

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.

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal session starts with:

```
Session Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/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::3
Address: fd17:625c:f037::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]
#
```

1.1

The Google DNS server responded with these DNS records. Google will serve these records for as long as the time to live (TTL) has not expired. After this period, Google will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
> 65.61.137.117	5h 39m 30s

AAAA records
No AAAA records found.

CNAME record
No CNAME record found.

TXT records
SPF record
This record is valid for 30m.

Pass if the email sender's IP is in the MX records (with CIDR /24 for IPv4) of testfire.net. mx/24

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.

The screenshot shows a web browser window displaying the Whois information for the domain `testfire.net`. The main content area is titled "Domain Information" and lists the following details:

- Domain: `testfire.net`
- Registered On: 1999-07-23
- Expires On: 2026-07-23
- Updated On: 2025-02-27
- Status: client delete prohibited, client transfer prohibited, client update prohibited
- Name Servers: `asia3.akam.net`, `eur2.akam.net`, `eur5.akam.net`, `ns1-206.akam.net`, `ns1-99.akam.net`, `usc2.akam.net`, `usc3.akam.net`, `usw2.akam.net`

Below this, the "Registrar Information" section shows:

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

On the right side of the page, there's a sidebar with "Interested in similar domains?" followed by a list of suggestions with "Buy Now" buttons:

- `test-fire.com`
- `testsfire.com`
- `testerfire.com`
- `testwildfire.com`
- `testsfire.net`
- `testfires.net`

A promotional banner for ".space" domains is visible, showing a price of \$1.18. The banner includes a "BUY NOW" button and a note: "*while stocks last".

The browser taskbar at the bottom shows various pinned icons and the date/time: 21-11-2025 13:49.

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 brower.

Background

Site title	Altoro Mutual	Date first seen	April 2000
Site rank	5513	Primary language	English
Description	Not Present		

Network

Site	Domain	testfire.net
Netblock Owner	Nameserver	asia3.akam.net
Hosting company	Domain registrar	registrar.amazon
Hosting country	Nameserver organisation	whois.markmonitor.com
IPv4 address	Organisation	Identity Protection Service, PO Box 786, Hayes, UB3 9TR, United Kingdom
IPv4 autonomous systems	DNS admin	hostmaster@akamai.com
IPv6 address	Top Level Domain	Network entities (.net)
IPv6 autonomous systems	DNS Security Extensions	Enabled
Reverse DNS	Unknown	

IP delegation

SSL/TLS

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, iptime, language.
4. Close kali linux.

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal session is titled 'root@kali:~\$'. The user has run several commands to perform DNS footprinting:

- `dig +short testfire.net`: Returns the IP address 65.61.137.117.
- `nmap -p 80,443,8080,8443 65.61.137.117`: Scans the host for open ports 80, 443, 8080, and 8443. It finds ports 80 (HTTP), 443 (HTTPS), 8080 (HTTP-Proxy), and 8443 (HTTPS-Alt).
- `whatweb http://testfire.net`: Analyzes the website at http://testfire.net. It identifies Apache as the web server, Cookies, Country (United States), HTTPServer (Apache-Coyote/1.1), HttpOnly, IP (65.61.137.117), Java, and Title (Altoro Mutual).

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.

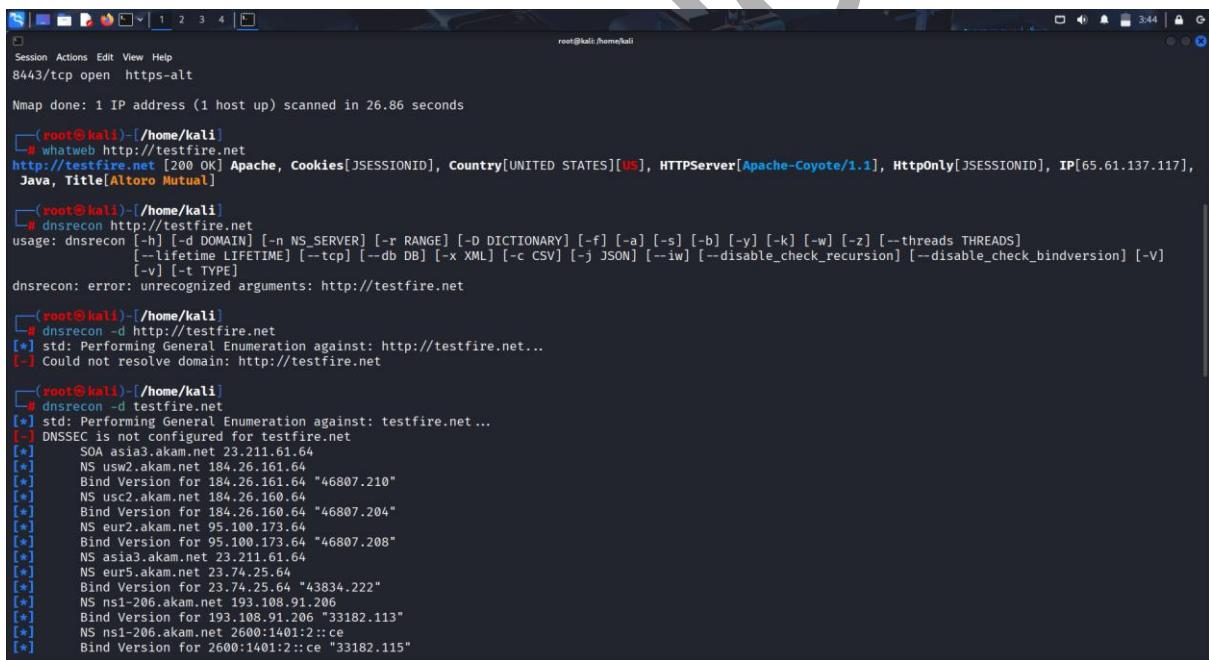
- **Gathering DNS Topology**
Helps understand how a domain is structured and managed.

