****

**MODULE – 2**

**FOOTPRINTING RECONNAISSANCE**

**- Mahesh Najan**

|  |  |  |
| --- | --- | --- |
| **Sr Number** | **Module Name** | **Page Number** |
|  | **Footprinting Reconnaissance** | 2 |
| 1 | **Footprinting and its Type** | 3 |
| 2 | **Footprinting via Search Engines** | 4 |
| 3 | **Footprinting via Social Media** | 7 |
| 4 | **WHOIS Footprinting vs DNS Footprinting** | 9 |
| 5 | **Footprinting via Whois** | 10 |
| 6 | **Footprinting via DNS** | 14 |
| 7 | **Network Footprinting** | 19 |
| 8 | **Email Footprinting** | 21 |

**FOOTPRINTING :**

Collecting information about a target system, network, or organization is gathered. It is also called reconnaissance or information gathering.

# **TYPES :**

1. Passive Footprinting

Definition: Collecting information about the target without directly interacting with its systems. It’s stealthy, so the target usually doesn’t know it’s happening.

**Methods of Passive Footprinting:**

* Search Engines (Google Hacking / Google Dorks)
* WHOIS Lookup
* DNS Footprinting
* Social Media Footprinting
* Job Portals & Forums
* Website Information Gathering

2. Active Footprinting

**Definition:** Involves **direct interaction** with the target system/network to extract information. It is riskier because it can be detected.

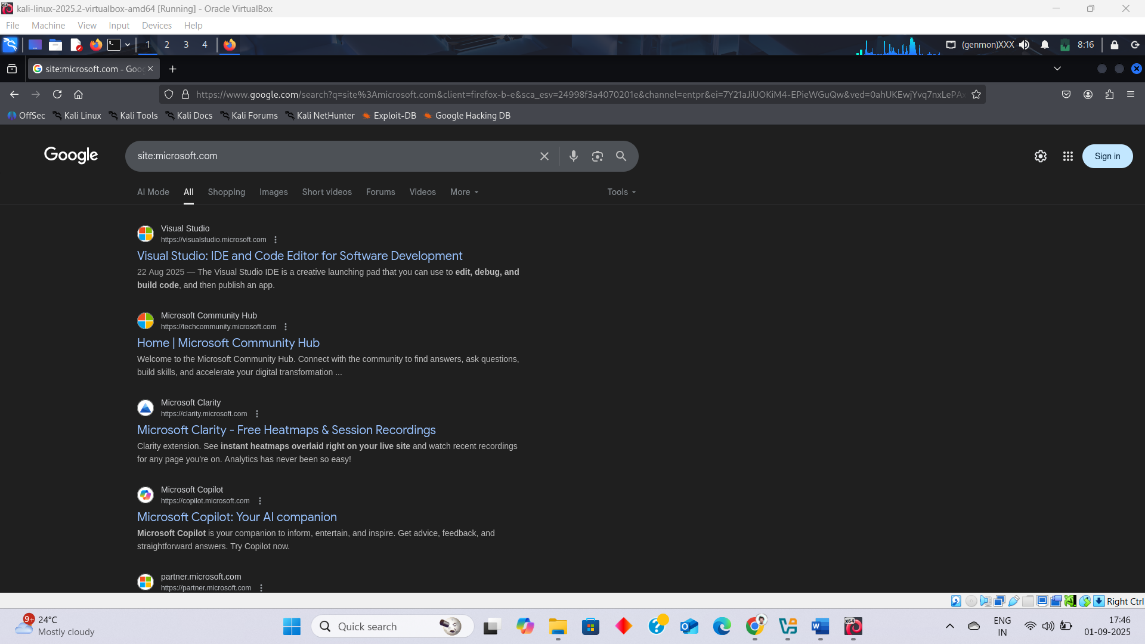
**Methods of Active Footprinting:**

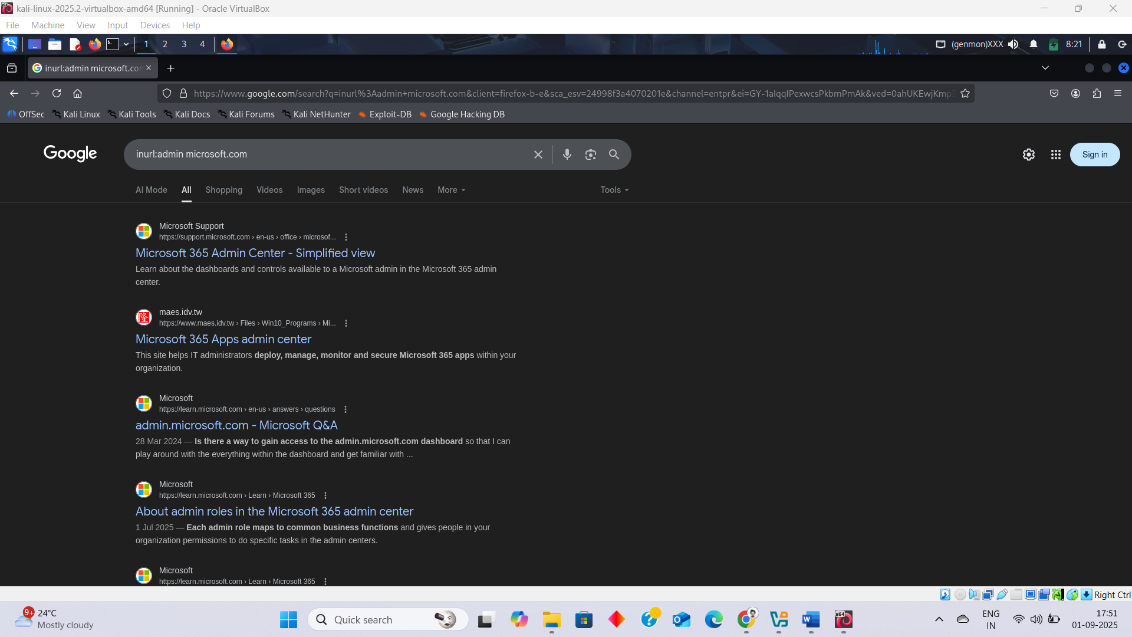
* Ping Sweep / ICMP Scanning
* Port Scanning (Nmap, Netcat)
* DNS Zone Transfer (dig / nslookup)
* Network Footprinting
* Email Footprinting
* Banner Grabbing

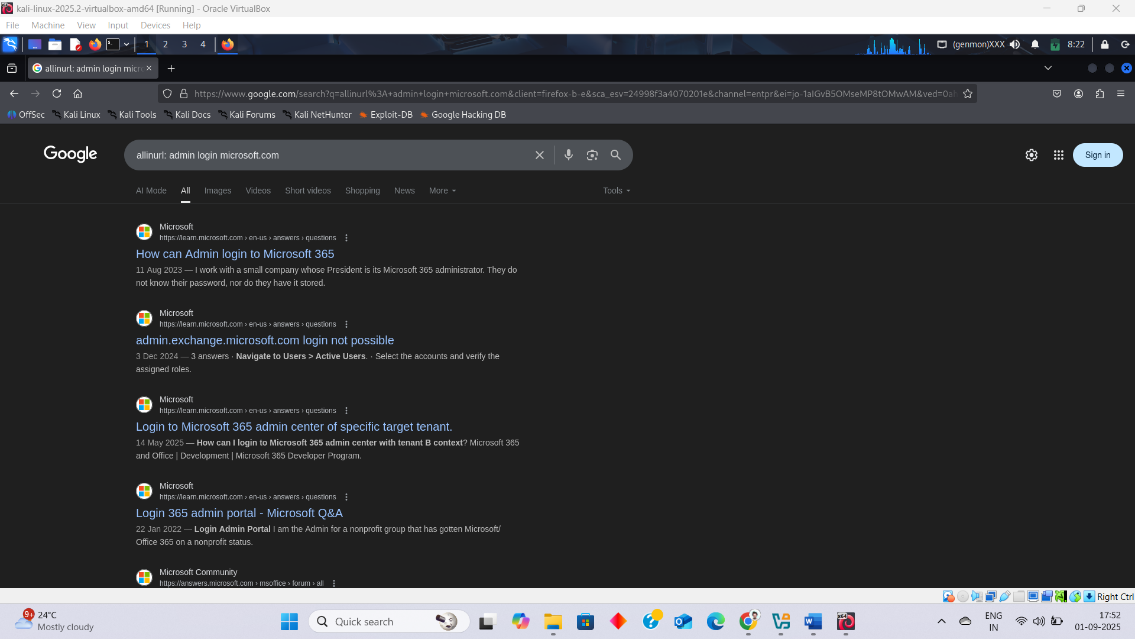
# **Footprinting via Search Engines :**

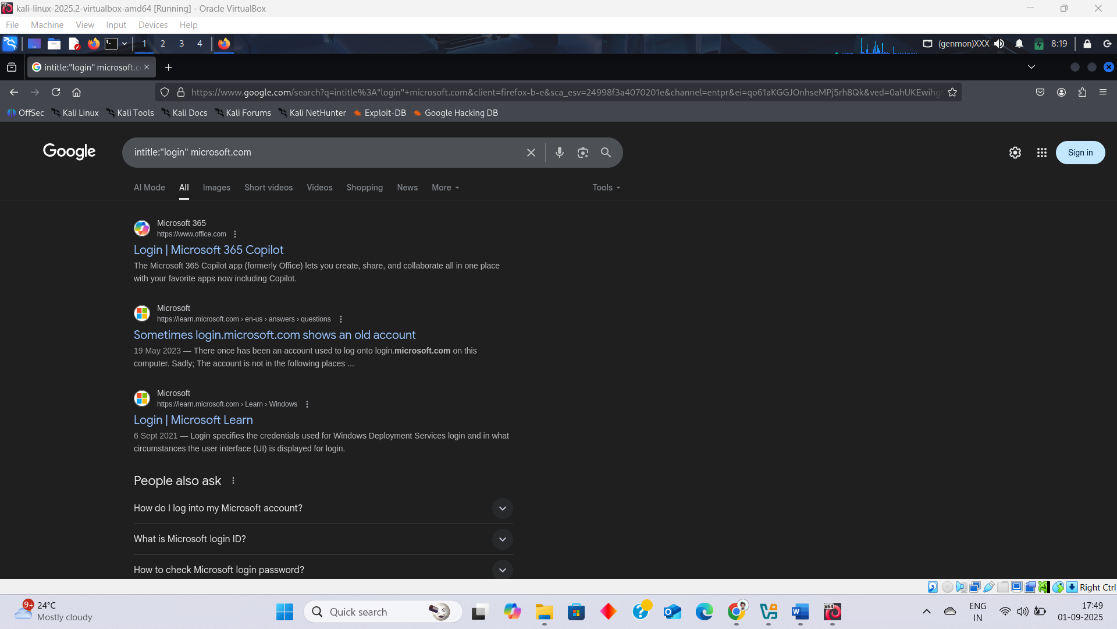
1. **Google Dorking :** Google Dorking (also called Google Hacking) it is used advanced Google search to find hidden, sensitive, or useful information that is publicly available but not easily visible through normal searches.

| Operator | Example | Description |
| --- | --- | --- |
| site: | site:microsoft.com | Shows all indexed pages from a domain |
| intitle: | intitle:"login" | Finds pages with “login” in the title |
| inurl: | inurl:admin | Finds pages with “admin” in the URL |
| allinurl: | allinurl: admin login | Finds URLs containing multiple keywords |
| allintitle: | allintitle: security report | Finds titles containing multiple keywords |
| filetype: OR ext: | filetype:pdf site:microsoft.com | Searches for specific file types (pdf, xls, docx, ppt, sql, etc.) |
| cache: | cache:microsoft.com | Shows Google’s cached version of a page |
| \* | "admin \* panel" | Wildcard for unknown words |

