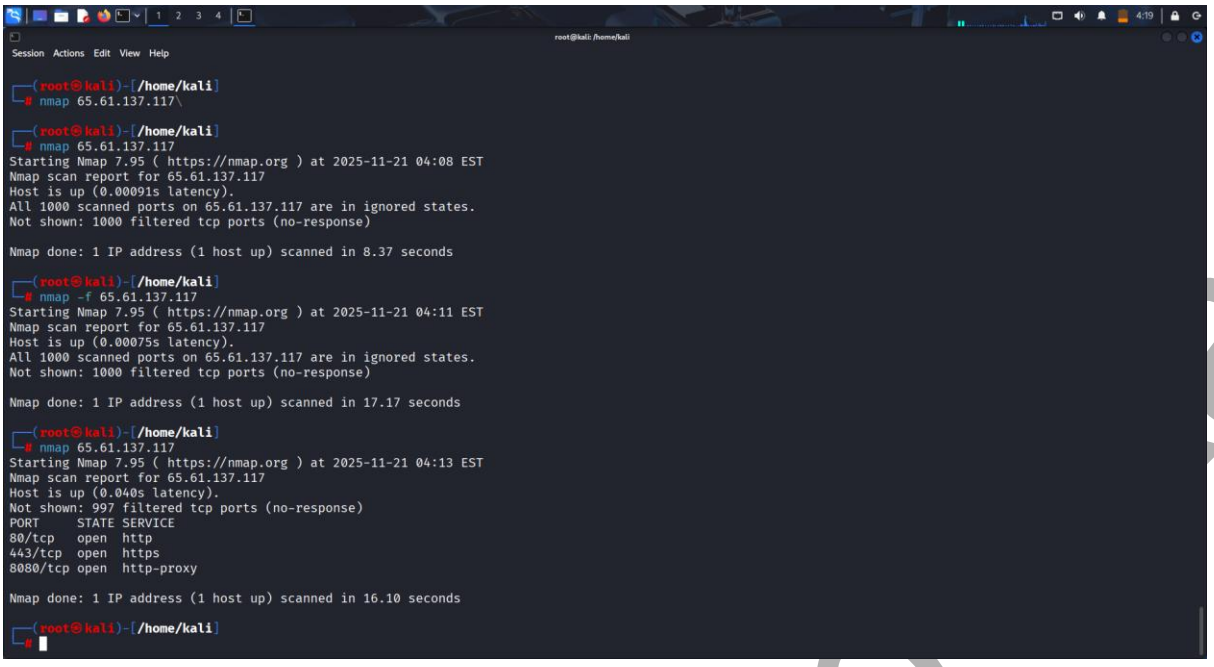
Helps identify firewall rules and packet filtering.

10 .Steps :

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

mugdha govilkar

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



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**

mugdha gawar

- **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.

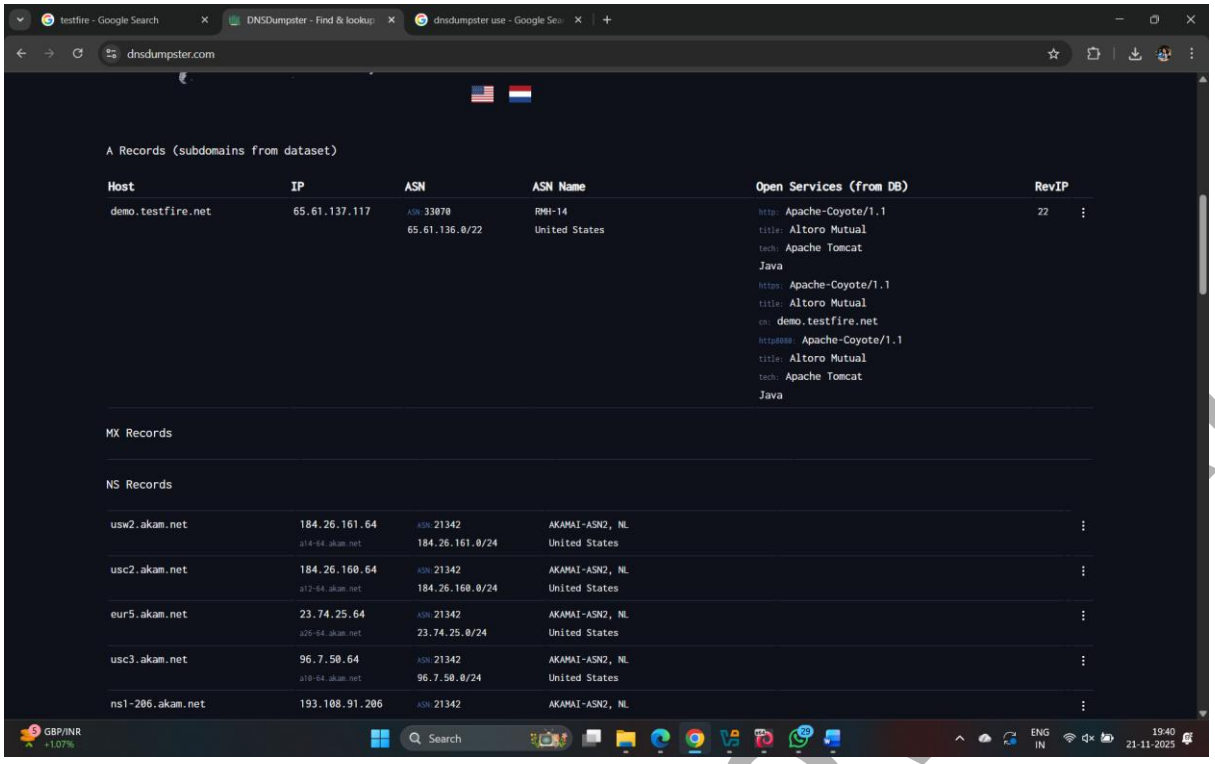
6. Checking DNS Configurations

Helps identify misconfigurations or outdated DNS entries.

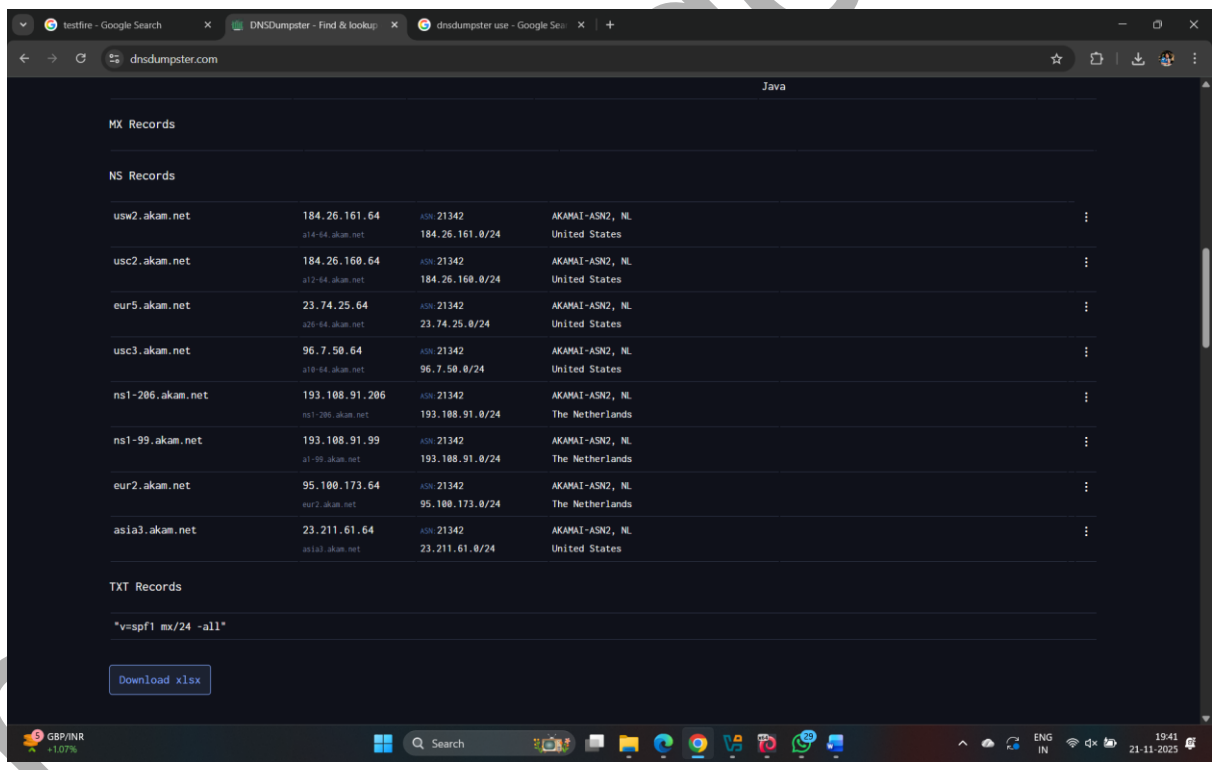
7 . Steps :