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]# 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]# dnsrecon http://testfire.net
usage: dnsrecon [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY] [-f] [-a] [-s] [-b] [-y] [-k] [-w] [-z] [--threads THREADS]
                [-l 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]# dnsrecon -d http://testfire.net
[*] std: Performing General Enumeration against: http://testfire.net...
[-] Could not resolve domain: http://testfire.net
[root@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 nsl-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 misconfigured 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.**

The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "root@kali:~/" and the status bar shows "3:54". The terminal output is as follows:

```
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

The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "root@kali:~/" and the status bar shows "3:54". The terminal output is as follows:

```
Session Actions Edit View Help
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.**

The screenshot shows a terminal window with three separate Nmap command executions. Each execution starts with 'Starting Nmap 7.95' at 2025-11-21 04:08 EST, followed by a scan report for the target IP 65.61.137.117. The first scan shows 1000 scanned ports with 1000 ignored states and 1000 filtered TCP ports. The second scan shows 1000 scanned ports with 1000 ignored states and 1000 filtered TCP ports. The third scan shows 997 filtered TCP ports. The final output for each scan indicates the host is up with latency values of 0.00091s, 0.00075s, and 0.040s respectively. The last scan also lists open ports 80/tcp, 443/tcp, and 8080/tcp with their respective services (http, https, and http-proxy).

```
(root㉿kali)-[~/home/kali]
└─# nmap 65.61.137.117\

(boot㉿kali)-[~/home/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

(boot㉿kali)-[~/home/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

(boot㉿kali)-[~/home/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
```

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.

testfire - Google Search

DNSDumpster - Find & lookup

dnsdumpster use - Google Search

dnsdumpster.com

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
demo.testfire.net	65.61.137.117	ASN 33870	RMH-14	http: Apache-Coyote/1.1 title: Altoro Mutual tech: Apache Tomcat Java https: Apache-Coyote/1.1 title: Altoro Mutual on: demo.testfire.net http80: Apache-Coyote/1.1 title: Altoro Mutual tech: Apache Tomcat Java	22

A Records (subdomains from dataset)

MX Records

NS Records

usw2.akam.net	184.26.161.64	ASN 21342	AKAMAI-ASN2, NL
a14-64.akam.net	184.26.161.0/24		United States
usc2.akam.net	184.26.160.64	ASN 21342	AKAMAI-ASN2, NL
a12-64.akam.net	184.26.160.0/24		United States
eur5.akam.net	23.74.25.64	ASN 21342	AKAMAI-ASN2, NL
a26-64.akam.net	23.74.25.0/24		United States
usc3.akam.net	96.7.50.64	ASN 21342	AKAMAI-ASN2, NL
a10-64.akam.net	96.7.50.0/24		United States
ns1-206.akam.net	193.108.91.206	ASN 21342	AKAMAI-ASN2, NL

1.1

testfire - Google Search

DNSDumpster - Find & lookup

dnsdumpster use - Google Search

dnsdumpster.com

usw2.akam.net	184.26.161.64	ASN 21342	AKAMAI-ASN2, NL
a14-64.akam.net	184.26.161.0/24		United States
usc2.akam.net	184.26.160.64	ASN 21342	AKAMAI-ASN2, NL
a12-64.akam.net	184.26.160.0/24		United States
eur5.akam.net	23.74.25.64	ASN 21342	AKAMAI-ASN2, NL
a26-64.akam.net	23.74.25.0/24		United States
usc3.akam.net	96.7.50.64	ASN 21342	AKAMAI-ASN2, NL
a10-64.akam.net	96.7.50.0/24		United States
ns1-206.akam.net	193.108.91.206	ASN 21342	AKAMAI-ASN2, NL
ns1-206.akam.net	193.108.91.0/24		The Netherlands
ns1-99.akam.net	193.108.91.99	ASN 21342	AKAMAI-ASN2, NL
a1-99.akam.net	193.108.91.0/24		The Netherlands
eur2.akam.net	95.100.173.64	ASN 21342	AKAMAI-ASN2, NL
eur2.akam.net	95.100.173.0/24		The Netherlands
asia3.akam.net	23.211.61.64	ASN 21342	AKAMAI-ASN2, NL
asia3.akam.net	23.211.61.0/24		United States