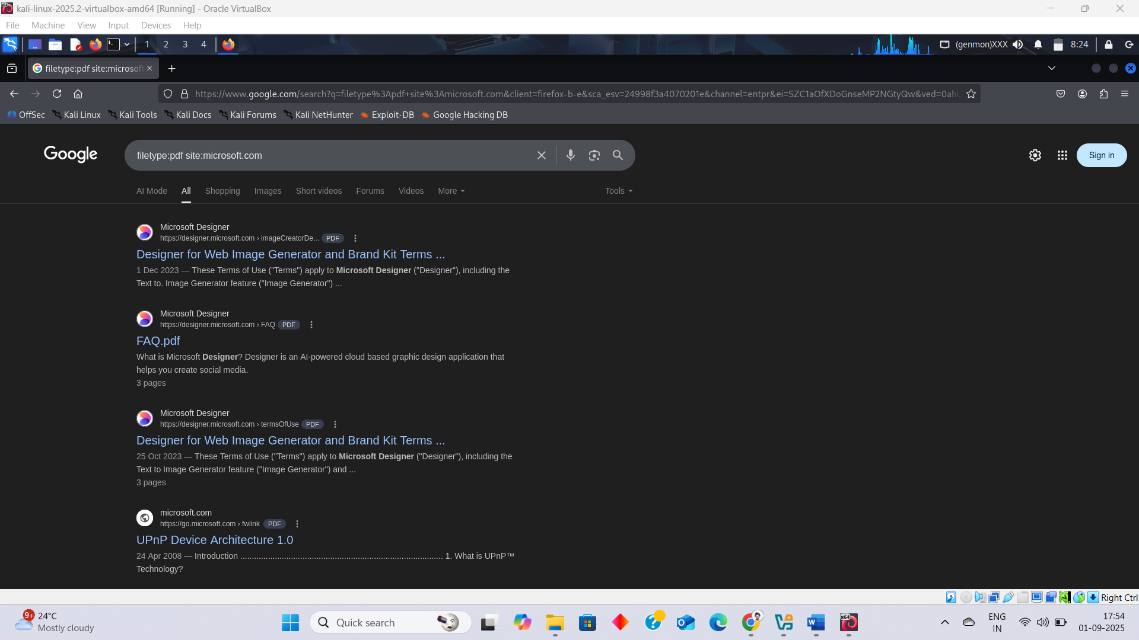






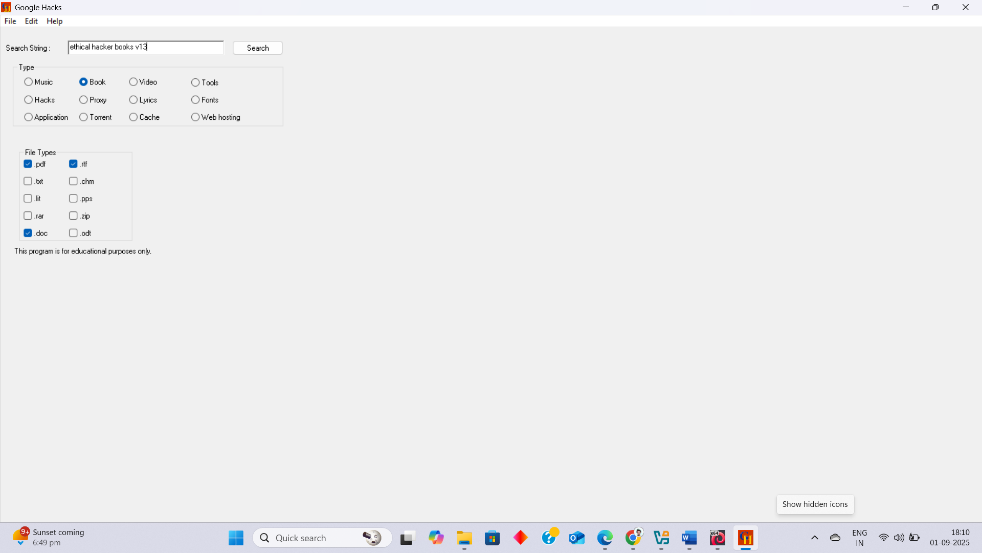


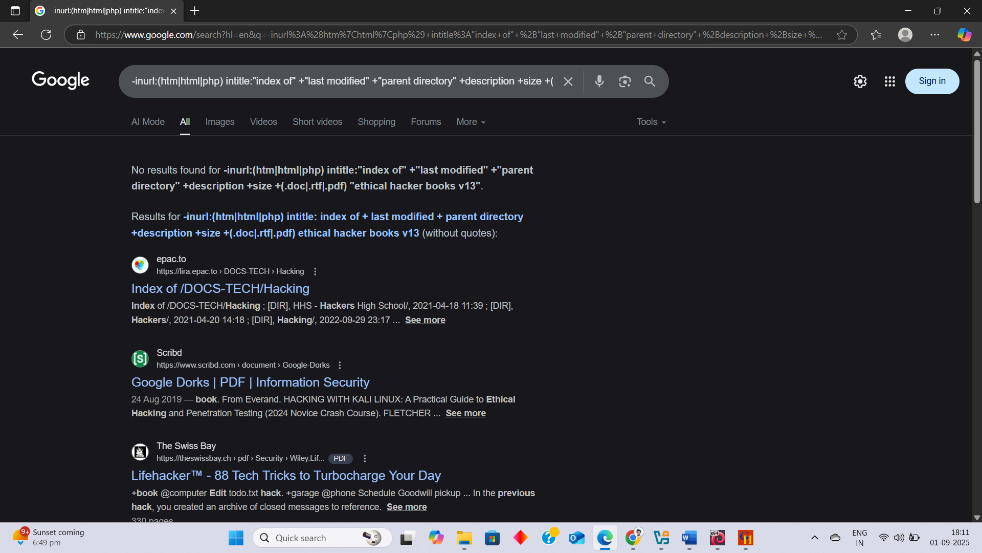




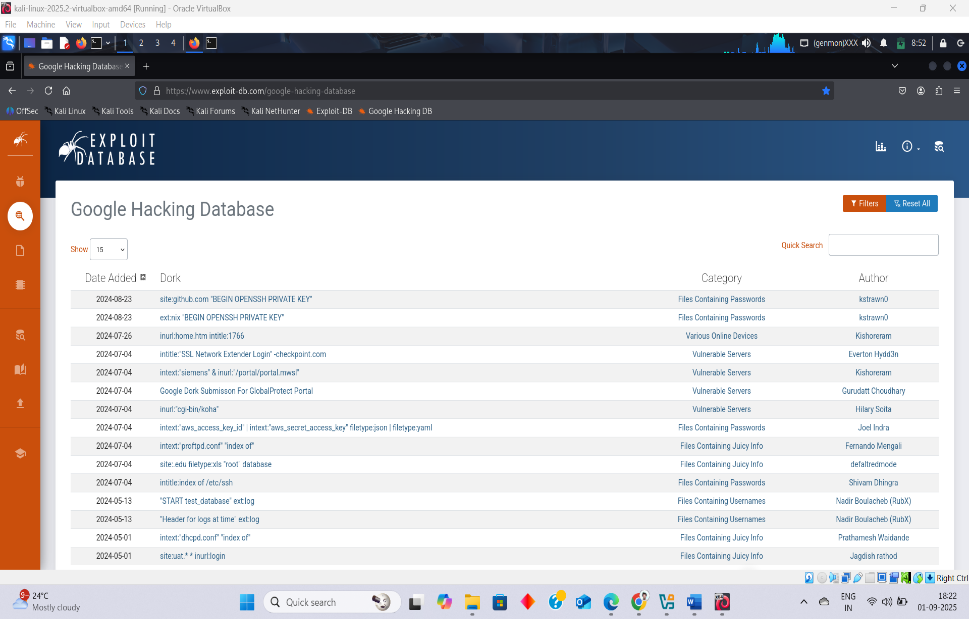
**Similar tools/Website:**

* Google Hack Tool : Google Hack to discover sensitive information exposed on websites. It is an essential tool in ethical hacking and penetration testing for footprinting and information gathering. **“By giving a prompt, it gives a result.”**





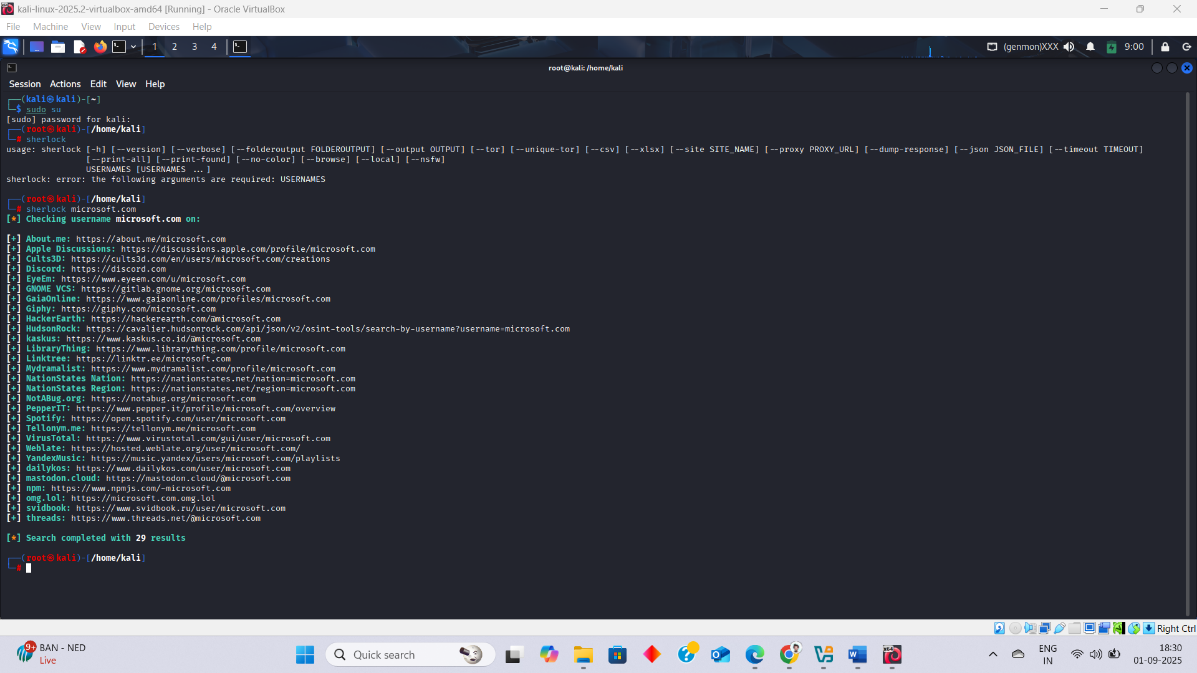
* Google Hacking DB : **“It is similar to google Hack”**