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.**

mugdha govilkar



1.1



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**

mugdha govilkar

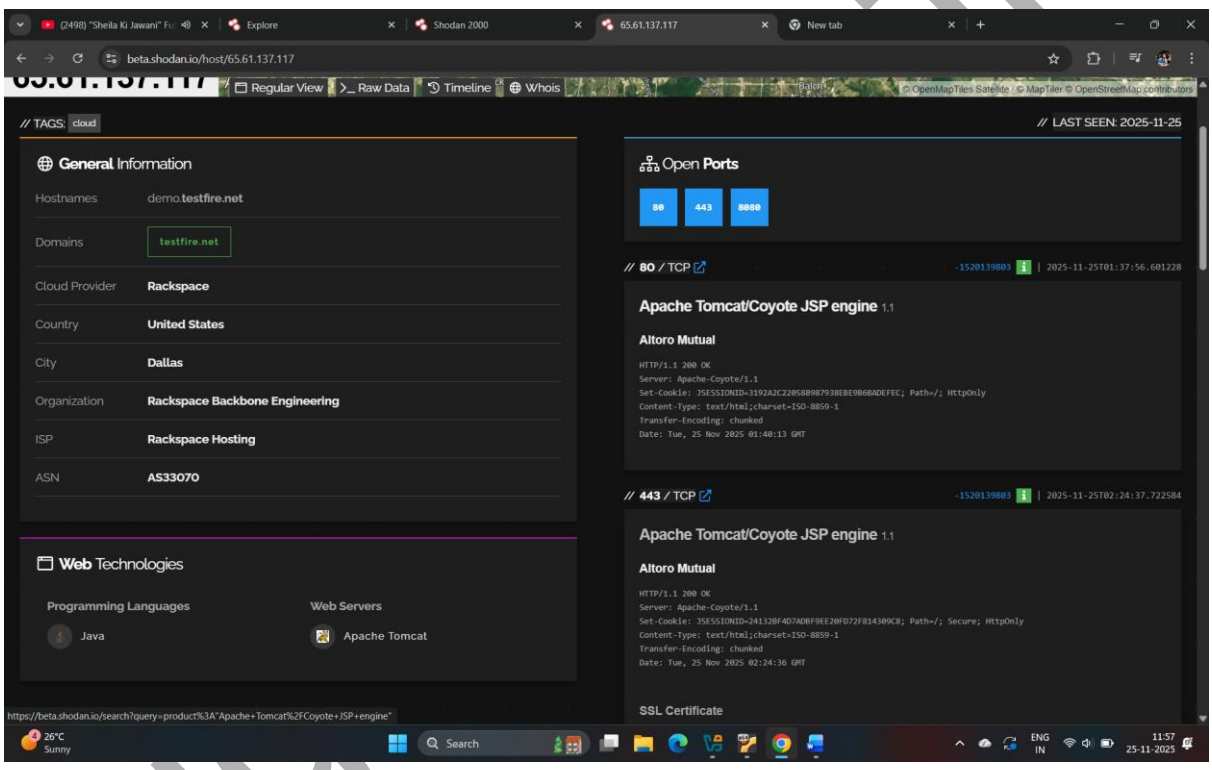
- **Banners**

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,countr,city,organisation**
5. **Close browser.**



10 . footprinting via sherlock:

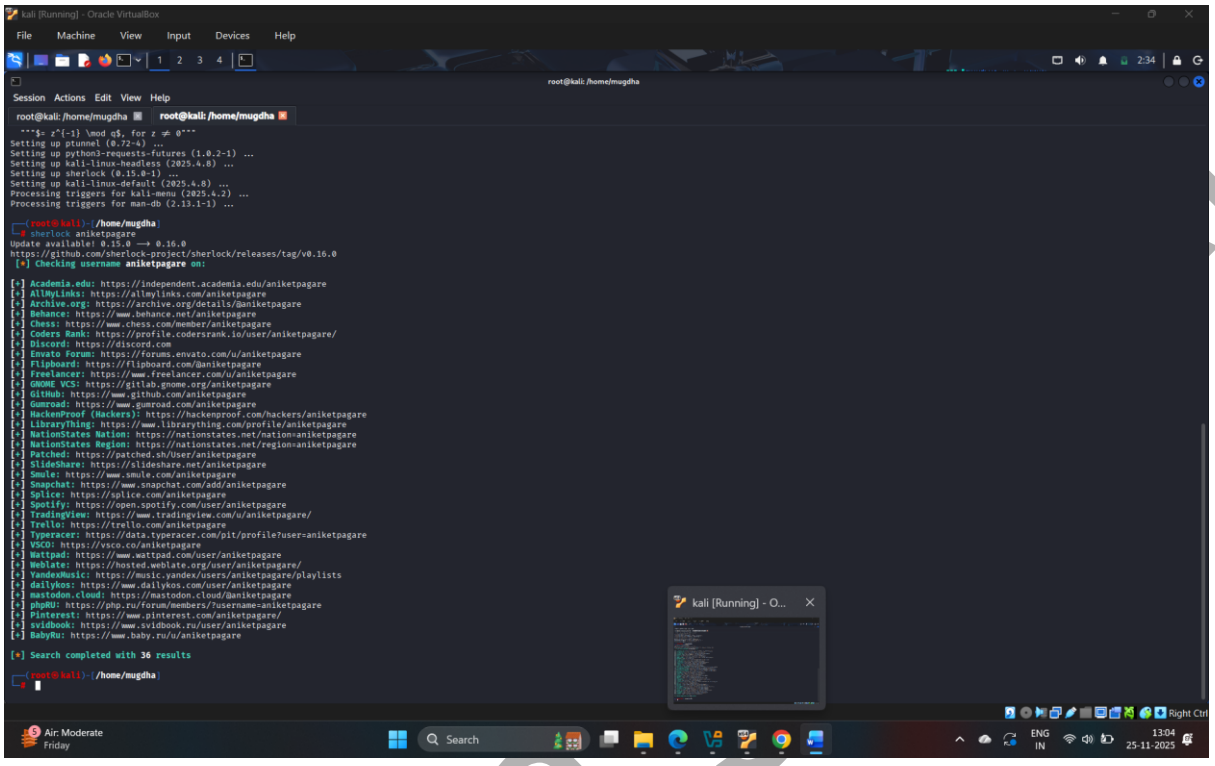
1 . Sherlock is an open-source tool used to find usernames across social media platforms and websites.

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.



11 . subfinder:

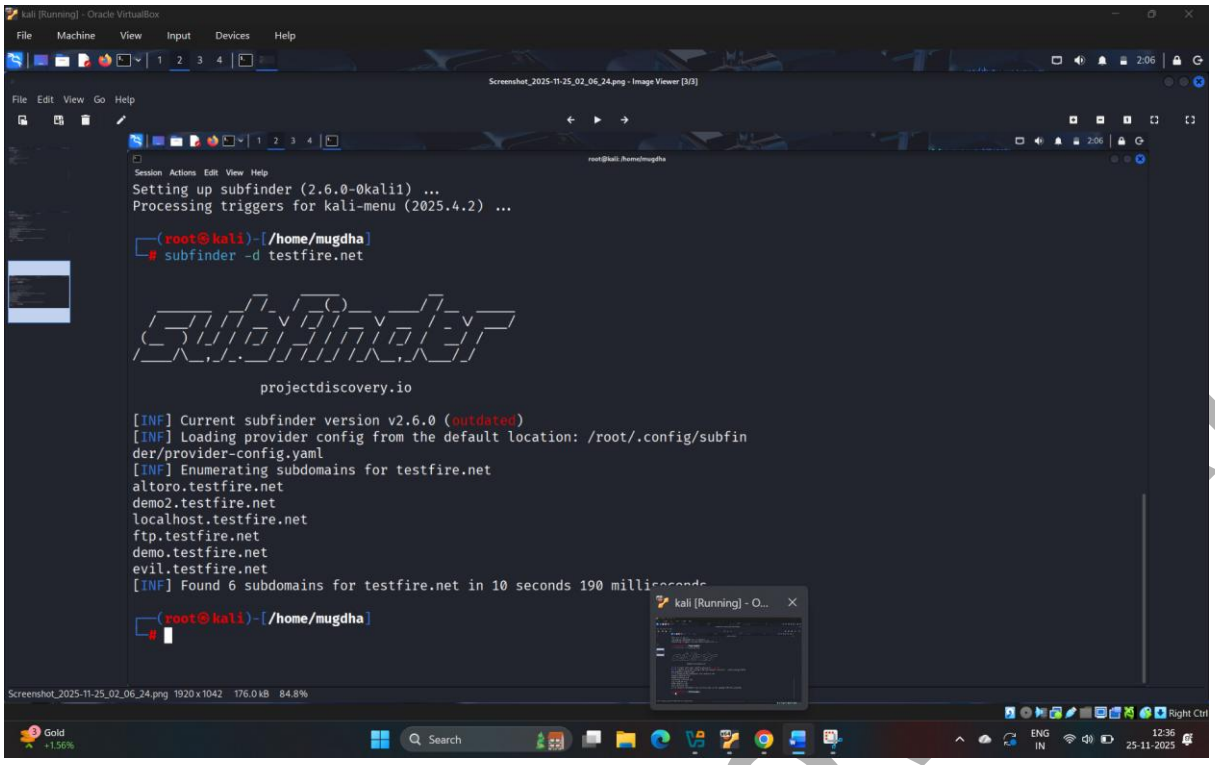
1 . Subfinder is a popular OSINT and recon tool used in cyber security to find subdomains of a target domain.