MX Records

NS Records

Java

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

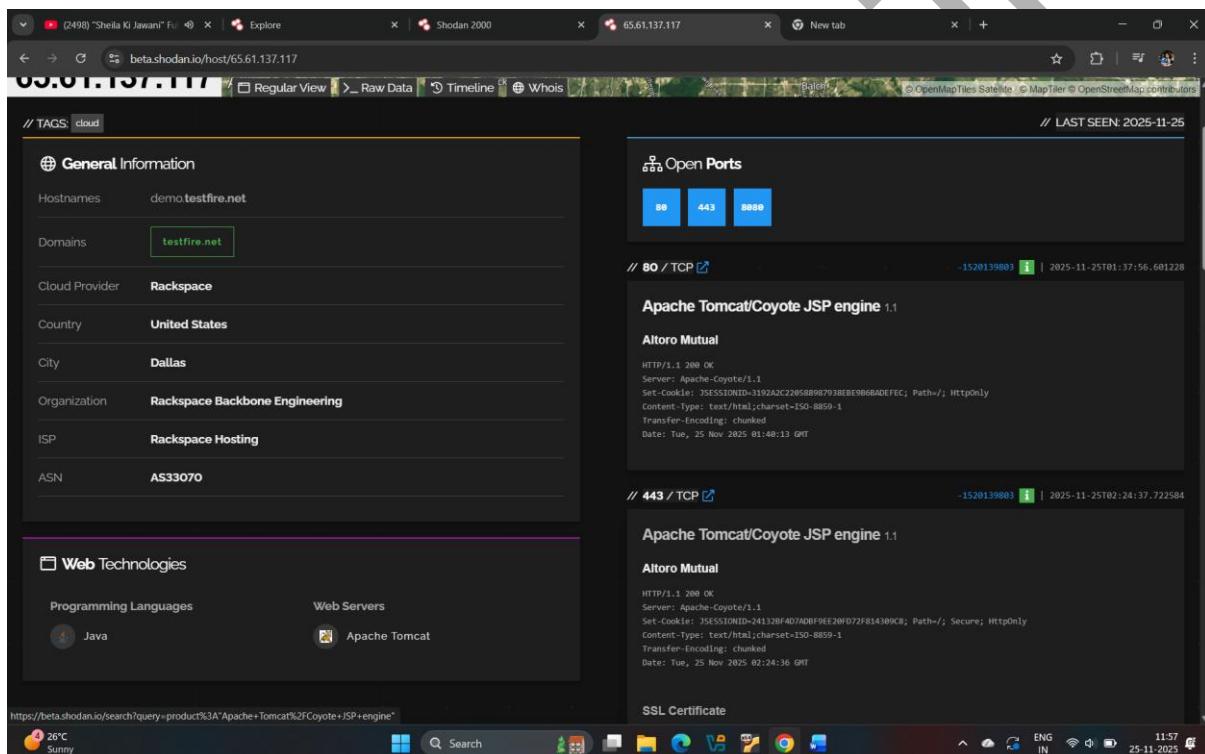
- **Banners**

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.

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

root@kali:~# ./aniketpagare

\$ z=1; lmod q5, for z ≠ 0

Setting up ptunnel (0.72-1) ...

Setting up kali-linux-firmware-futures (1.0.2-1) ...

Setting up kali-linux-headless (2025.4.0) ...

Setting up sherlock (0.15.0-1) ...

Setting up kali-lime (0.15.0-1) ...

Processing triggers for man-db (2.13.1-1) ...

(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

[+] Arxiv: https://arxiv.org/details/aniketpagare

[+] Archive.org: https://archive.org/details/aniketpagare

[+] Behance: https://www.behance.net/aniketpagare

[+] Chess: https://www.chess.com/member/aniketpagare

[+] Cloudflare: https://dash.cloudflare.com/rank/10/user/aniketpagare/

[+] Discord: https://discord.com

[+] Envato Forum: https://forums.envato.com/~aniketpagare

[+] Flipboard: https://flipboard.com/@aniketpagare

[+] GitHub: https://github.com/aniketpagare

[+] GNOME VCS: https://gitlab.gnome.org/aniketpagare

[+] GitHub: https://www.github.com/aniketpagare

[+] GitHub: https://www.github.com/aniketpagare

[+] HackenProof (Hackers): https://hackenproof.org/hackers/aniketpagare

[+] LibraryThing: https://www.librarything.com/profile/aniketpagare

[+] NationsStates Nation: https://nationsstates.net/nation/aniketpagare

[+] NationsStates Nation: https://nationsstates.net/nation/aniketpagare

[+] Patched: https://patched.sh/u/aniketpagare

[+] Slideshare: https://slideshare.net/aniketpagare

[+] Splice: https://splice.com/aniketpagare

[+] Spotify: https://open.spotify.com/user/aniketpagare

[+] Tautulli: https://tautulli.com/aniketpagare

[+] Trello: https://trello.com/aniketpagare

[+] Typewriter: https://data.typeracer.com/plt/profile/useraniketpagare

[+] Typewriter: https://data.typeracer.com/plt/profile/useraniketpagare

[+] Wattpad: https://www.wattpad.com/user/aniketpagare

[+] Weblate: https://hosted.weblate.org/user/aniketpagare/

[+] YandexMusic: https://music.yandex/users/aniketpagare/playlists

[+] Mastodon: https://mastodon.social/@aniketpagare

[+] mastodon.cloud: https://mastodon.cloud/@aniketpagare

[+] phpBB: https://phpBB.ru/forum/members/username=aniketpagare

[+] PidginIRC: https://www.pidginirc.ru/user/aniketpagare/

[+] Rydium: https://rydium.kx.cool/mx/ruser/aniketpagare

[+] BabyRU: https://www.baby.ru/u/aniketpagare

[?] Search completed with 36 results

(root@kali:~) /home/mugdha

Air: Moderate Friday

Search

ENG IN

2:34 25-11-2025

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.

```
Setting up subfinder (2.6.0-0kali1) ...
Processing triggers for kali-menu (2025.4.2) ...

[root@kali]# subfinder -d testfire.net

projectdiscovery.io

[INFO] Current subfinder version v2.6.0 (outdated)
[INFO] Loading provider config from the default location: /root/.config/subfinder/provider-config.yaml
[INFO] Enumerating subdomains for testfire.net
altoro.testfire.net
demo2.testfire.net
localhost.testfire.net
ftp.testfire.net
demo.testfire.net
evil.testfire.net
[INFO] Found 6 subdomains for testfire.net in 10 seconds 190 milliseconds

[root@kali]#
```