# **Footprinting via Social Media :**

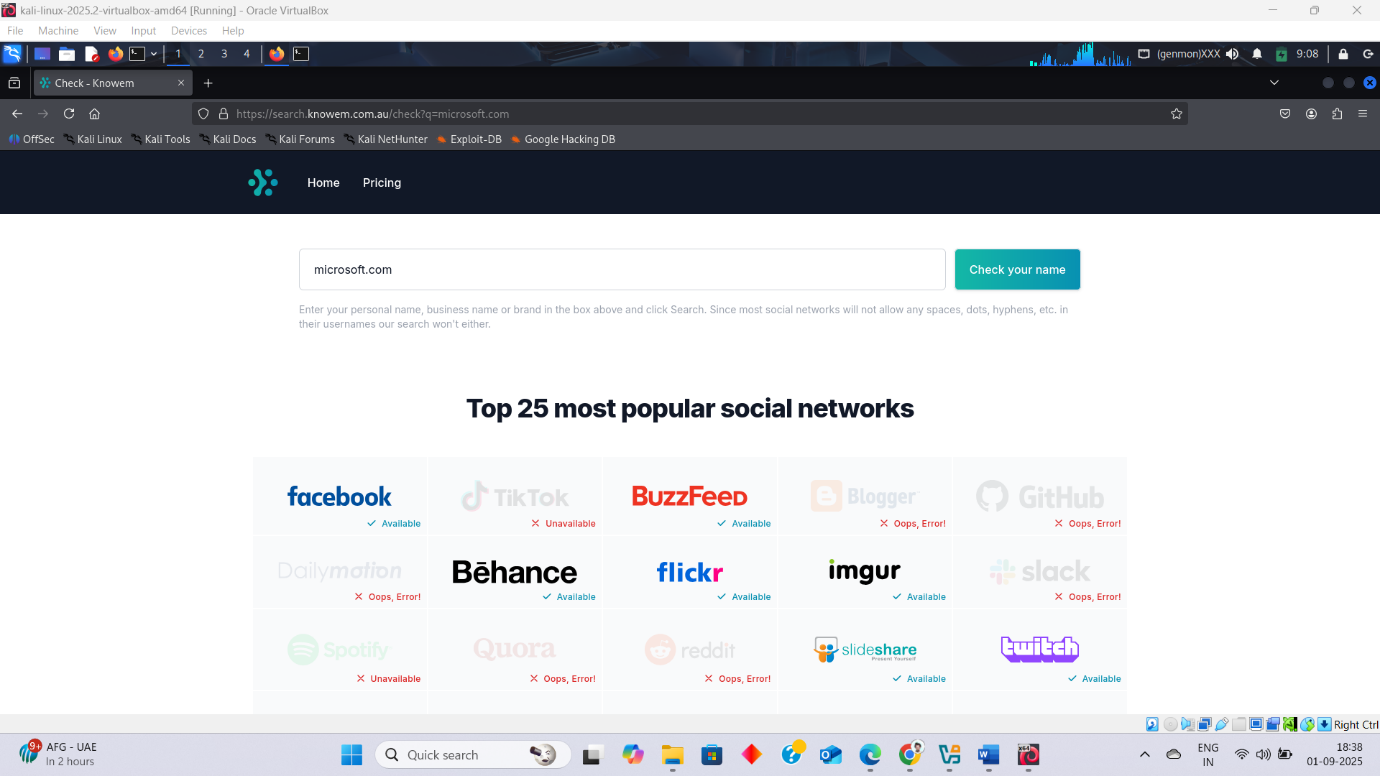
**Sherlock :** Sherlock checks if a username exists on sites like Twitter, Facebook, Instagram, GitHub, LinkedIn, Reddit, etc**.** OSINT (Open Source Intelligence) / Information Gathering.

| **Operator** | **Meaning / Function** |
| --- | --- |
| -h or --help | Show help menu (all options). |
| --version | Show Sherlock version. |
| --verbose | Show detailed output while searching. |
| --folderoutput <folder> | Save results in a specific folder. |
| --output <filename> | Save results in a file. |
| --csv | Save results in CSV format. |
| --site <sitename> | Search only on a specific site (e.g., --site twitter). |
| --proxy <proxy\_url> | Use a proxy (e.g., Tor: socks5://127.0.0.1:9050). |
| --timeout <sec> | Set timeout for requests (default: 60 sec). |
| --tor | Use Tor network for anonymity. |
| --print-found | Show only results where the username is found. |
| --browse | Open found results in browser automatically. |
| --json | Save output in JSON format. |



**Similar tools/Website:**

* **KnowEm :** Checks username availability on hundreds of sites, often used for brand monitoring. <https://knowem.com.au/>



# **WHOIS Footprinting vs DNS Footprinting:**

| **Feature** | **WHOIS Footprinting** | **DNS Footprinting** |
| --- | --- | --- |
| **Definition** | Collects domain registration info from WHOIS databases | Collects DNS records and infrastructure details of a domain |
| **Focus** | *Who owns the domain?* (administrative details) | *How the domain works on the internet?* (technical details) |
| **Information Gathered** | - Registrant/Owner name - Organization - Registrar - Contact details (phone, email, address) - Domain creation & expiry dates - Name servers | - IP addresses (A records) - Mail servers (MX) - Name servers (NS) - Subdomains - TXT/SPF/DMARC records - Zone transfers (if misconfigured) |
| **Tools** | whois, ICANN WHOIS, domaintools.com | nslookup, dig, dnsrecon, dnsenum, fierce |
| **Purpose** | Identify **domain ownership and admin info** | Identify **technical infrastructure & attack surfaces** |
| **Example Command** | whois microsoft.com | dig microsoft.com ANY |
| **CEH Category** | Passive footprinting | Passive (querying) or Active (zone transfers, brute forcing) |

**In short**:

* **WHOIS = Ownership info** (who registered the domain)
* **DNS = Technical info** (how the domain is set up and runs)

# **Footprinting via Whois :**

**Whois:** Uses WHOIS databases to find information about a domain (e.g., owner, registrar, IP address, contact info, DNS details). Since this data is publicly available and doesn’t involve contacting the target system, it is **Passive Footprinting .**

**WHOIS Output**

* Domain Name - The target domain.
* Registrar - Company that registered the domain.
* Registrant Contact - Owner details (often privacy-protected).
* Name Servers - DNS servers in use.
* Creation Date - When domain was registered.
* Expiry Date - When registration ends.
* Updated Date - Last modification.
* IP Range (for IP WHOIS) - Shows organization using the IP block.

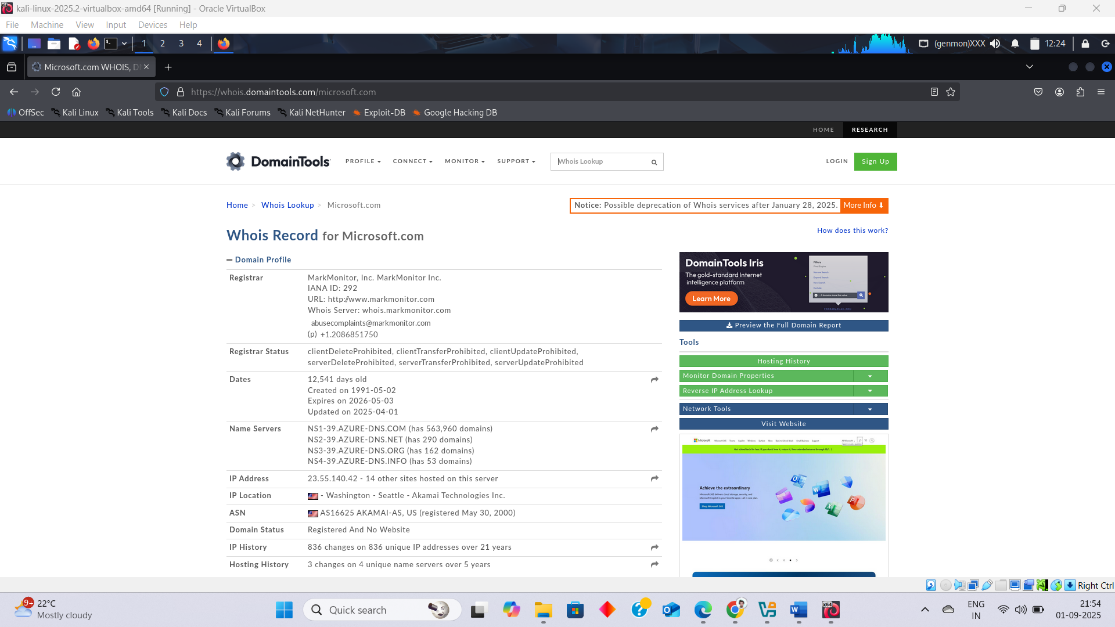
**Operators**

| **Command** | **Description** |
| --- | --- |
| whois microsoft.com | Get WHOIS record for a domain |
| whois -h whois.verisign-grs.com microsoft.com | Query a specific WHOIS server (useful if default one is rate-limited) |
| whois 8.8.8.8 | WHOIS lookup on an IP address |
| whois -h whois.arin.net 8.8.8.8 | Query ARIN (North America) directly for an IP |
| whois -h whois.ripe.net IP | Query RIPE NCC (Europe) |
| whois -h whois.apnic.net IP | Query APNIC (Asia-Pacific) |
| whois -h whois.lacnic.net IP | Query LACNIC (Latin America) |
| whois -h whois.afrinic.net IP | Query AFRINIC (Africa) |

**Similar tools/Website:**

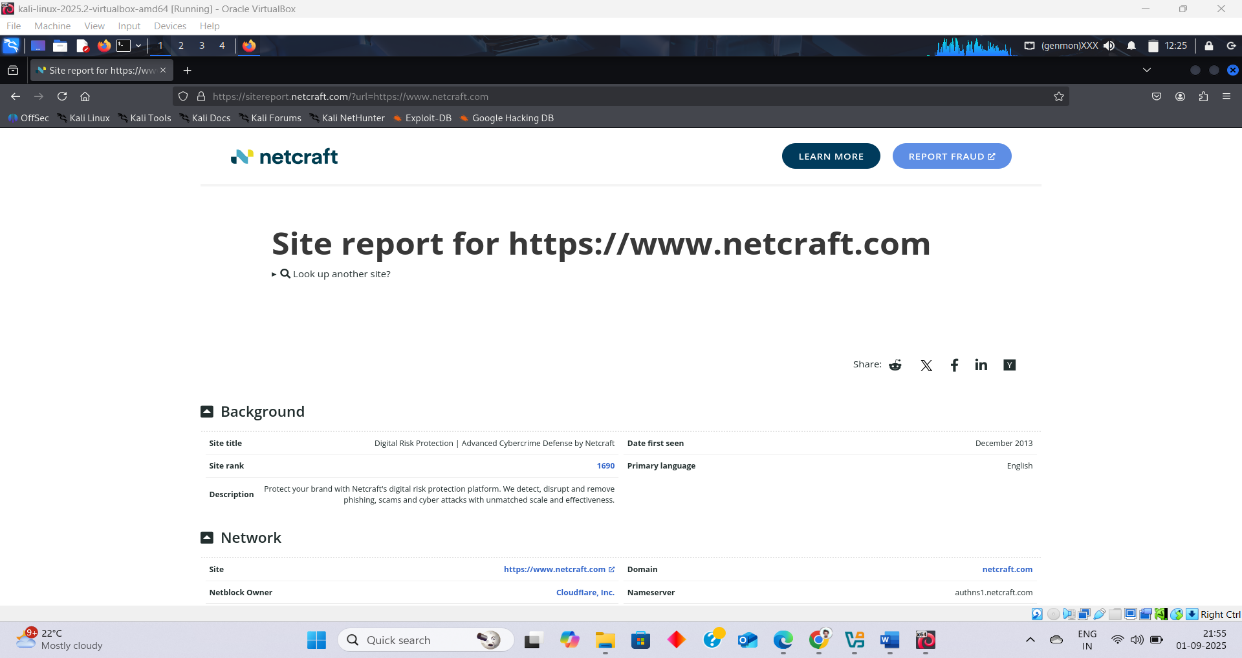
**Whois** : Online Website

[**https://whois.domaintools.com/**](https://whois.domaintools.com/)