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 aout subdomain here altoro.testfire.net,demo2.testfire.net,localhost.testfire.net,ftp.testfire.net,demo.testfire.net,evil.testfire.net.
4. Close kali linux.

mugdha



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).

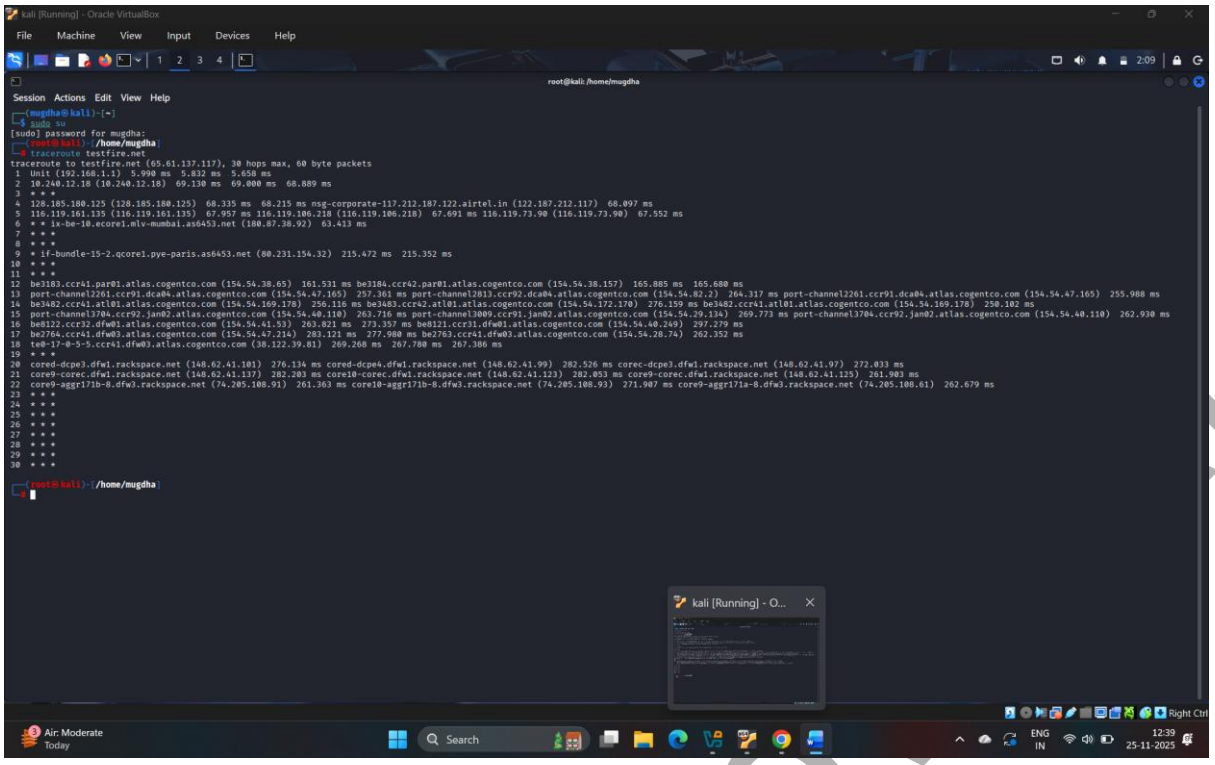
2 . It helps in network troubleshooting, OSINT, pentesting, and mapping network infrastructure.

3 . * means no response received from that hop

4 . Stps :

1. **Open kali linux.**
2. **Run treaceroute testfire.net**
3. **It gives information about the path testfire.net's packets uses to reach destination.**
4. **Close kali linux.**

mugdha go



13 . recon-ng:

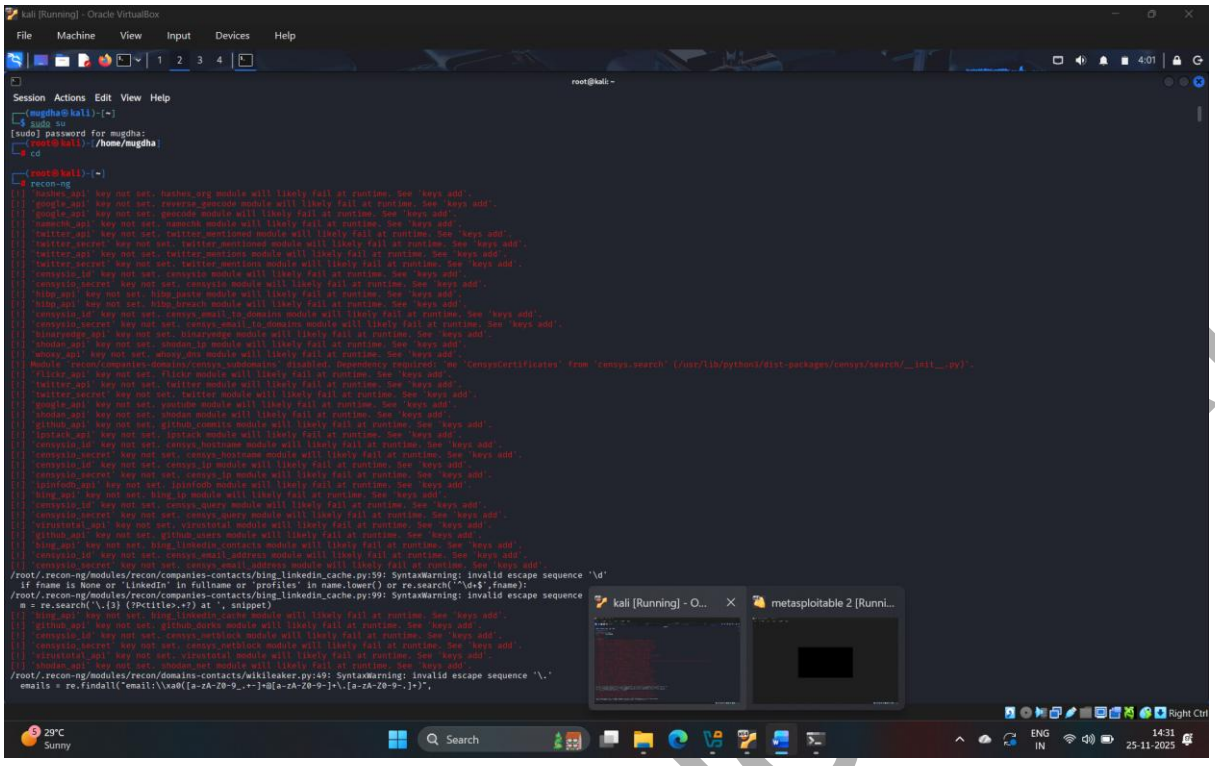
1 . It is used to gather information about targets such as domains, companies, people, IP addresses, emails, and social media profiles.