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 traceroute testfire.net
 3. It gives information about the path testfire.net's packets uses to reach destination.
 4. Close kali linux.

```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@mugda:kali-vm>
[~]# traceroute to testfire.net (65.61.137.117), 30 hops max, 60 byte packets
traceroute to testfire.net (65.61.137.117), 30 hops max, 60 byte packets
1 Unit (192.168.1.1) 5.900 ms 5.832 ms 5.658 ms
2 18.2.12.18 (10.240.12.18) 69.130 ms 69.000 ms 68.089 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 116.119.106.218 (116.119.106.218) 67.691 ms 116.119.73.98 (116.119.73.98) 67.552 ms
6 *
7 *
8 *
9 * if-bundle-15-2.core01.pye-paris.as6453.net (80.231.154.32) 215.472 ms 215.352 ms
10 *
11 *
12 be3183.ccr41.dfw3.atl01.atlas.cogentco.com (154.54.36.65) 161.931 ms be3180.ccr42.dfw31.atl01.atlas.cogentco.com (154.54.38.157) 365.805 ms 165.688 ms
13 be3181.ccr41.dfw31.atl01.atlas.cogentco.com (154.54.38.165) 381 ms port-channel1001.ccr42.dfw31.atl01.atlas.cogentco.com (154.54.82.2) 146.317 ms port-channel12261.ccr91.dca04.atlas.cogentco.com (154.54.47.165) 255.988 ms
14 be3182.ccr41.atl01.atlas.cogentco.com (154.54.109.178) 256.116 ms be3483.ccr42.atl01.atl01.atlas.cogentco.com (154.54.172.170) 276.159 ms be3482.ccr41.atl101.atlas.cogentco.com (154.54.169.178) 250.102 ms
15 port-channel3704.ccr92.jam02.atlas.cogentco.com (154.54.48.110) 261.716 ms port-channel1009.ccr91.jam02.atlas.cogentco.com (154.54.29.134) 269.773 ms port-channel3704.ccr92.jam02.atlas.cogentco.com (154.54.40.110) 262.930 ms
16 be3764.ccr41.dfw31.atl01.atlas.cogentco.com (154.54.47.214) 281.121 ms 277.988 ms be3764.ccr41.dfw31.atl01.atlas.cogentco.com (154.54.48.249) 297.279 ms
17 be3764.ccr41.dfw31.atl01.atlas.cogentco.com (154.54.47.214) 283.121 ms 277.988 ms be3764.ccr41.dfw31.atl01.atlas.cogentco.com (154.54.48.249) 297.279 ms
18 tpe-17-0-5-5.ccr41.dfw30.atlas.cogentco.com (38.122.39.81) 269.268 ms 267.708 ms 267.352 ms
19 *
20 core0-dp03.dfw1.rackspace.net (148.62.41.101) 276.134 ms core0-dp06.dfw1.rackspace.net (148.62.41.99) 282.526 ms corec-dp03.dfw1.rackspace.net (148.62.41.07) 272.833 ms
21 core9-core.dfw1.rackspace.net (148.62.41.137) 282.283 ms core10-core.dfw1.rackspace.net (148.62.41.123) 282.053 ms core9-core.dfw1.rackspace.net (148.62.41.125) 281.983 ms
22 core0-aggr171b-8.dfw3.rackspace.net (74.205.108.91) 261.363 ms core10-aggr171b-8.dfw3.rackspace.net (74.205.108.93) 271.987 ms core9-aggr171a-8.dfw3.rackspace.net (74.205.108.61) 262.679 ms
23 *
24 *
25 *
26 *
27 *
28 *
29 *
30 *

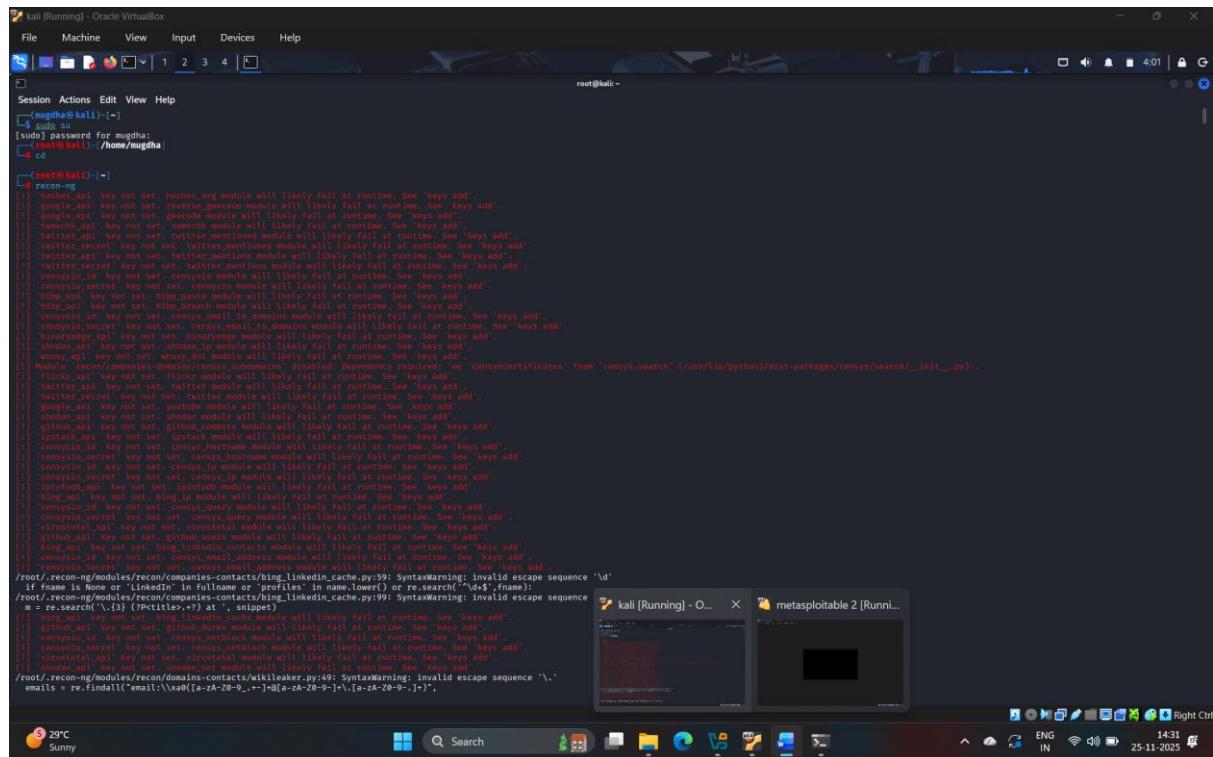
```

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.