**Netcraft :** Online service for domain research, hosting info, technologies used.

[**https://www.netcraft.com/**](https://www.netcraft.com/)



**Domain Dossier (CentralOps.net):** Online tool showing WHOIS, traceroute, DNS, blacklist status, etc.

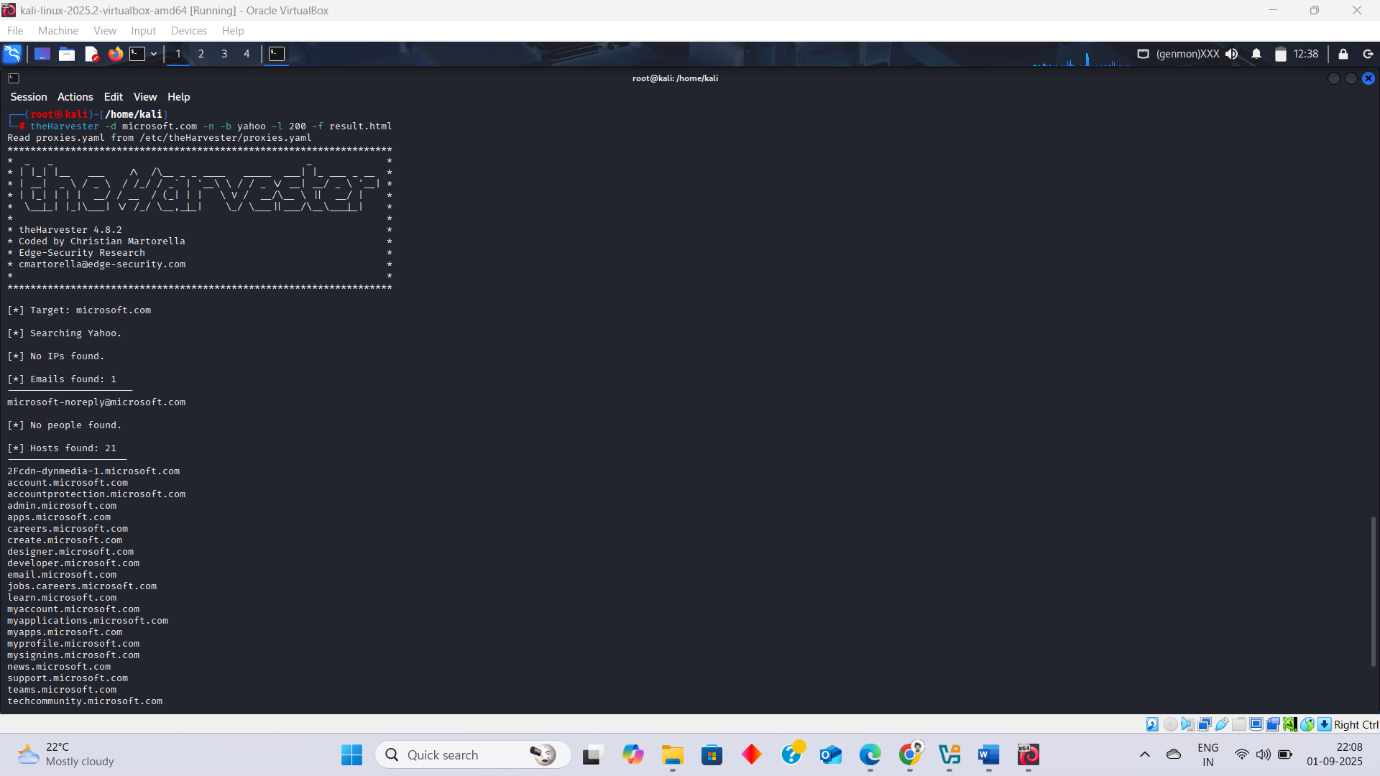
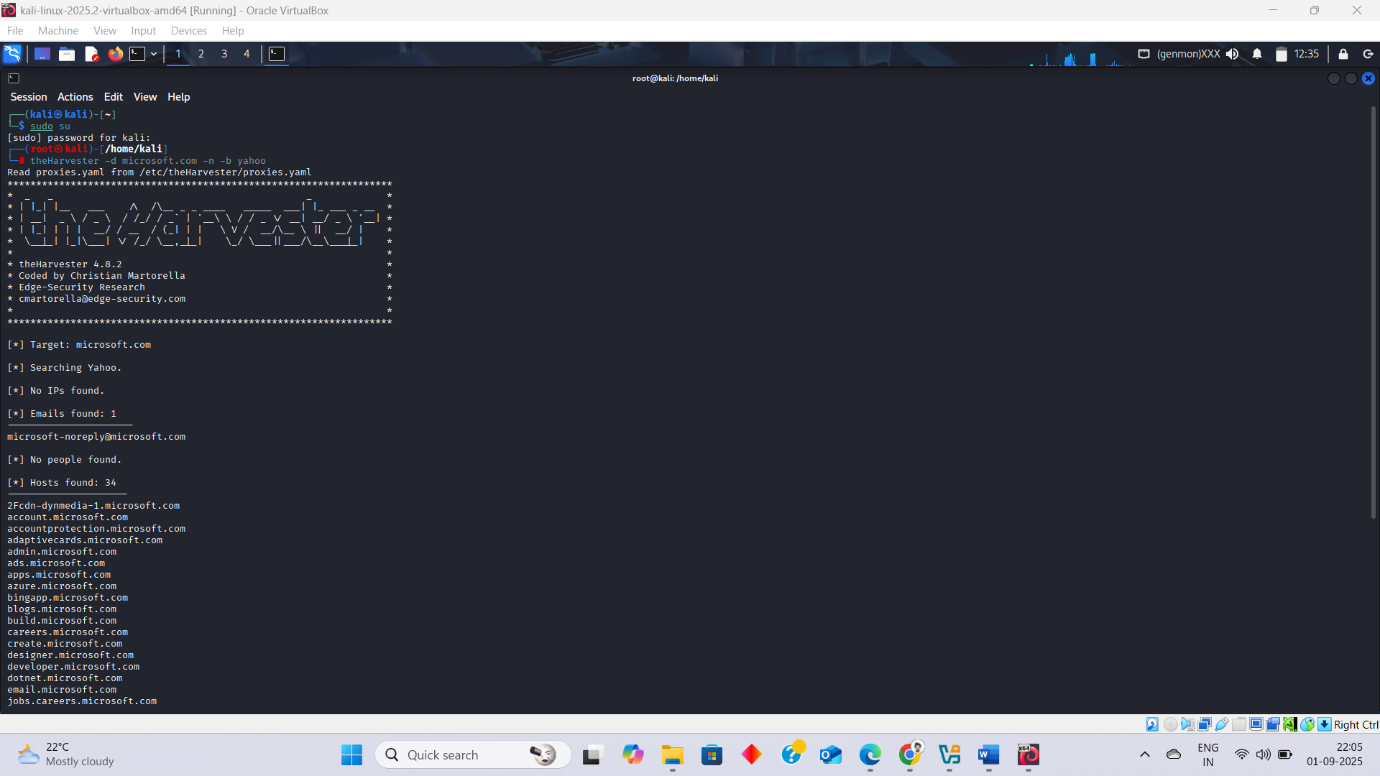
[**https://centralops.net/co/**](https://centralops.net/co/)



**TheHarvester :**  is an open-source intelligence (OSINT) tool in **Kali Linux**. It helps in **footprinting and reconnaissance** by gathering emails, subdomains, IP addresses, and hosts.

* **Common Operators**

1. **-d : Domain name to search (example.com)**
2. **-b : Data source (google, bing, yahoo, etc.)**
3. **-l : Limit the number of results to fetch**
4. **-h : Show help**
5. **-f : Save output in an HTML or XML file**



# **Footprinting via DNS :**

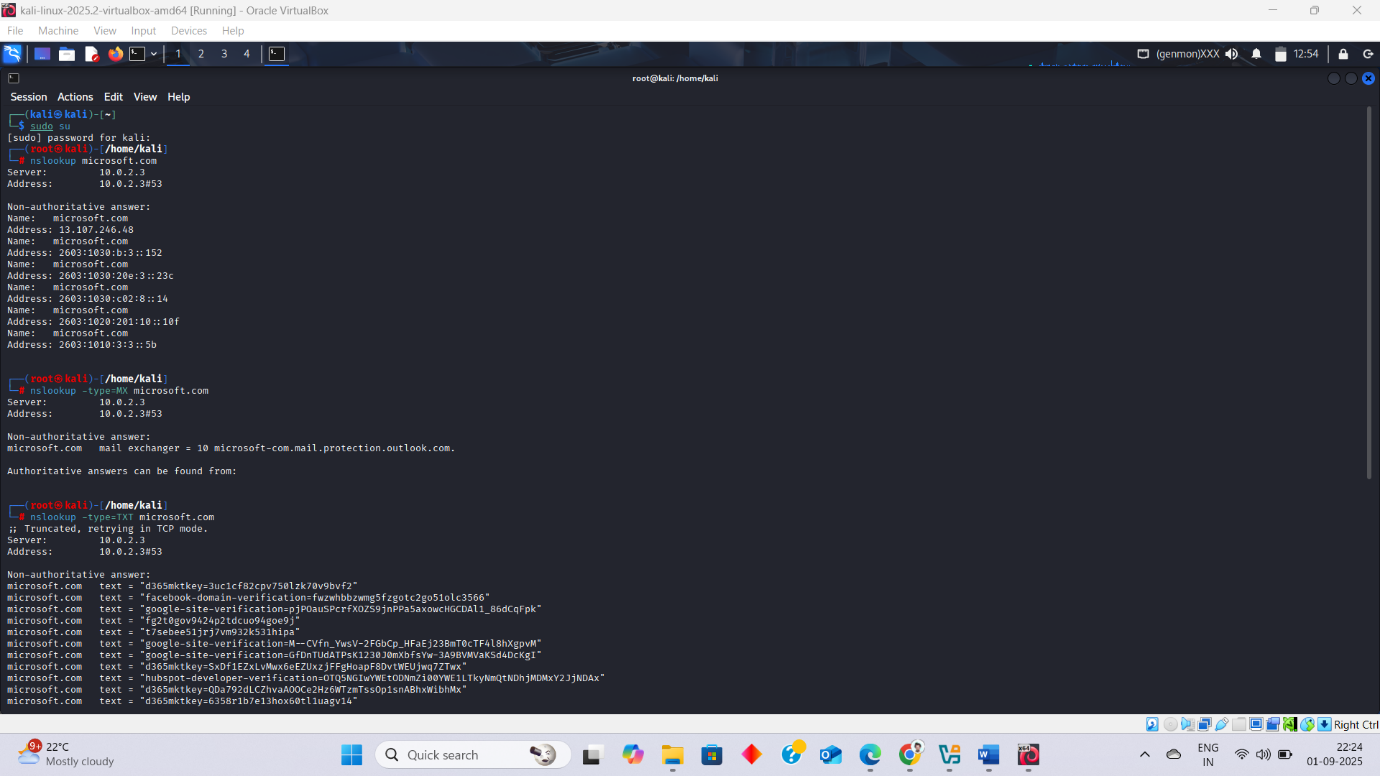
**DNS :** DNS (Domain Name System) Footprinting is the process of gathering information about the DNS records of a target domain.Subdomains, IP addresses, and other valuable network details

**Information Gathered with DNS Footprinting**

1. **Domain Details: Domain name, Registrar info**
2. **DNS Records:** 
   * + - A record → Domain → IP address
       - MX record → Mail server(s)
       - NS record → Name servers
       - CNAME record → Alias domains
       - TXT record → SPF/DKIM policies, sometimes leaks info
3. **Subdomains:** (like mail.example.com, ftp.example.com)
4. **Zone Transfers (AXFR):** If misconfigured, can dump the entire DNS database of the target → huge info leak.