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 :

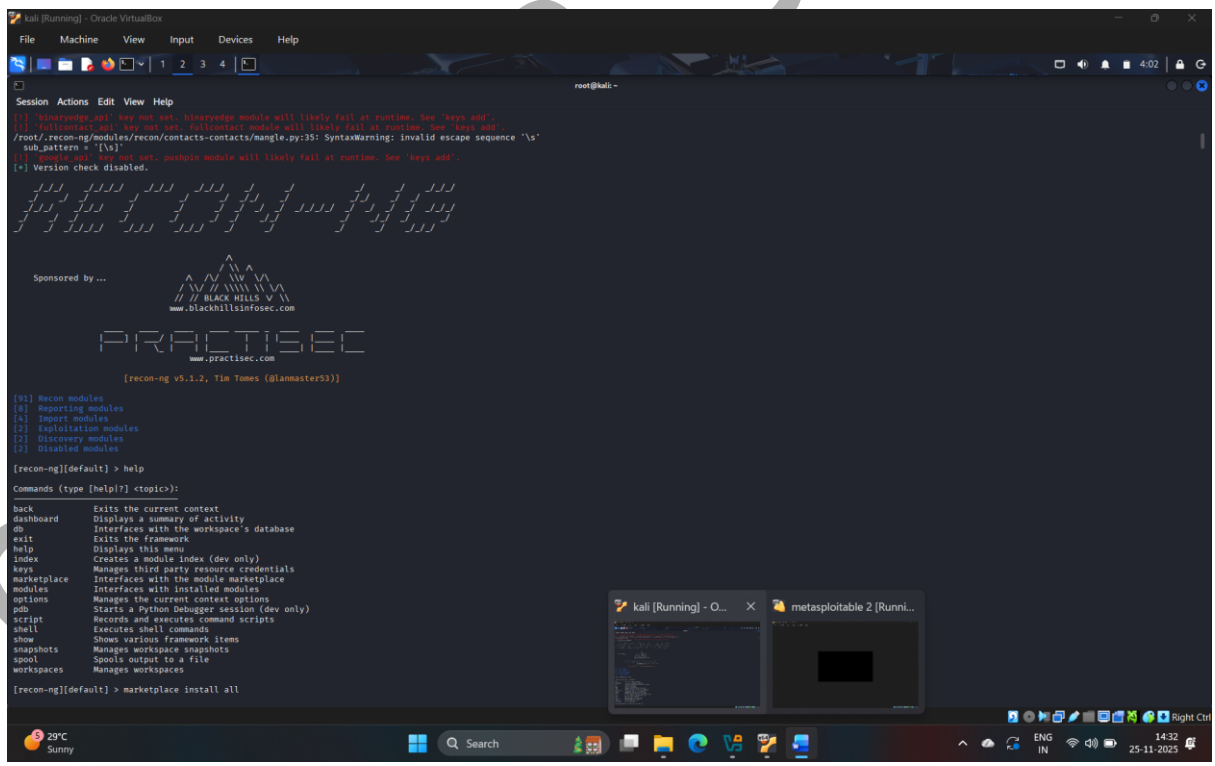
1. **Open kali linux.**
2. **Run sudo su**
3. **Then run cd**
4. **Then run recon-ng**