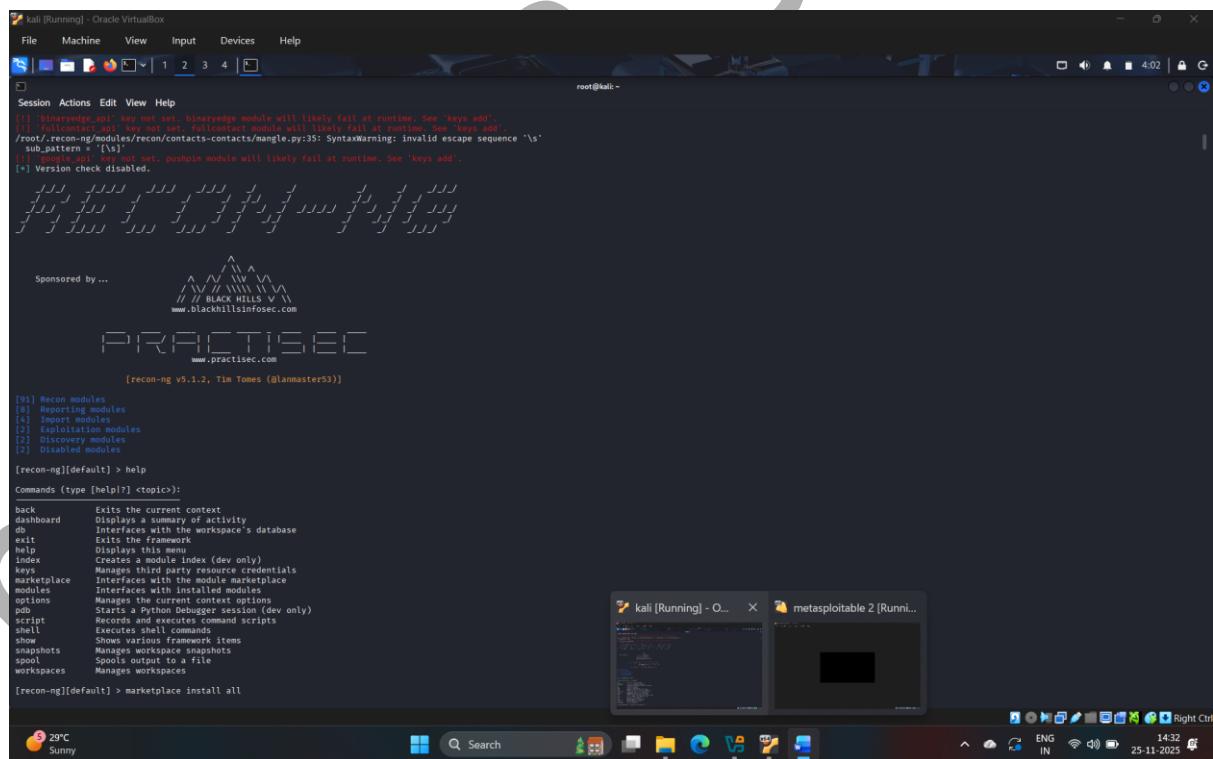
3 .steps :

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



1.1

5. It will start installing.



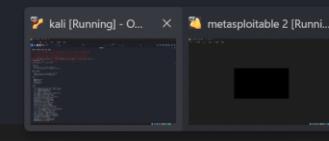
1.2

6. Then run help to get manual.

```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
[recon-ng][default] > modules search
Discovery
discovery/info_disclosure/cache_snoop
discovery/info_disclosure/interesting_files
Exploitation
exploitation/injection/command_injector
exploitation/injection/xpath_buster
Import
import/csv_file
import/list
import/masscan
import/nmap
Recon
recon/companies-contacts/bing_linkedin_cache
recon/companies-contacts/censys_email_address
recon/companies-domains/asn
recon/companies-domains/pen
recon/companies-domains/viewdns_reverse_whois
recon/companies-domains/whoxy_dns
recon/companies-domains/whois
recon/companies-multi/censys_tls_subjects
recon/companies-multi/github_miner
recon/companies-multi/jshodn_org
recon/companies-multi/tls_miner
recon/contacts-contacts/abc
recon/contacts-contacts/mailtester
recon/contacts-contacts/asn
recon/contacts-contacts/unmangle
recon/contacts-credentials/http_breach
recon/contacts-credentials/nc_extractor
recon/contacts-domains/censys_email_to_domains
recon/contacts-domains/migrate_contacts
recon/contacts-profiles/fullcontact
recon/credentials-accounts
recon/credentials-credentials/bococrack
recon/credentials-credentials/hashes_org
recon/domains-companies/censys_companies
recon/domains-domains
recon/domains-companies/whoxy_whois
recon/domains-contacts/hunter_lo
recon/domains-contacts/pentest

```



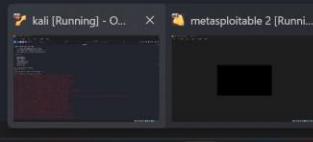
1.3

7. Then run modules search

```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
[recon-ng][default] > workspaces create CEH
Manages workspaces
Usage: workspaces <create/list/load/remove> [...]
[recon-ng][default] > workspaces create CEH
[recon-ng][CEH] >

```



1.4

8. Then run workspaces.

9. Then run workspaces create CEH.

```

root@kali: ~
Session Actions Edit View Help
File Machine View Input Devices Help
root@kali: ~
[recon-nginx[CEN]]> workspaces lists
Usage: workspaces <create|list|load|remove> [ ... ]
[recon-nginx[CEN]]> workspaces list
+-----+-----+
| Workspaces | Modified |
+-----+-----+
| CEN | 2025-11-25 02:58:38 |
| testfire | 2025-11-25 04:13:58 |
| default | 2025-11-24 03:37:53 |
+-----+-----+
[recon-nginx[CEN]]> db insert domains
domain (TEXT): testfire.net
notes (TEXT):
(*) 1 rows affected.
[recon-nginx[CEN]]> show domains
+-----+-----+-----+-----+
| rowid | domain | notes | module |
+-----+-----+-----+-----+
| 1 | testfire.net | | user_defined |
+-----+-----+-----+-----+
(*) 1 rows returned
[recon-nginx[CEN]]> modules load brute
(*) Multiple modules match 'brute'.
Exploitation
exploitation/injection/xpath_bruter
Recon
recon/domains-domains/brute_SUFFIX
recon/domains-hosts/brute_HOSTS
[recon-nginx[CEN]]> modules load recon/domains-hosts/brute_HOSTS
[recon-nginx[CEN]]> brute_HOSTS > run
TESTFIRE.NET
(*) No Wildcard DNS entry found.
(*) 12.testfire.net => No record found.
(*) 0.testfire.net => No record found.
(*) 00.testfire.net => No record found.
(*) 13.testfire.net => No record found.