**Tools:**

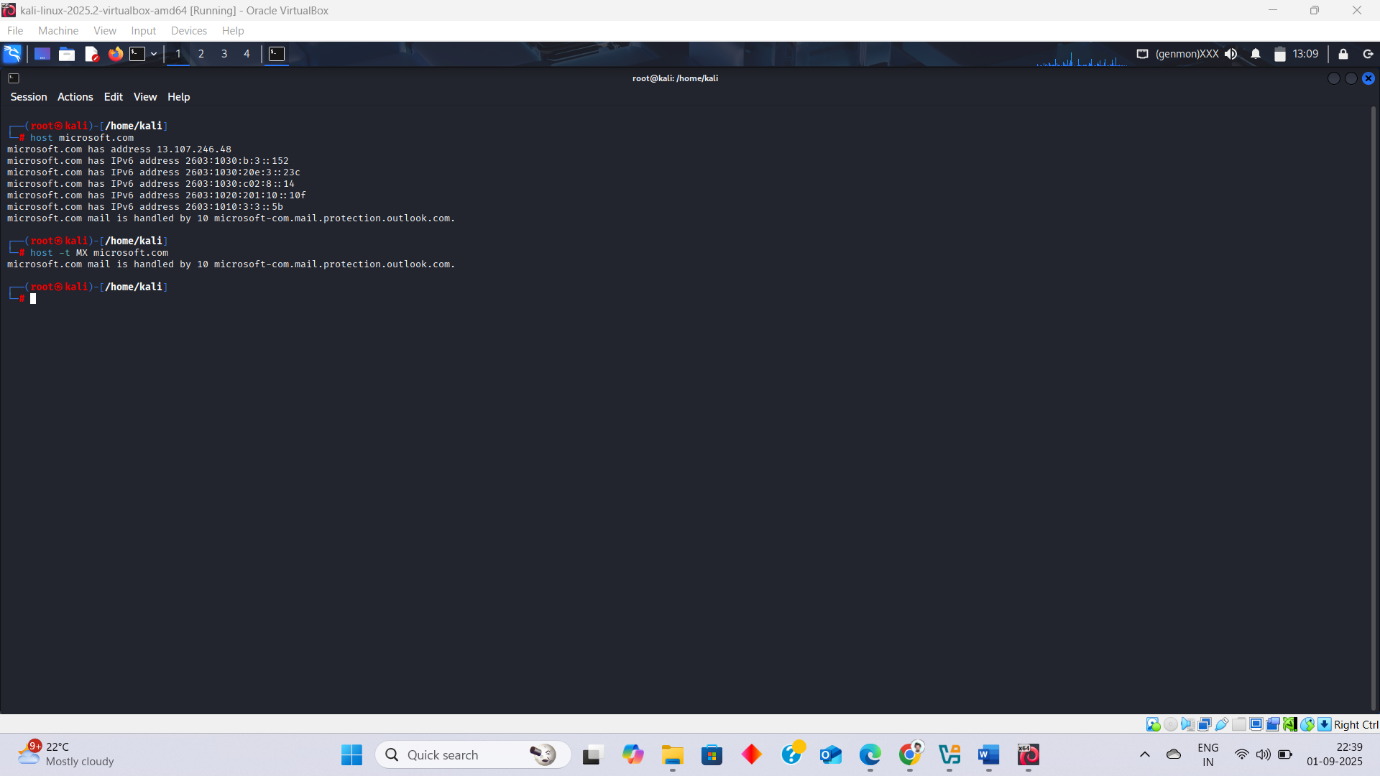
**Nslookup:** (Name Server Lookup) tool to query DNS (IP ↔ domain info).

****

**Dig:**(Domain Information Groper) is a powerful command-line tool used for DNS lookups. It’s more advanced and detailed than nslookup.

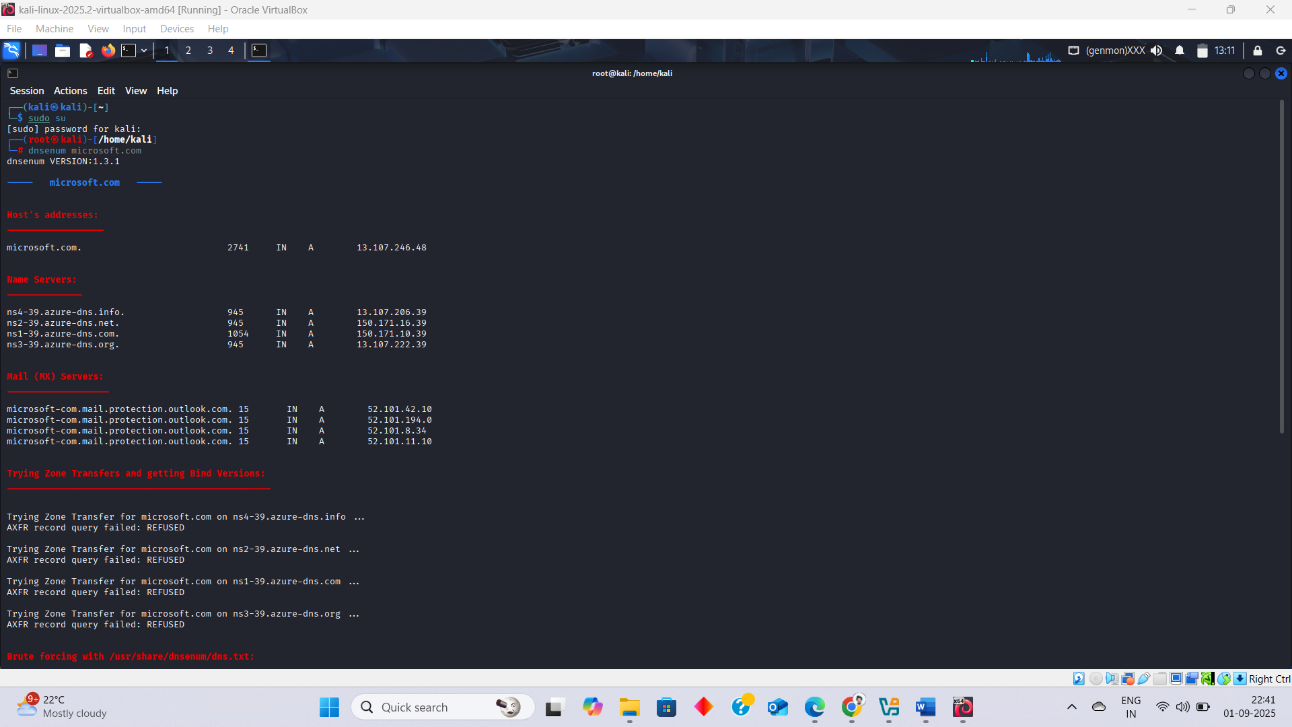
****

**Host:** host is a simple DNS lookup utility used in Linux systems. It’s easier than dig and mainly used to find IP addresses from domain names and vice versa.