mugdha go



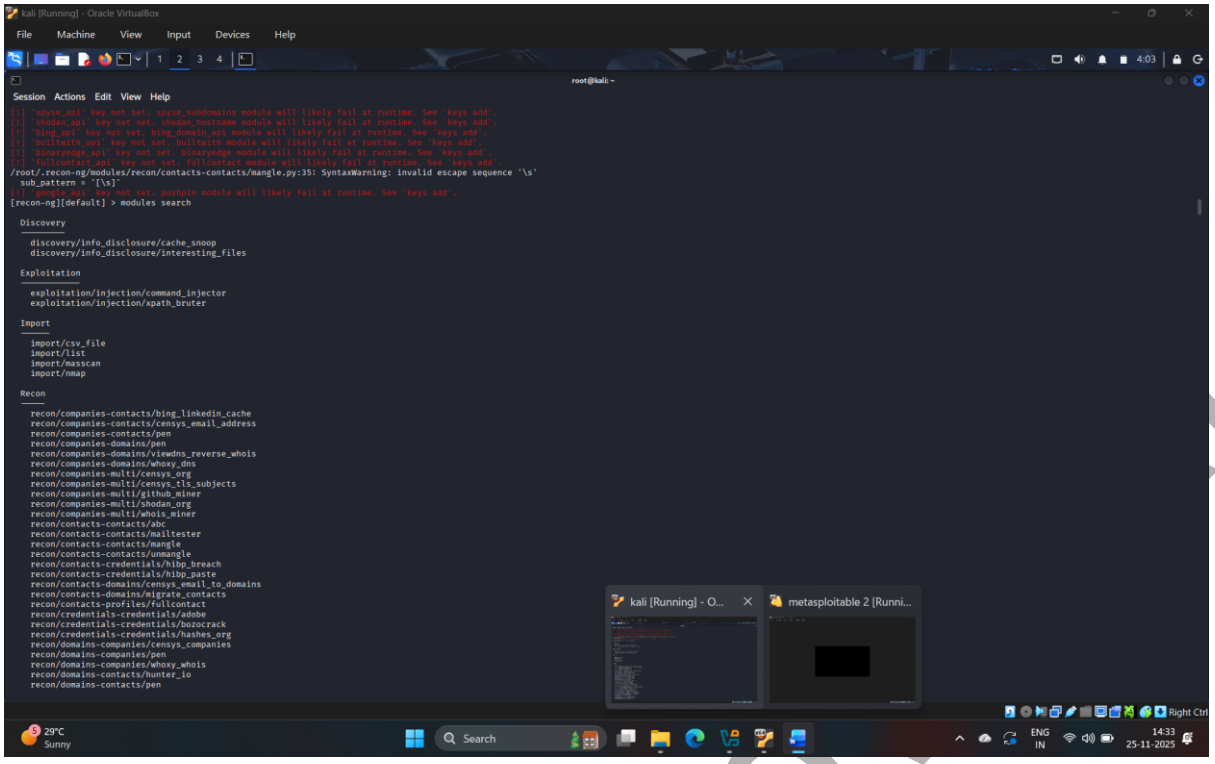
1.1

5. **It will start installing.**



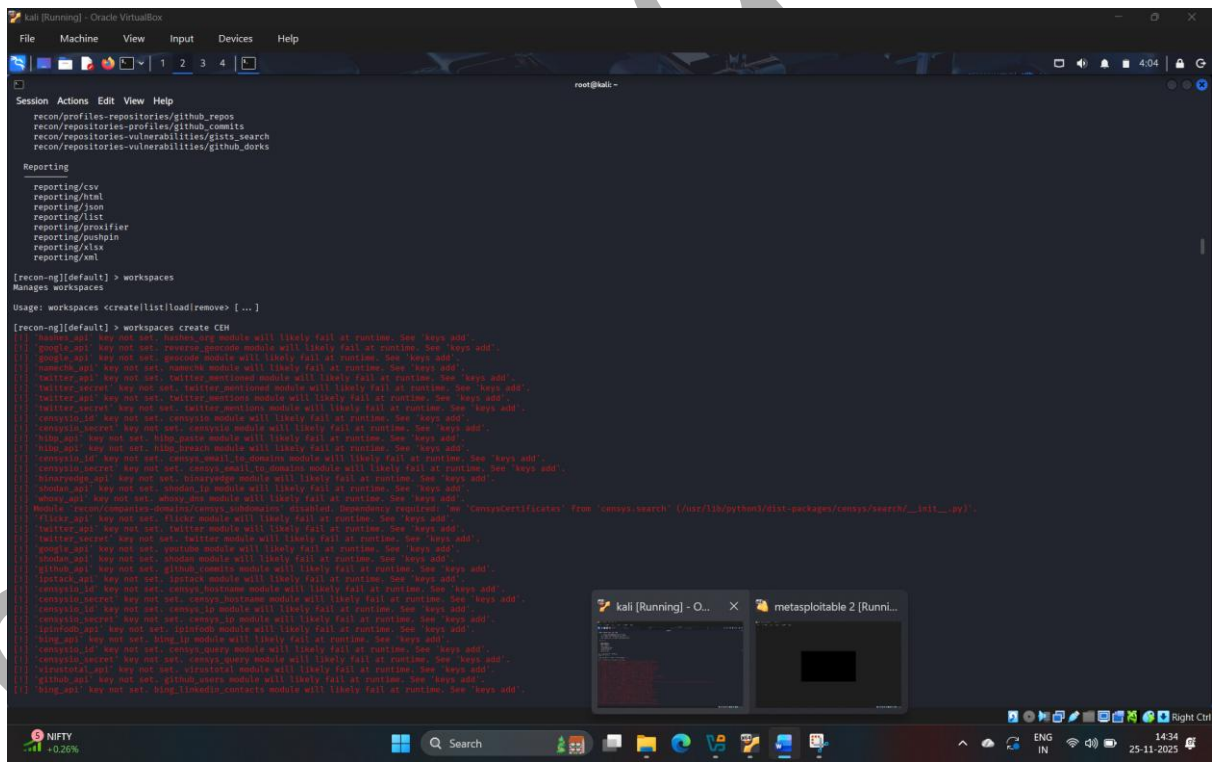
1.2

6. **Then run help to get manual.**



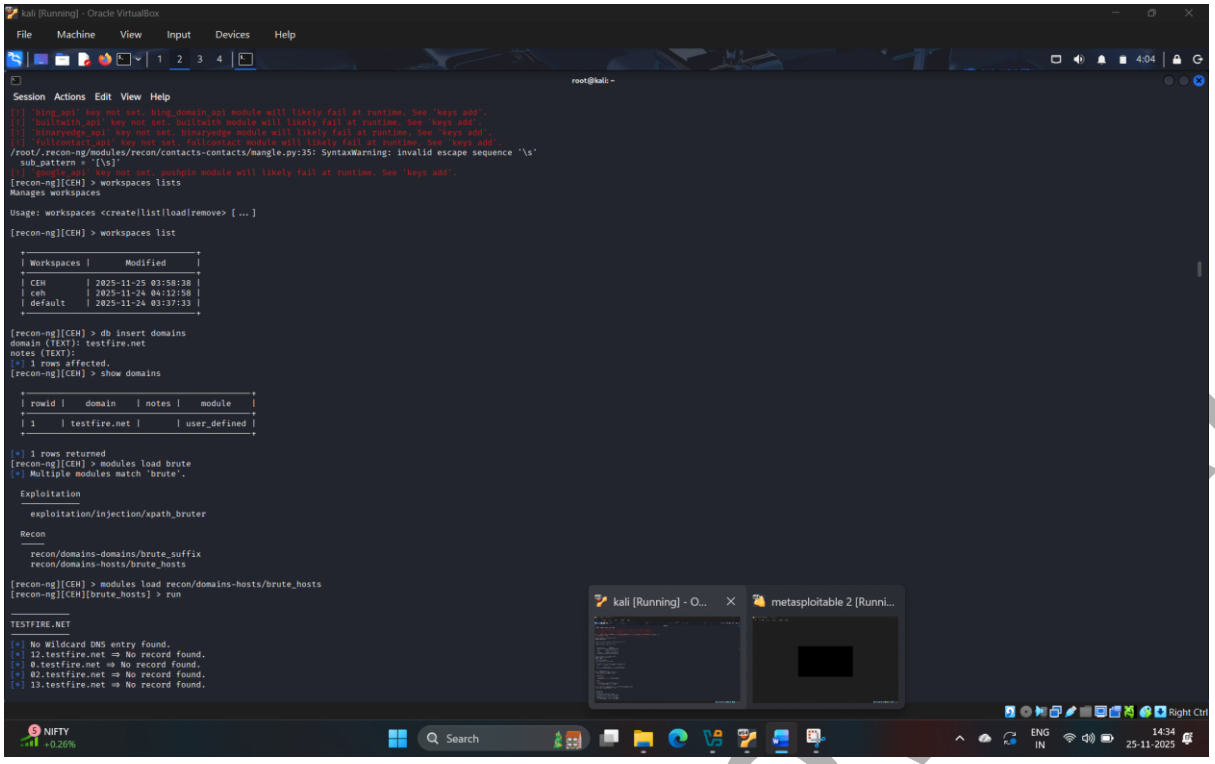
1.3

7. **Then run modules search**



1.4

8. **Then runworkspaces.**
9. **Then run workspaces create CEH.**



1.5

10. Run workspaces list.
11. run db insert domains.
12. run yestfire.net.
13. run show options.
14. run modules load brute.
15. it gave result as no record found means The source (API, search engine, database) has no information about the target you queried.

14 . Additional tools :

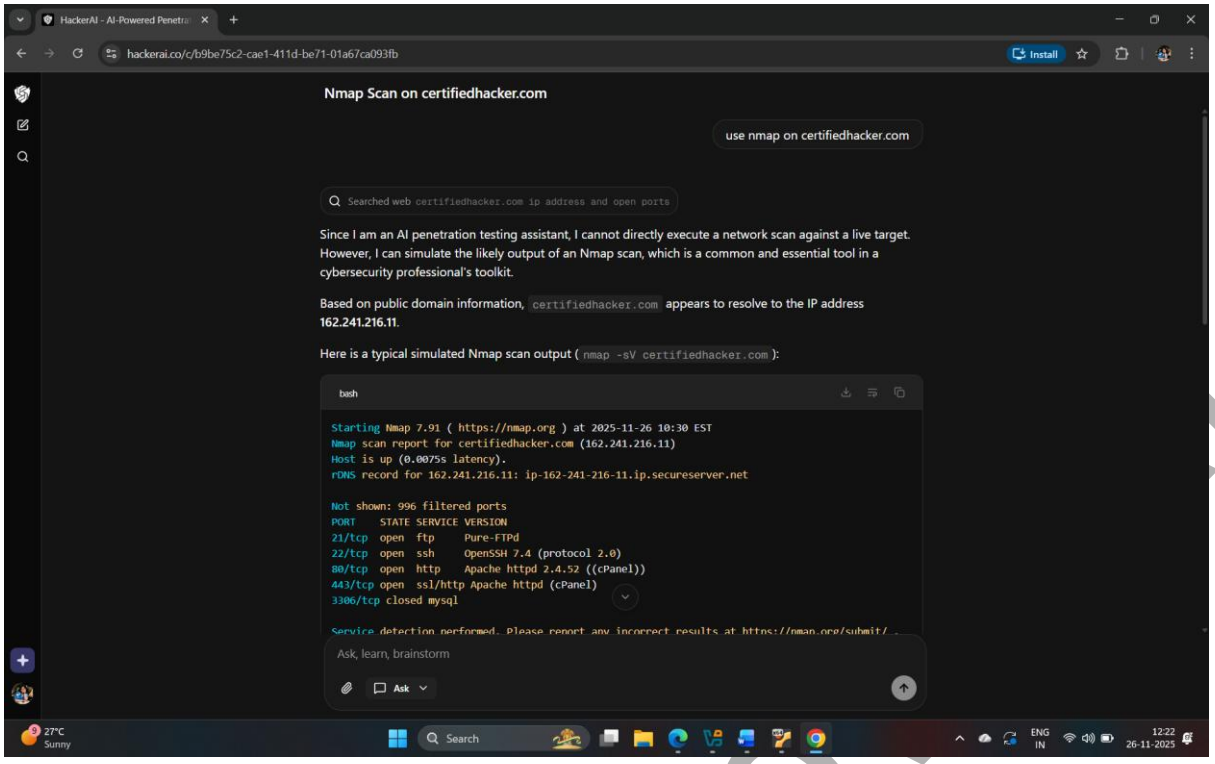
14.1.pentestGPT :

1 . PentestGPT is an AI-powered penetration testing assistant designed to help ethical hackers, cybersecurity students, and bug bounty hunters perform security testing more effectively.Think of it as a ChatGPT specially trained for hacking & pentesting tasks.

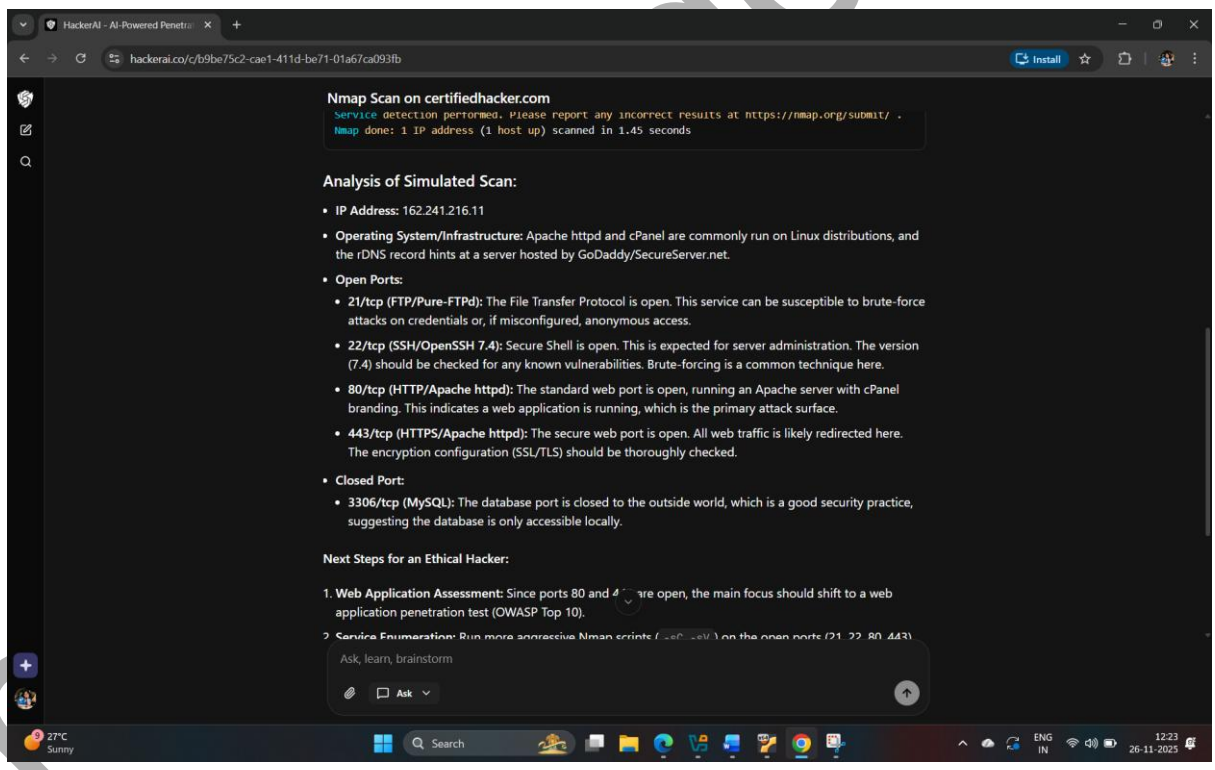
2 . Steps :