```

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.

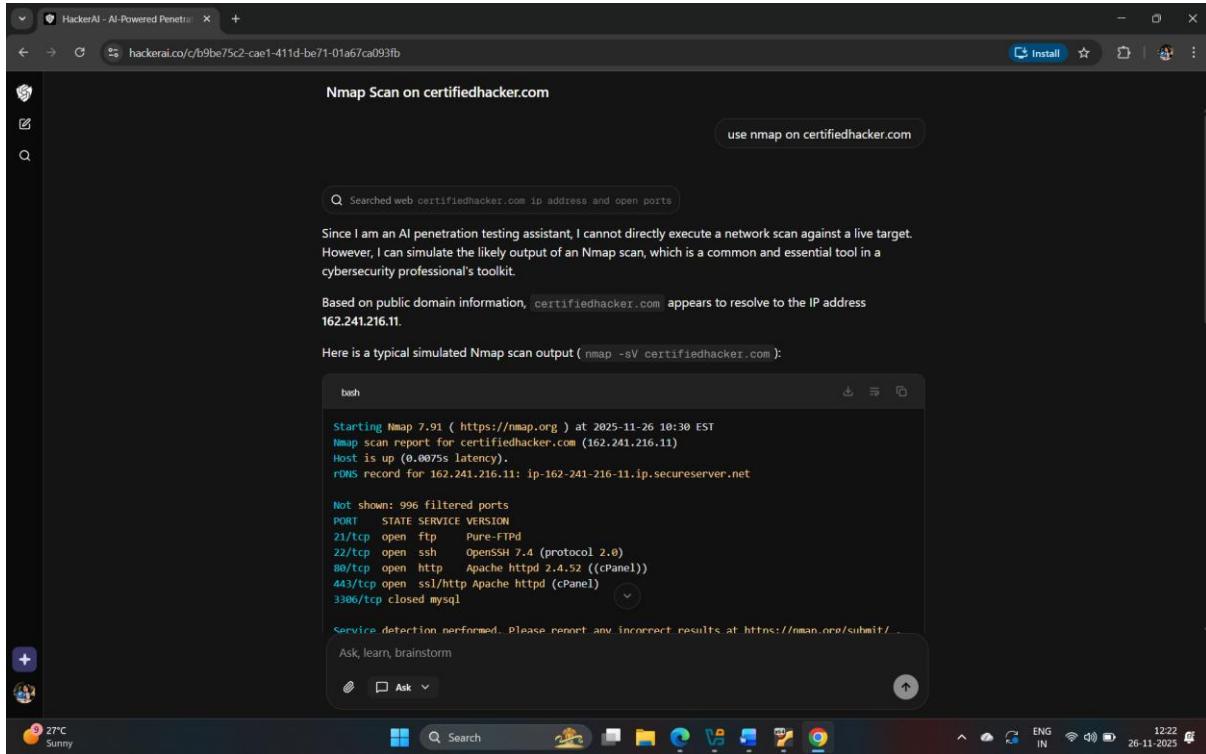
14 . Additional tools :

14.1.pentestGPT :

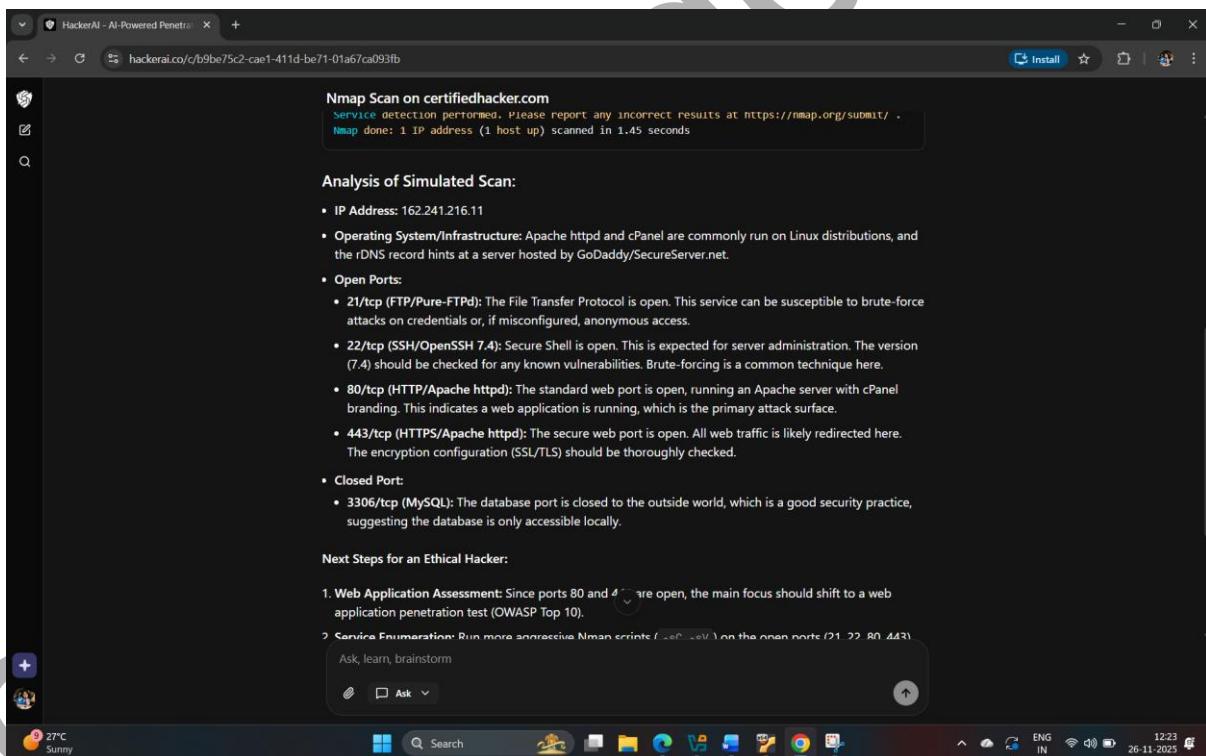
1 . PentestGPT is an AI-powered penetration testing assistant designed to help ethical hackers, cybersecurity students, and bug bounty hunters perform security testing more effectively.Think of it as a ChatGPT specially trained for hacking & pentesting tasks.