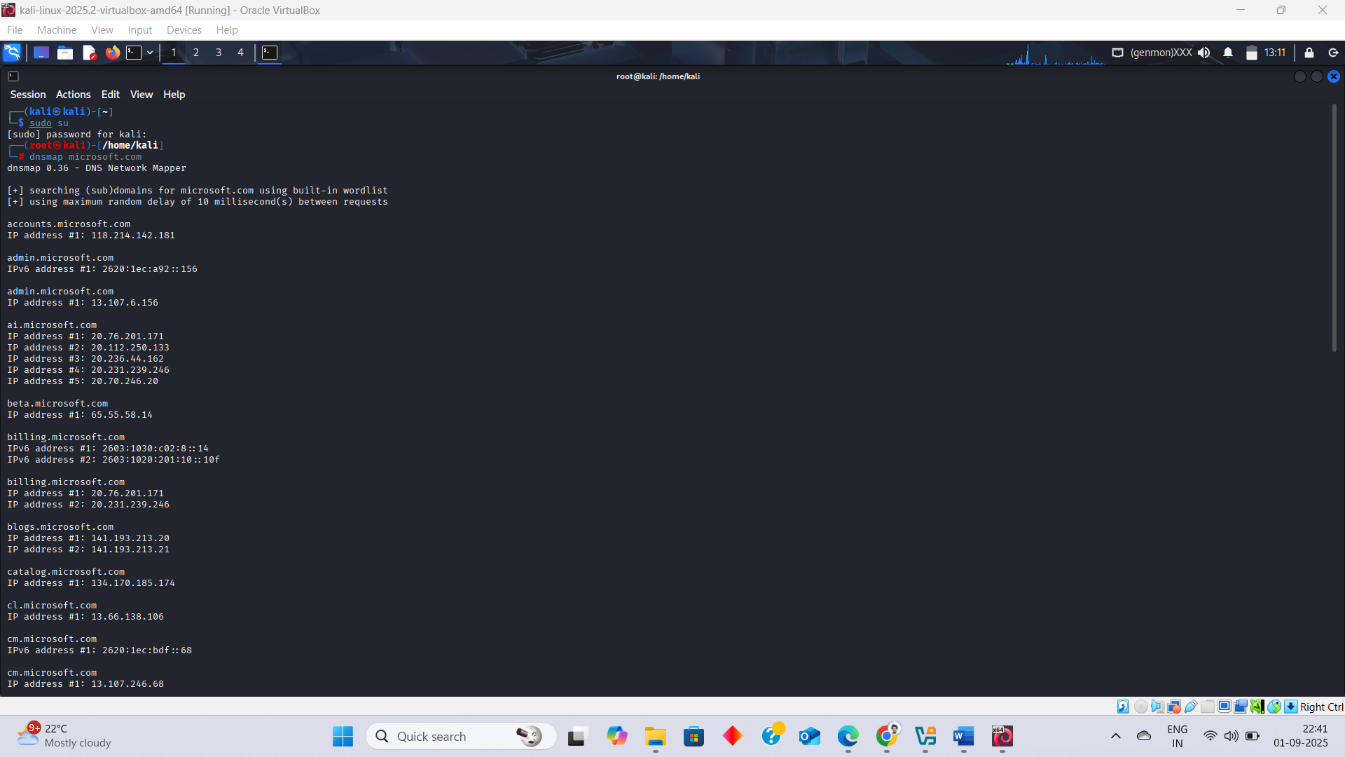


**Similar tools/Website:** *for more details*

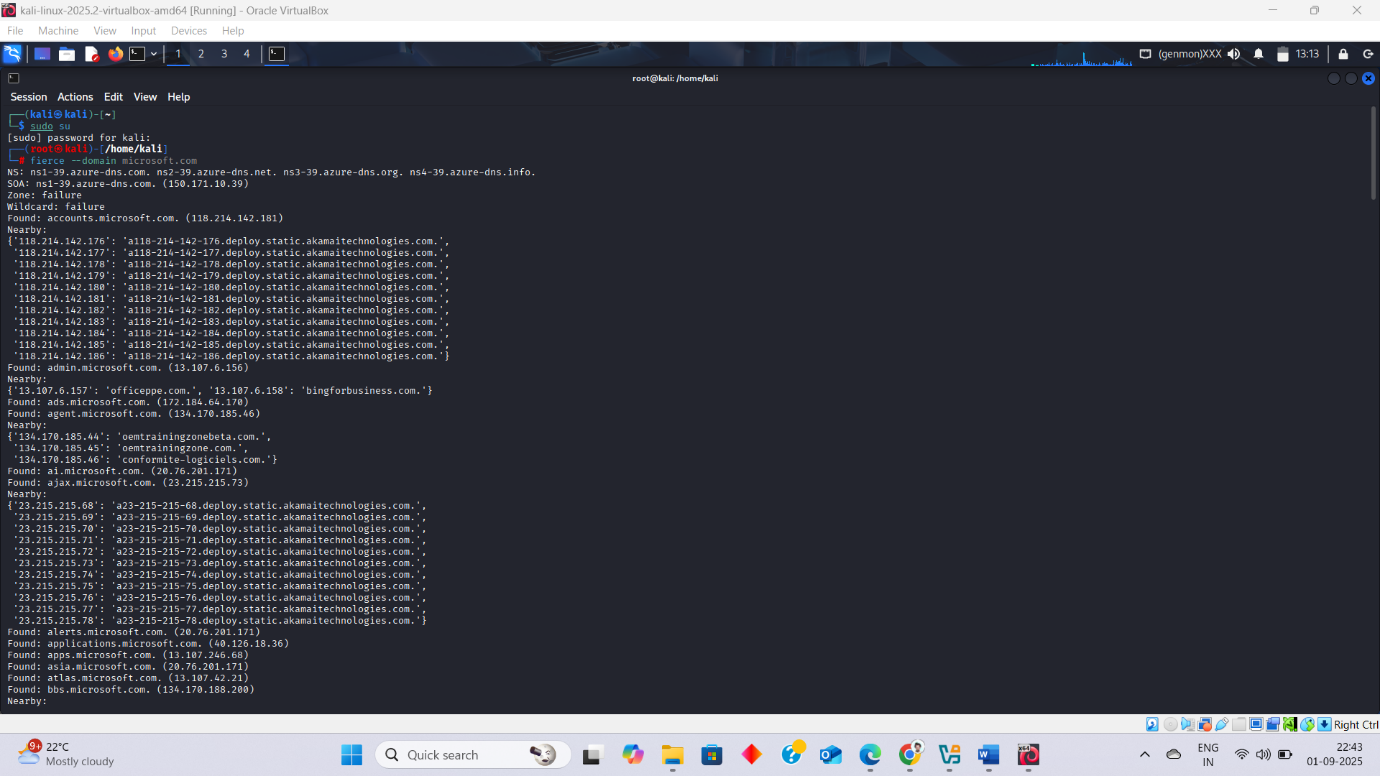
* **Dnsenum:** dnsenum example.com

****

* **Dnsmap:** dnsmap example.com

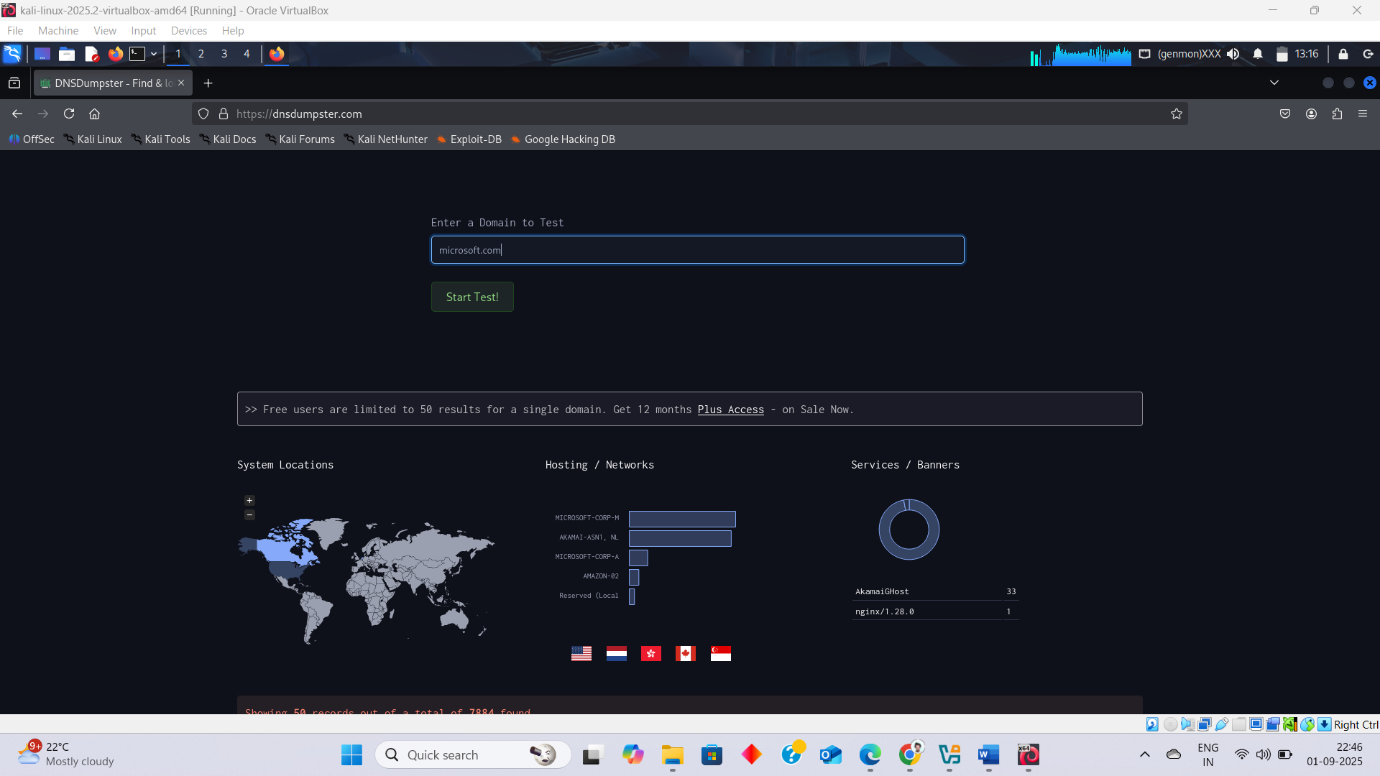
****

* **fierce (brute-forces subdomains):** fierce --domain example.com

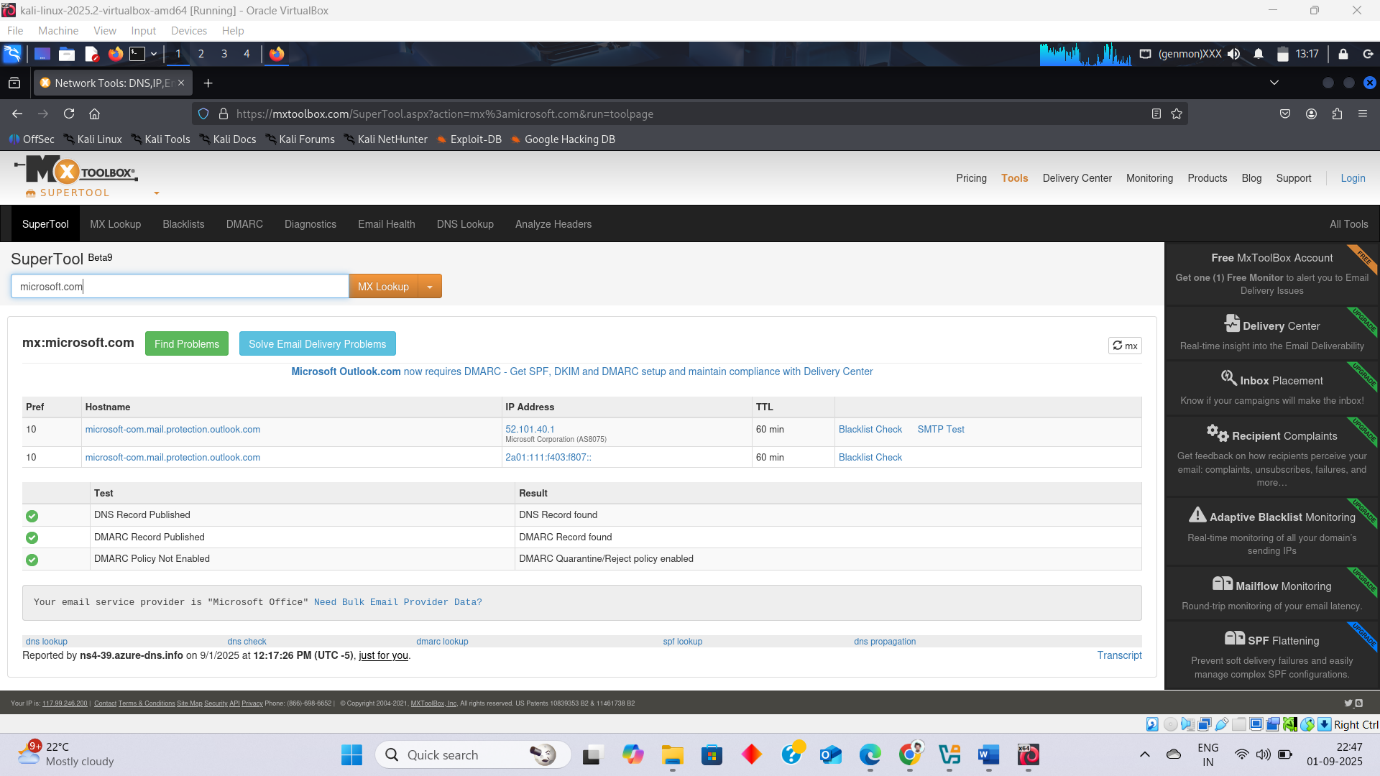


**Online Tools :**

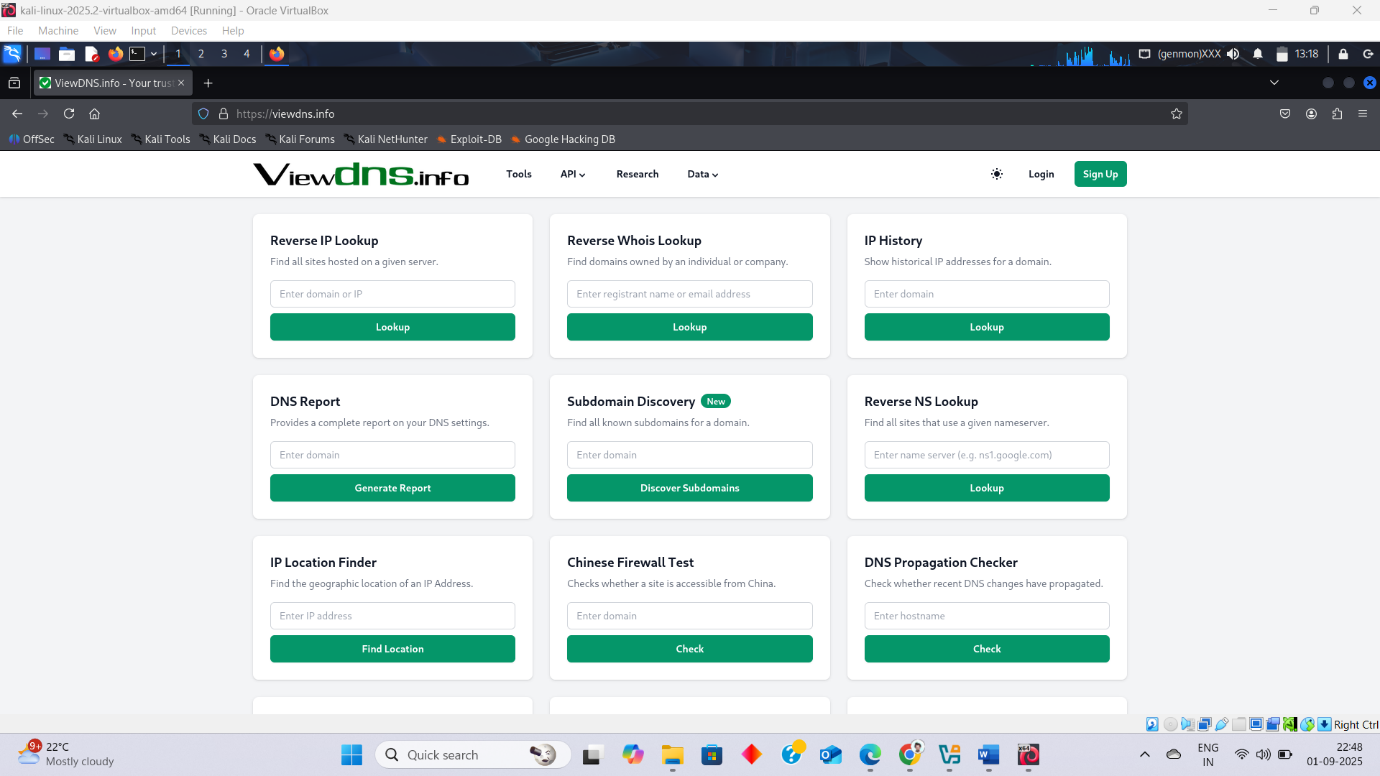
**DNSdumpster →** [**https://dnsdumpster.com**](https://dnsdumpster.com)