1. **Open browser**
2. **Run pentestGPT in search bar**
3. **Run use nmap on certifiedhacker.com**
4. **It starts giving information about ports.operating systems,etc.**
5. **Close browser.**

mugdha go


HackerAI - AI-Powered Penetra
hackerai.co/c/b9be75c2-cae1-411d-be71-01a67ca093fb
Install
Nmap Scan on certifiedhacker.com
use nmap on certifiedhacker.com
Searched web certifiedhacker.com ip address and open ports
Since I am an AI penetration testing assistant, I cannot directly execute a network scan against a live target. However, I can simulate the likely output of an Nmap scan, which is a common and essential tool in a cybersecurity professional's toolkit.
Based on public domain information, certifiedhacker.com appears to resolve to the IP address 162.241.216.11.
Here is a typical simulated Nmap scan output (nmap -sV certifiedhacker.com):
bash
Starting Nmap 7.91 (https://nmap.org) at 2025-11-26 10:30 EST
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.0075s latency).
rDNS record for 162.241.216.11: ip-162-241-216-11.ip.secureserver.net
Not shown: 996 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
22/tcp open ssh OpenSSH 7.4 (protocol 2.0)
80/tcp open http Apache httpd 2.4.52 ((cPanel))
443/tcp open ssl/http Apache httpd (cPanel)
3306/tcp closed mysql
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Ask, learn, brainstorm
Ask
27°C
Sunny
Search
ENG
IN
12:22
26-11-2025

1.1


HackerAI - AI-Powered Penetra
hackerai.co/c/b9be75c2-cae1-411d-be71-01a67ca093fb
Install
Nmap Scan on certifiedhacker.com
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds
Analysis of Simulated Scan:
IP Address: 162.241.216.11
Operating System/Infrastructure: Apache httpd and cPanel are commonly run on Linux distributions, and the rDNS record hints at a server hosted by GoDaddy/SecureServer.net.
Open Ports:
21/tcp (FTP/Pure-FTPd): The File Transfer Protocol is open. This service can be susceptible to brute-force attacks on credentials or, if misconfigured, anonymous access.
22/tcp (SSH/OpenSSH 7.4): Secure Shell is open. This is expected for server administration. The version (7.4) should be checked for any known vulnerabilities. Brute-forcing is a common technique here.
80/tcp (HTTP/Apache httpd): The standard web port is open, running an Apache server with cPanel branding. This indicates a web application is running, which is the primary attack surface.
443/tcp (HTTPS/Apache httpd): The secure web port is open. All web traffic is likely redirected here. The encryption configuration (SSL/TLS) should be thoroughly checked.
Closed Port:
3306/tcp (MySQL): The database port is closed to the outside world, which is a good security practice, suggesting the database is only accessible locally.
Next Steps for an Ethical Hacker:
1. Web Application Assessment: Since ports 80 and 4 re open, the main focus should shift to a web application penetration test (OWASP Top 10).
Ask, learn, brainstorm
Ask
27°C
Sunny
Search
ENG
IN
12:23
26-11-2025

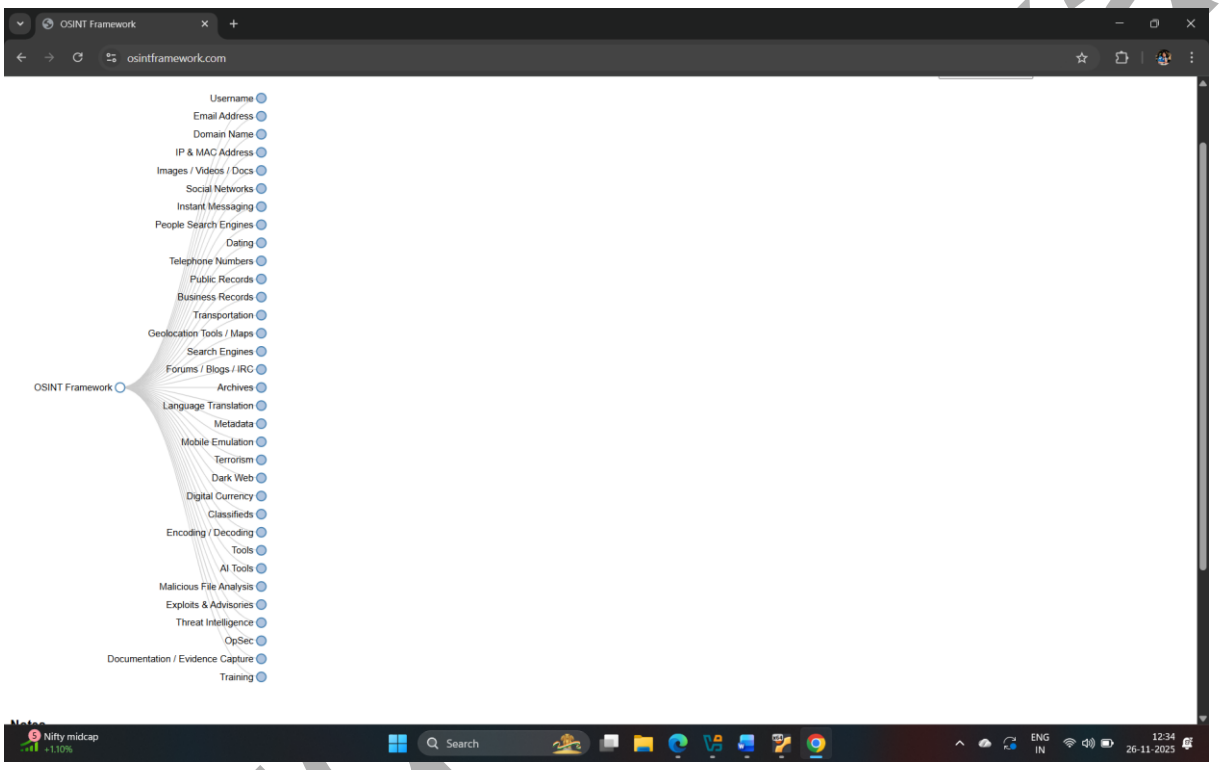
1.2

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 :

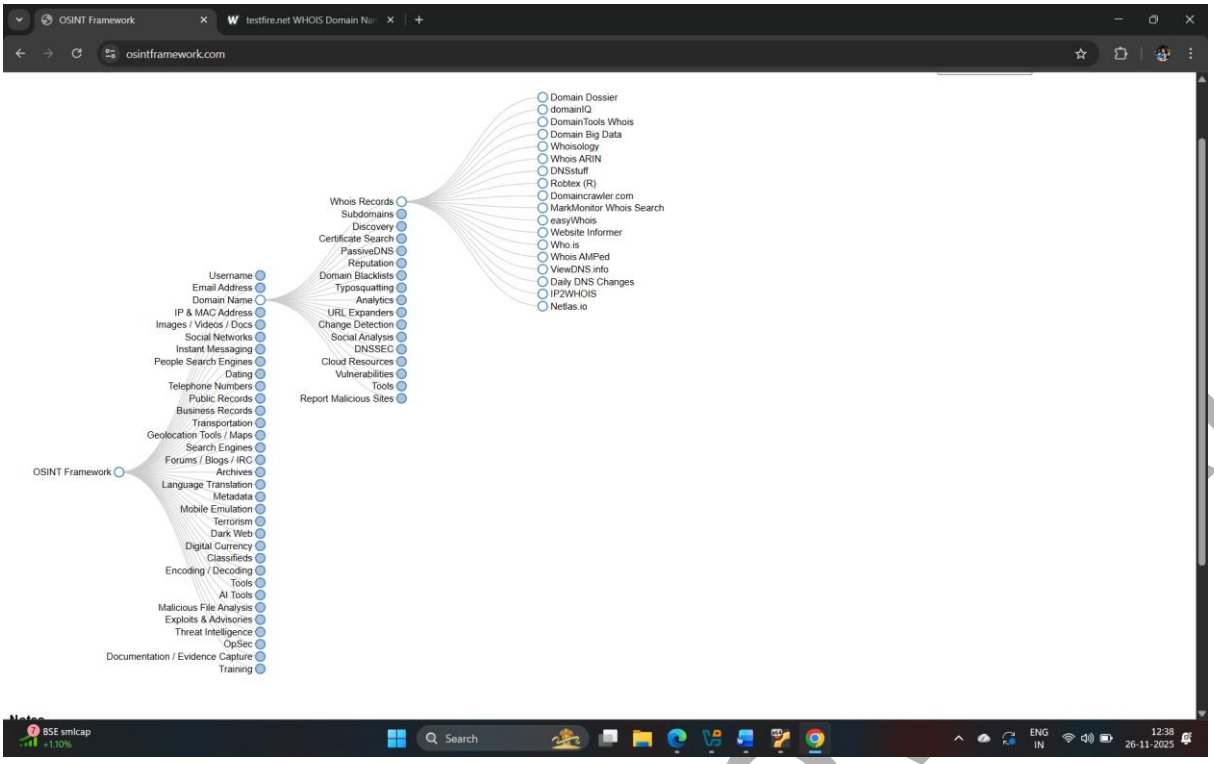
1. **Open browser.**
2. **Search OSINT Framework .**
3. **Choose domain name from all the frameworks.**