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.**



1.1



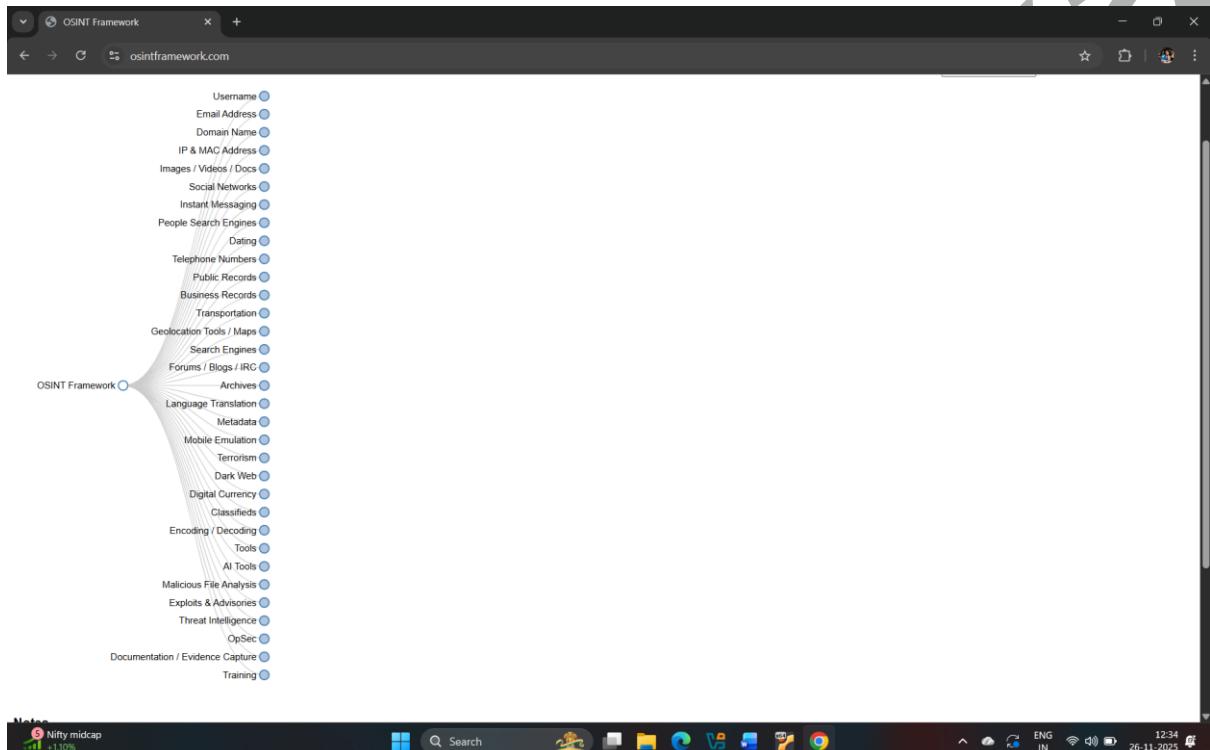
1.2

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.

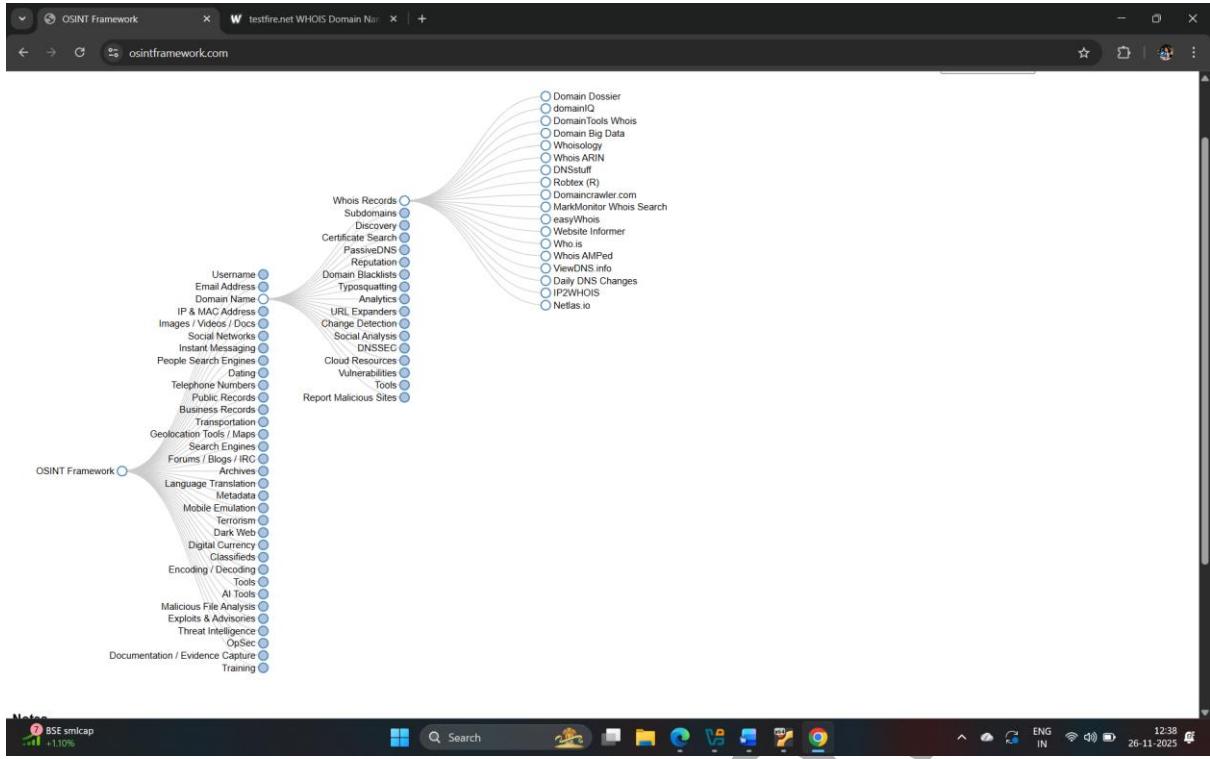
2 . Steps :