****

**MXToolbox →** [**https://mxtoolbox.com**](https://mxtoolbox.com)

****

**ViewDNS.info →** [**https://viewdns.info**](https://viewdns.info)

****

# **Network Footprinting:**

Network footprinting is the process of **gathering information about a target network** to understand its structure, devices, and vulnerabilities. Network footprinting = finding details about a network (IP addresses, devices, topology, services, etc.) to create a “blueprint” of it.

**Information Collected in Network Footprinting :**

1. **Domain names** – Example: example.com
2. **IP addresses & Subnets** – e.g., 192.168.1.0/24
3. **Network topology** – routers, firewalls, servers
4. **Open ports** – services like HTTP (80), SSH (22)
5. **Operating systems** – Windows, Linux, etc.
6. **Services and applications** – web server, mail server, database
7. **Access points & VPNs** – entry points into the network

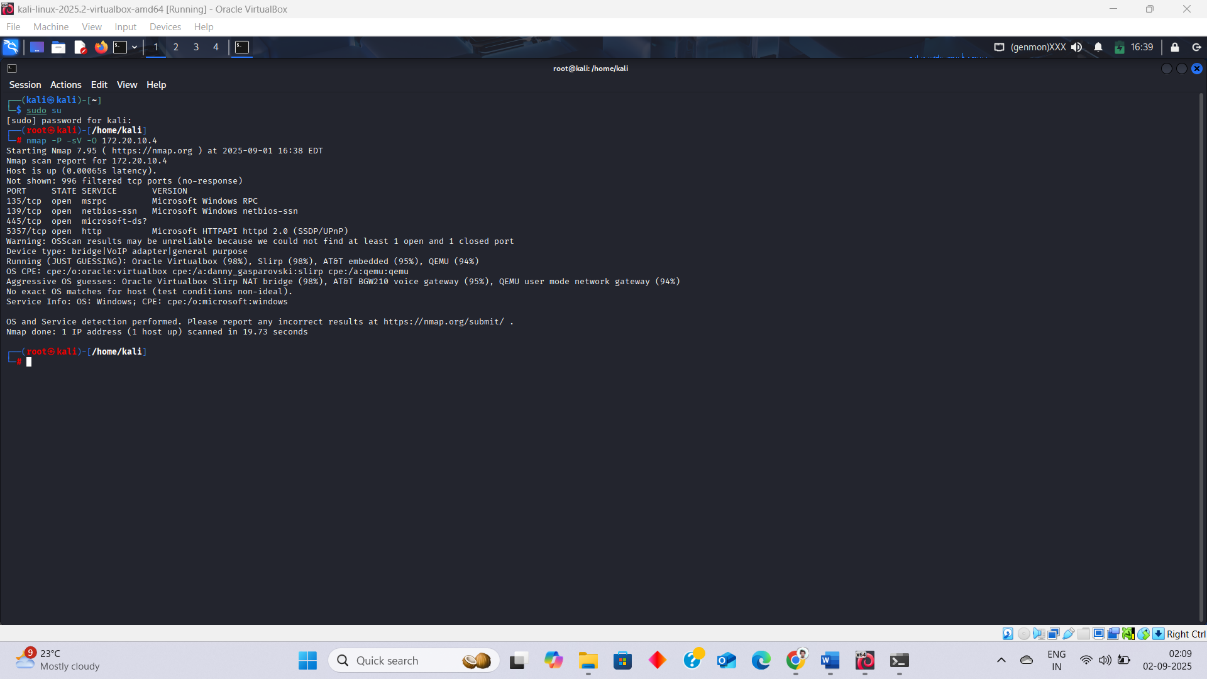
**Tools for Network Scanning :**

| **Tool** | **Usage in Footprinting** |
| --- | --- |
| **Nmap** | **Port scanning, service detection, OS fingerprinting** |
| **Netcat** | **Banner grabbing, simple port scanning** |
| **Hping3** | **Custom packet crafting, firewall testing** |
| **Angry IP Scanner** | **Quick ping sweeps** |
| **Zenmap** | **GUI for Nmap, visualization of network maps** |

**Tools Cammands :**

**1)Nmap:**

* Port Scanning = nmap -P 172.20.10.4
* Service Detection = nmap -sV 172.20.10.4
* OS Detection = nmap -O 172.20.10.4

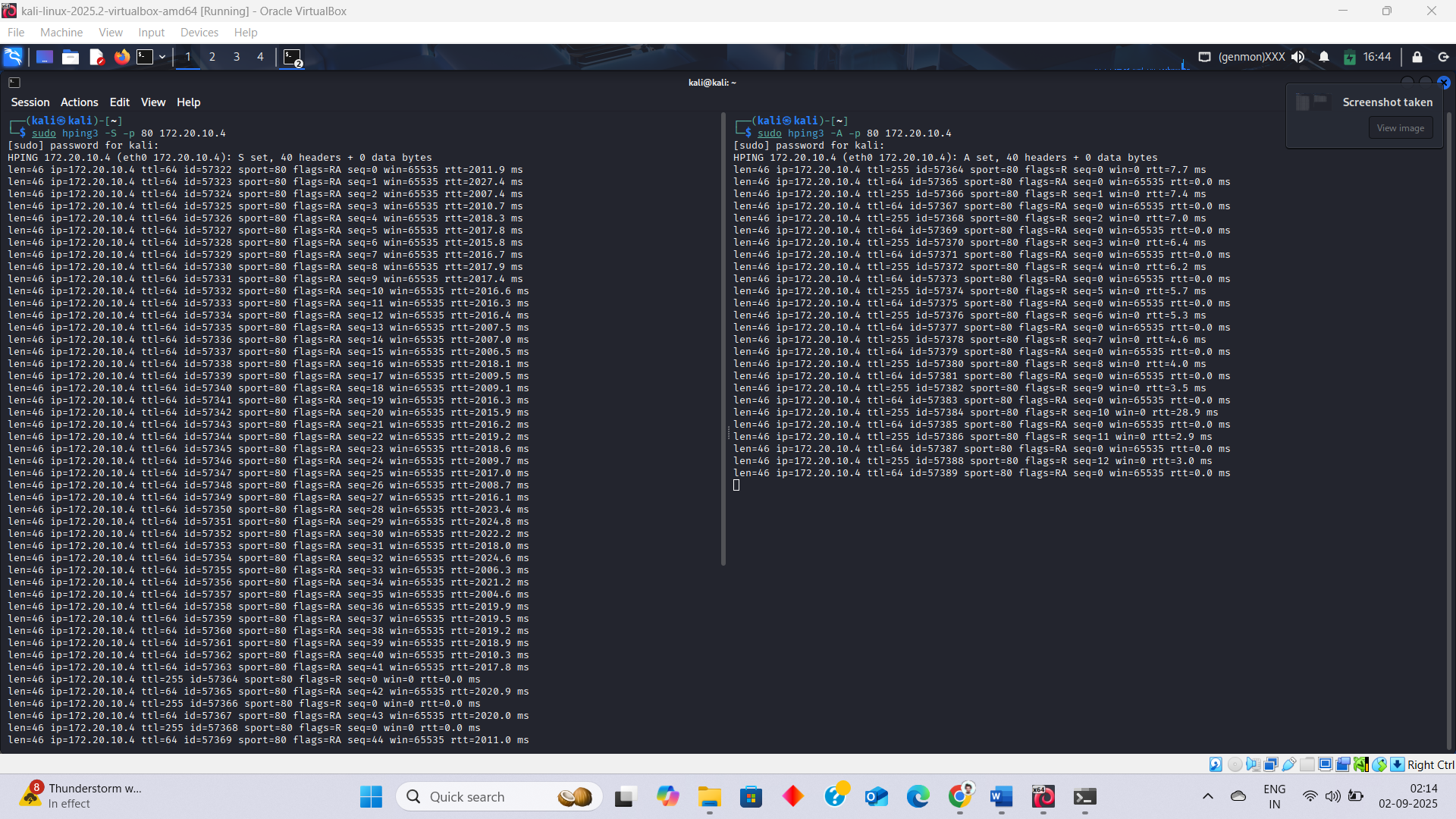


**2) Netcat**

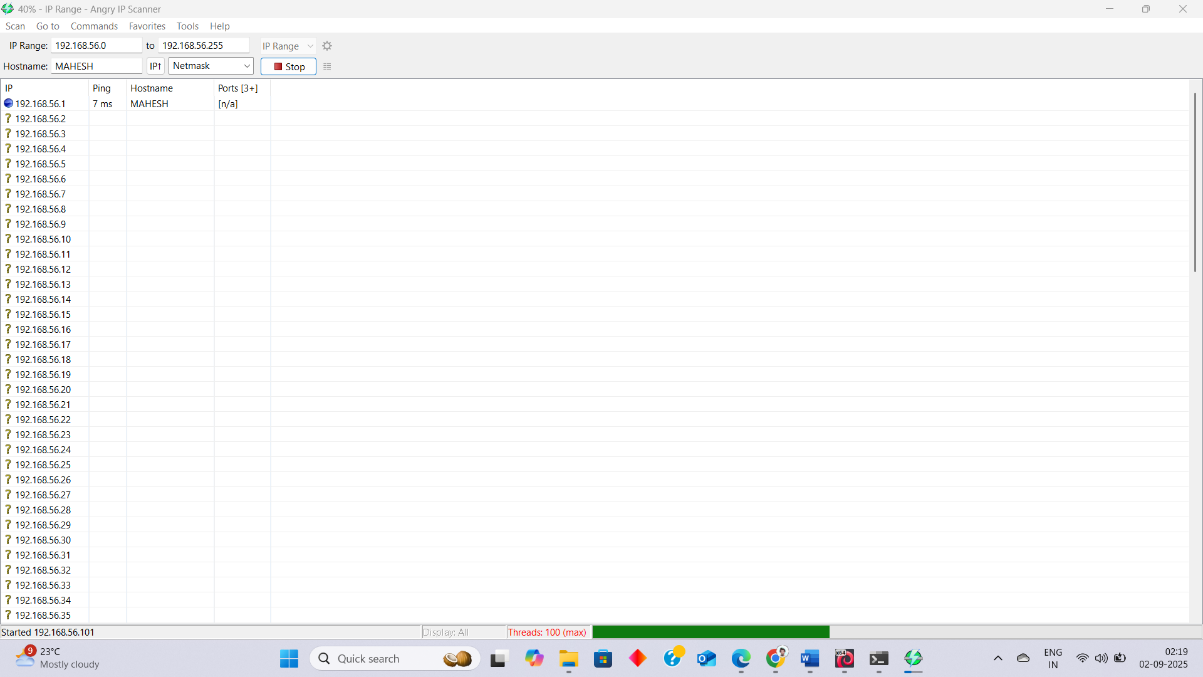
* Baner Grabbing = nc 172.20.10.4
* Simple Port Scan = nc -zv 172.20.10.4