1.1

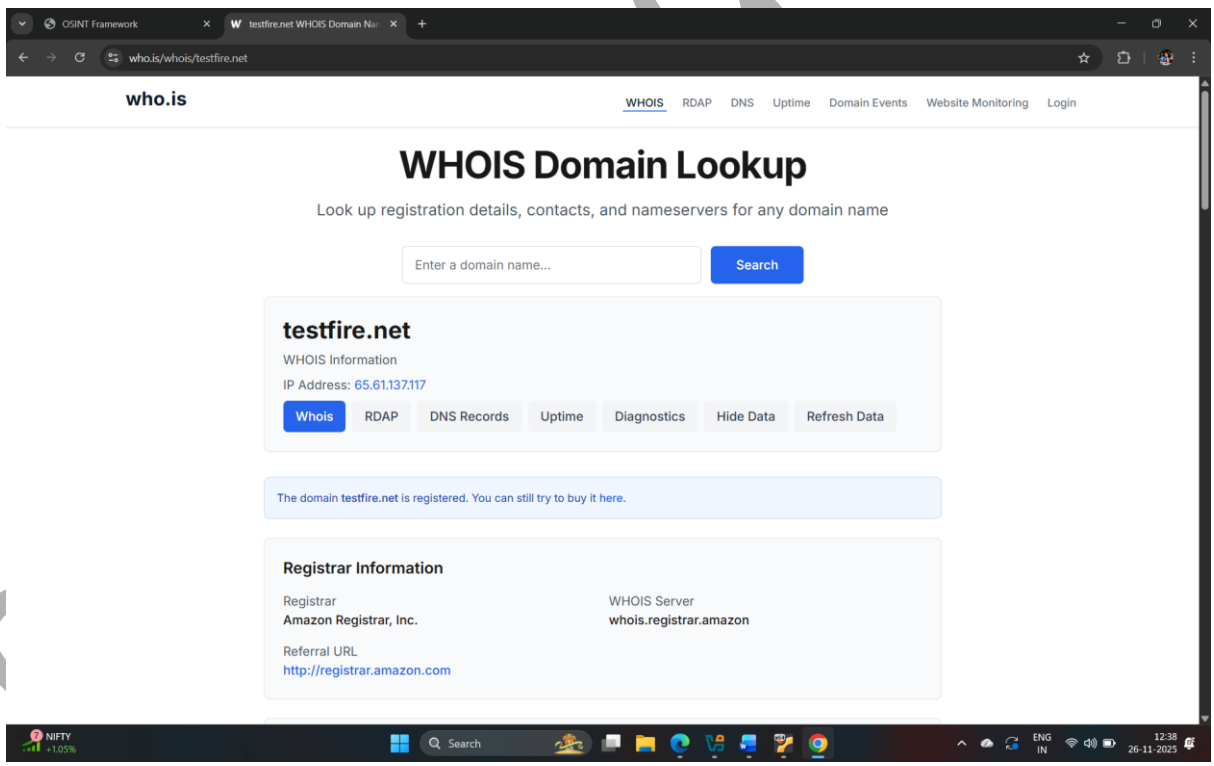
4. **Then click to whois records.**

mugdhakar



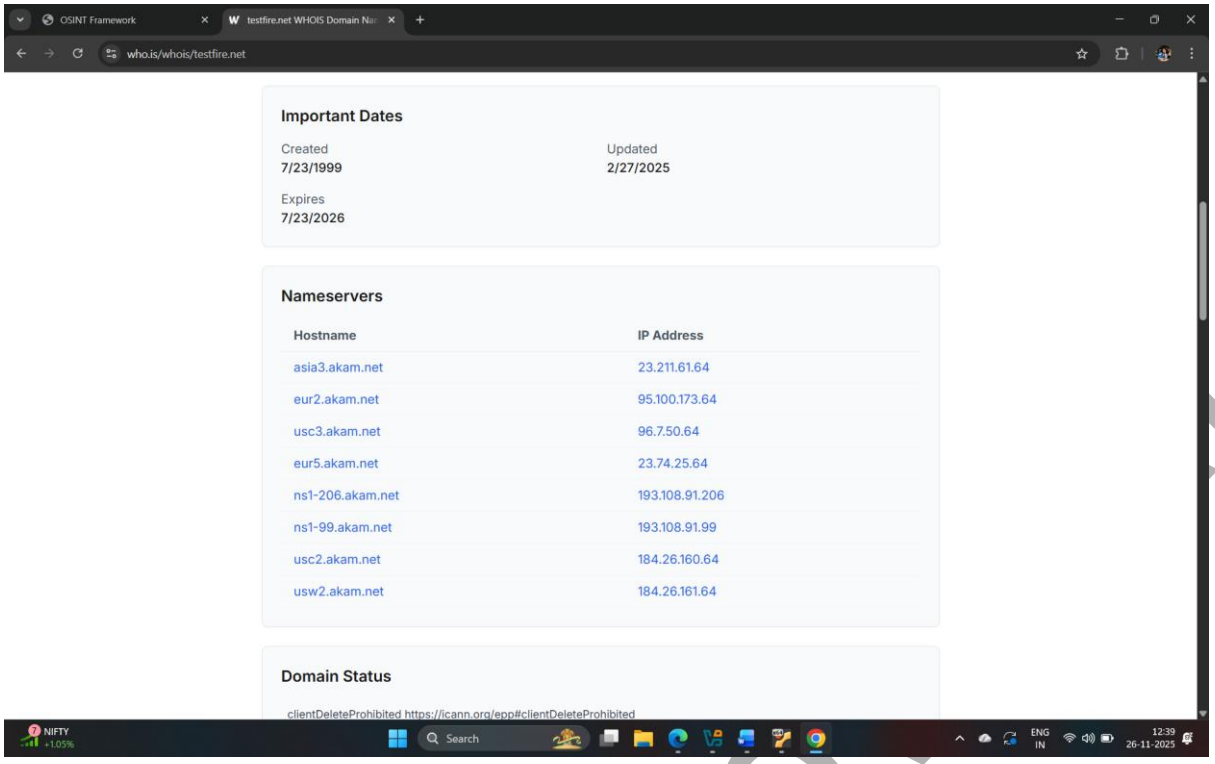
1.2

5. **Then click on who.is**

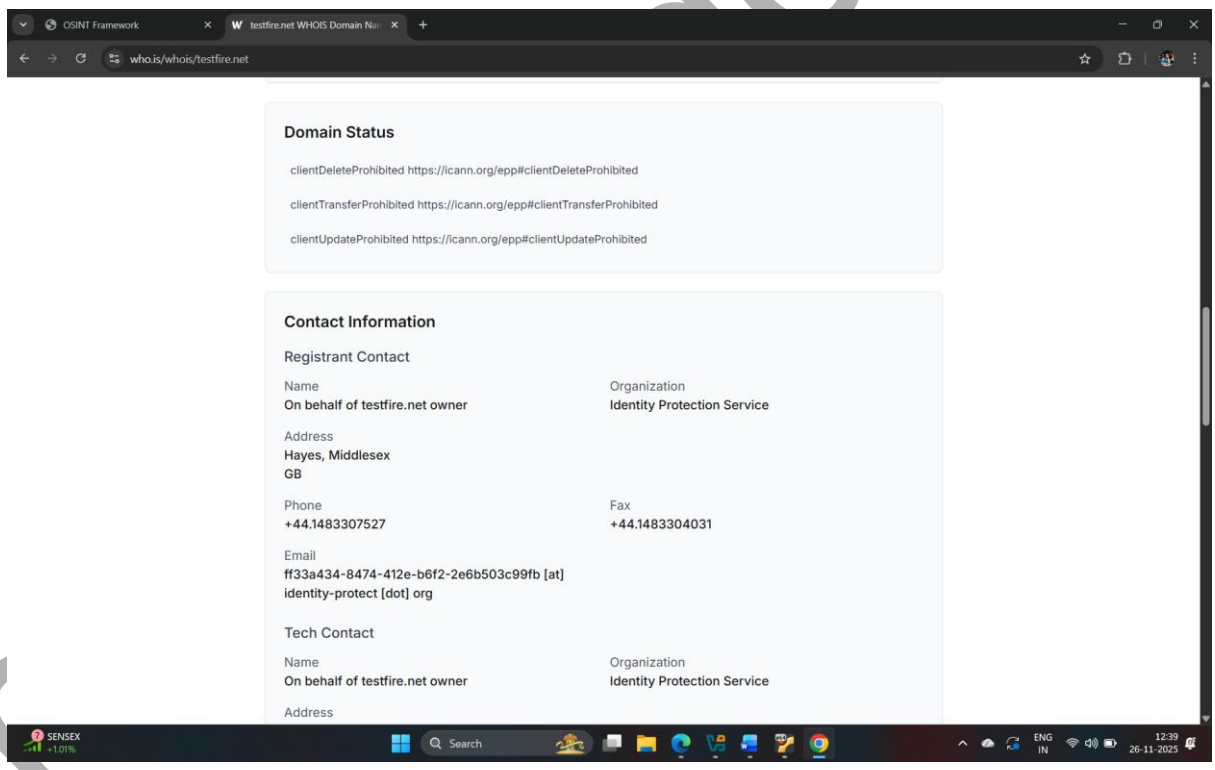


1.3

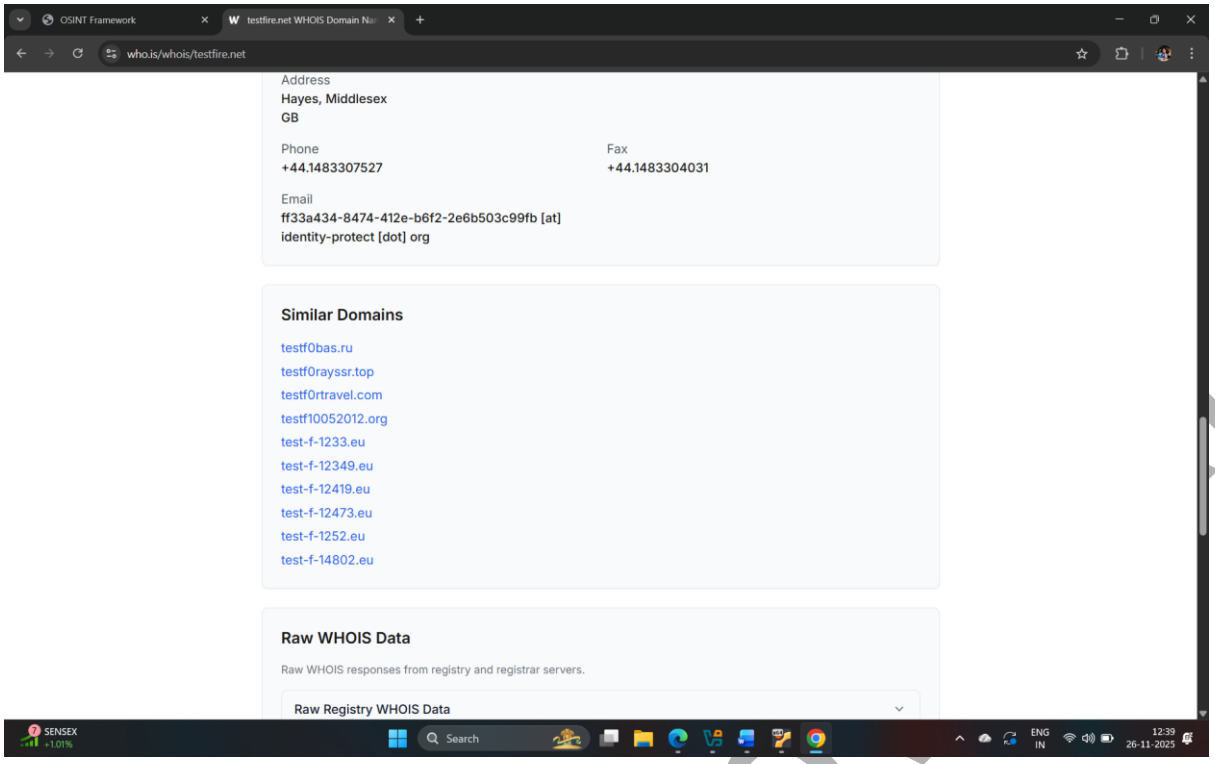
6. **Then run testfire.net in the search bar.**
7. **Then it starts giving information about testfire.net.**


OSINT Framework
testfire.net WHOIS Domain Na
who.is/whois/testfire.net
Important Dates
Created
7/23/1999
Updated
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
testfire.net WHOIS Domain Na