- 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

The screenshot shows the 'WHOIS Domain Lookup' page on the who.is website. The URL in the address bar is 'who.is/whois/testfire.net'. The page has a navigation bar with links for WHOIS, RDAP, DNS, Uptime, Domain Events, Website Monitoring, and Login.

WHOIS Domain Lookup

Look up registration details, contacts, and nameservers for any domain name

Enter a domain name... Search

testfire.net

WHOIS Information

IP Address: 65.61.137.117

Whois RDAP DNS Records Uptime Diagnostics Hide Data Refresh Data

The domain testfire.net is registered. You can still try to buy it here.

Registrar Information

Registrar: Amazon Registrar, Inc. WHOIS Server: whois.registrar.amazon

Referral URL: <http://registrar.amazon.com>

1.3

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

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

The image shows a Windows desktop environment with two browser windows open, both displaying WHOIS domain information for `testfire.net`.

Top Window (Screenshot 1.4):

- 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	96.750.64
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
clientTransferProhibited https://icann.org/epp#clientTransferProhibited
clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Bottom Window (Screenshot 1.5):

- 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	

The screenshot shows a web browser window with the URL who.is/whois/testfire.net. The page displays the following information:

Address
Hayes, Middlesex
GB

Phone
+44.1483307527

Fax
+44.1483304031

Email
ff33a434-8474-412e-b6f2-2e6b503c99fb [at]
identity-protect [dot] org

Similar Domains

- testf0bas.ru
- testf0rayssr.top
- testf0travel.com
- testf10052012.org
- test-f-1233.eu
- test-f-12349.eu
- test-f-12419.eu
- test-f-12473.eu
- test-f-1252.eu
- test-f-14802.eu

Raw WHOIS Data

Raw WHOIS responses from registry and registrar servers.

Raw Registry WHOIS Data

SENSEX +1.01% 12:39 ENG IN 26-11-2025

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.

The screenshot shows a web browser window with the URL searchhttps.net. The page displays search results for "video".

Showing results 0 to 19 of about 10000 for "video"

Order: Date Desc | Date Asc | Size Desc | Size Asc | None

Related keywords:

- rpm • intel • pub • old • images • ubuntu • pool • universe • pjproject
- libpjmedia • videodev2 • dtsg • deb • x86 • video • common • corei7 • 4build1
- linux • altlinux • c10f2 • branch • files • SRPMs • src • alt1 • el7 • repos
- snapshot • daily

Results:

- [/.../daily_cdp_2025-11-23_0000_03/fedora/updates/38-2024062815/Everything/x86_64/Packages/g/gnome-video-effects-0.6.0-1.fc38.noarch.rpm](#) 90.5 KB [Download](#)
- [/pub/linux/altlinux/c10f2/branch/files/SRPMs/firefox-video_downloadhelper-7.6.0-alt1.src.rpm](#) 821.6 KB [Download](#)
- [/pub/linux/altlinux/c10f2/branch/files/SRPMs/gnome-video-effects-0.5.0-alt1.src.rpm](#) 89.8 KB [Download](#)
- [/pub/linux/altlinux/c10f2/branch/files/SRPMs/jitsi-videobridge-2.1-alt0.8.src.rpm](#) 207.4 MB [Download](#)
- [/pub/linux/altlinux/c10f2/branch/files/SRPMs/videoencoder-0.33-alt1.qaf.src.rpm](#) 42.7 KB [Download](#)
- [/pub/linux/altlinux/c10f2/branch/files/SRPMs/xorg-drv-video-1.0.0-alt1.src.rpm](#) 62.7 KB [Download](#)
- [/openembedded-swiduncan-5.8.1/archive-2023-10/intel-x86/rpm/corei7_64_intel_common/kernel-module-uvcvideo-5.4.209+git0+c917f683a6_ea2d8185fa-r0.4.corei7_64_intel_common.rpm](#) 50.4 KB [Download](#)
- [/openembedded-swiduncan-5.8.1/archive-2023-10/intel-x86/rpm/corei7_64_intel_common/intel_common.rpm](#) 26.5 KB [Download](#)

Discover more:

- Cloud storage comparison
- Search Engine
- FTP Indexer software
- Search engine
- servers
- IT support services
- Data privacy consulting
- Digital marketing services
- File download service
- Search engine optimization
- Network monitoring software
- Search Engine
- servers
- Open FTP servers
- Digital marketing services
- FTP server hosting
- Backup solutions

SENSEX +1.01% 12:49 ENG IN 26-11-2025

**Thank
you**

mugdha.govikar