**3) Hping3**

* Custom Packet Crafting = hping3 -S -p 80 172.20.10.4
* Firewall Testing = hping3 -A -p 80 172.20.10.4

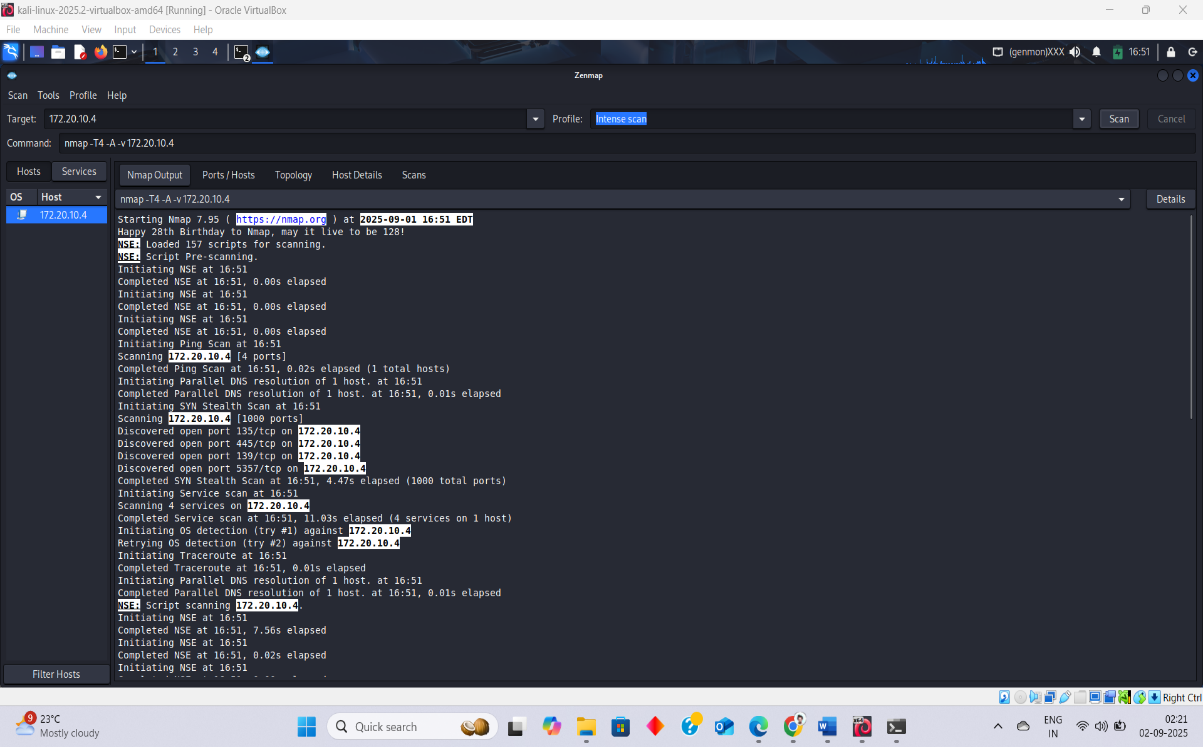


**4) Angry IP Scannar tool :** [**https://angryip.org**](https://angryip.org)

****

**5) zenmap tool :**

* In the Target field → enter an IP or range (e.g., 192.168.1.0/24).

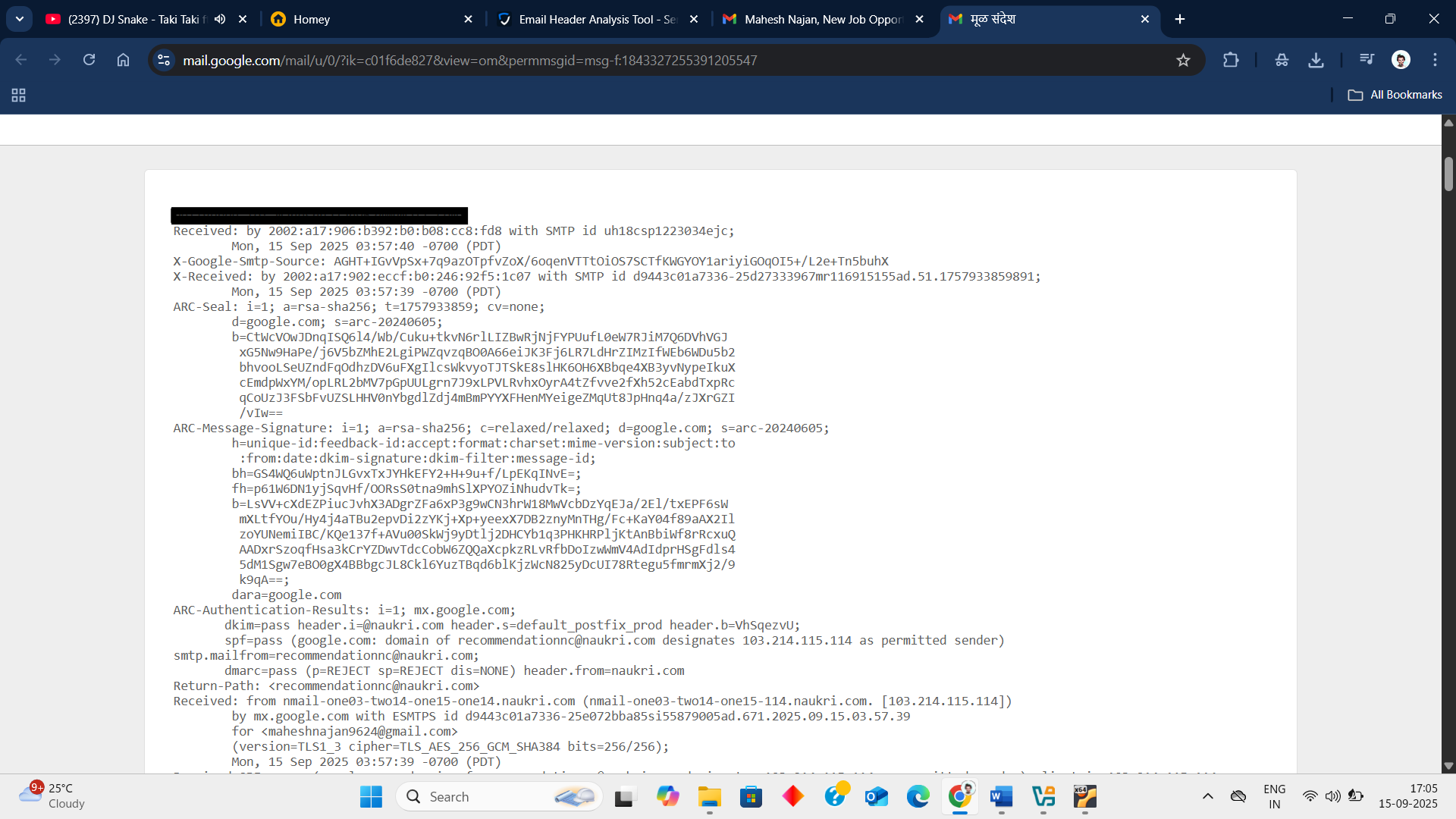


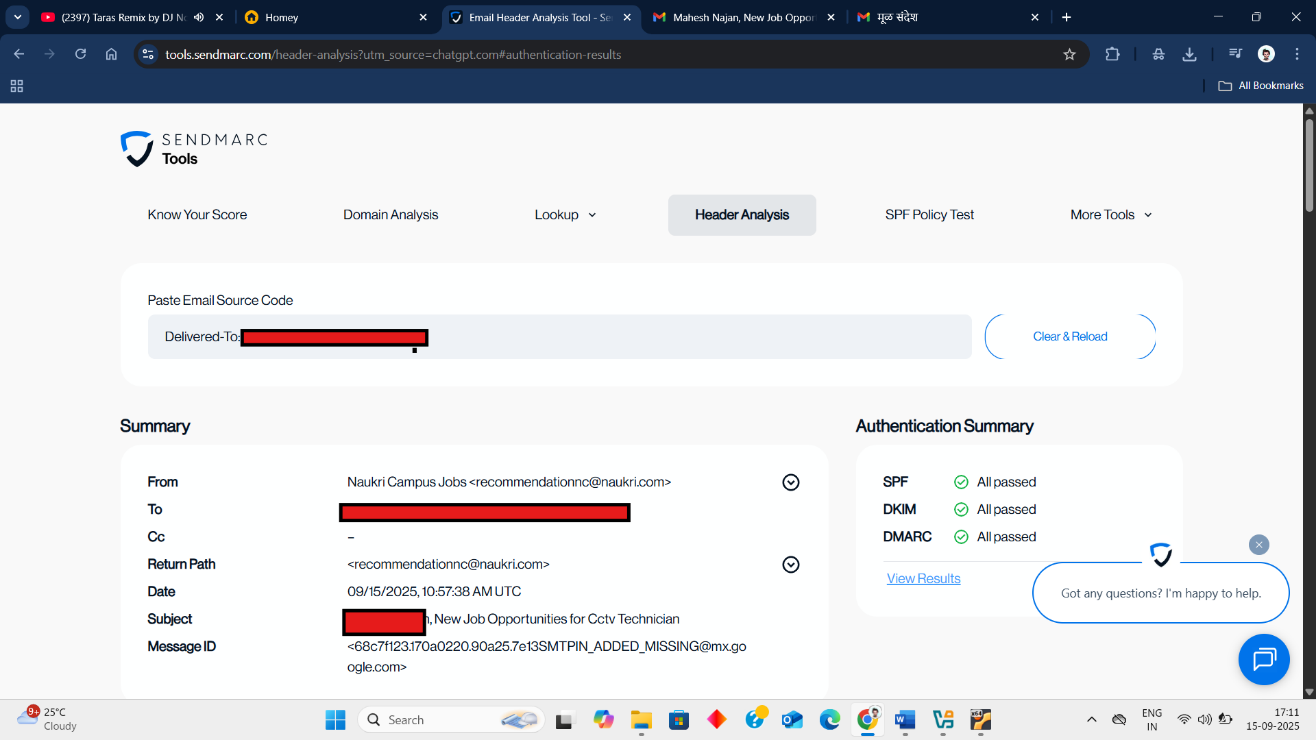
# **Email Footprinting:**

**Email footprinting =** gathering information about an email address, domain, and the mail infrastructure using public/OSINT techniques. And Verify the the received mail is from correct person .

**Tools :**

**SendMarc =**  This tool is used Header Analysis . if we want results like SPF/DKIM/DMARC clearly .

****

****