who.is/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
On behalf of testfire.net owner
Organization
Identity Protection Service
Address
Hayes, Middlesex
GB
Phone
+44.1483307527
Fax
+44.1483304031
Email
ff33a434-8474-412e-b6f2-2e6b503c99fb [at]
identity-protect [dot] org
Tech Contact
Name
On behalf of testfire.net owner
Organization
Identity Protection Service
Address
SENSEX
+1.01%
Search
ENG
IN
12:39
26-11-2025

1.5

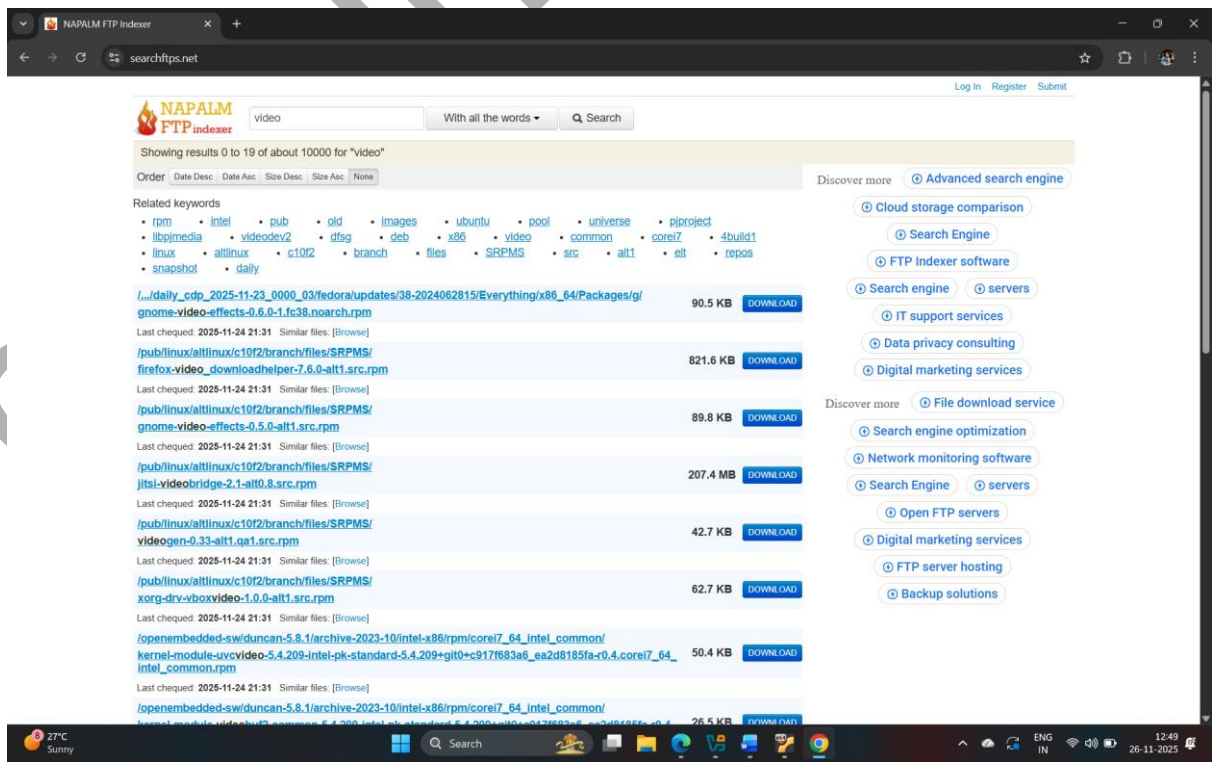


1.6

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

mugdhagovilkar