

Foot Printing

Foot Printing is an ethical hacking technique used first to gather as much data as possible about a specific targeted computer system, an infrastructure and network to identify opportunities to penetrate them.

There are two types of Foot Printing...

Passive Foot Printing:

Passive Foot Printing attackers collect information without knowing targets, passive foot printing attackers collecting information from different activities like Google search, IP address, DNS lookup.

Examples of passive foot printing techniques include:

Search Engines: Using search engines to find publicly accessible information about the target, such as websites, documents, and social media profiles.

Social Media Analysis: Examining publicly shared posts, profiles, and information on social media platforms to gather insights about individuals or organizations.

WHOIS Lookup: Querying domain registration records to gather details about domain ownership, registration dates, and contact information.

DNS Analysis: Extracting information from DNS records, such as MX records, NS records, and subdomains, to understand the target's domain structure. Passive footprinting is generally less intrusive and has a lower chance of alerting the target to the reconnaissance efforts. However, it may provide limited and publicly available information.

Active Foot Printing:

Active foot printing attackers knows about the target and collect the information by mirroring Web sites, E-mail tracing, Pining.

Examples of active footprinting techniques include:

Network Scanning: Scanning the target's network to identify live hosts, open ports, and services. Tools like Nmap are commonly used for network scanning.

Ping Sweeping: Sending ICMP (ping) requests to a range of IP addresses to determine which hosts are active.

Banner Grabbing: Collecting information from banners and headers of network services, which can reveal details about the software and versions in use.

Traceroute: Determining the path that network traffic takes between the attacker and the target, helping to map the network infrastructure.

Active foot printing can provide more detailed technical information about the target's network and services but carries a higher risk of detection and potential legal consequences.

Both passive and active foot printing have their place in reconnaissance, and attackers often use a combination of these techniques to gather a comprehensive understanding of the target's digital presence, architecture, and potential vulnerabilities.

Various steps of information Gathering

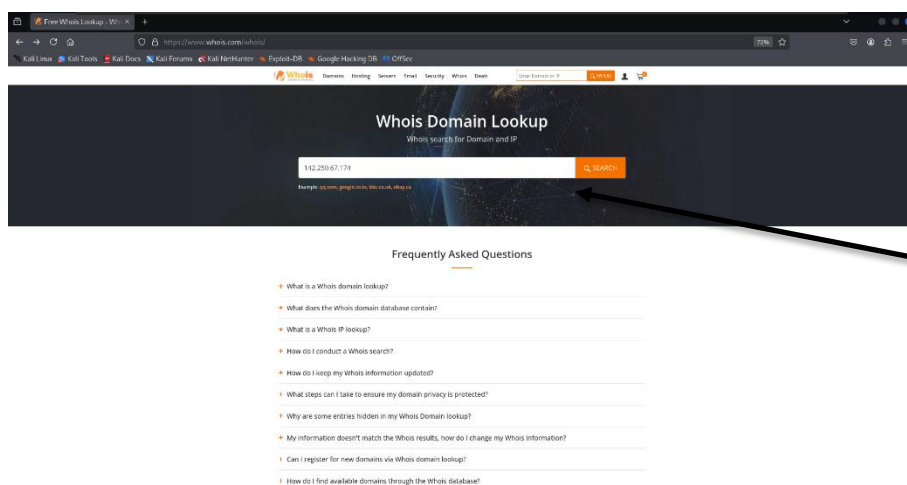
1) Website Foot Printing

Website footprinting is a technique in which information about the target is collected by monitoring the target's website.

Example: -

- A. **Whois lookup :-** Whois is a query and response protocol that is used for querying databases that store an Internet resource's registered users or assigness.

Using Whois lookup gives the registrar, name servers and registration dates.



Whois Domain Lookup

Whois search for Domain and IP

112.250.67.174

Search

Frequently Asked Questions

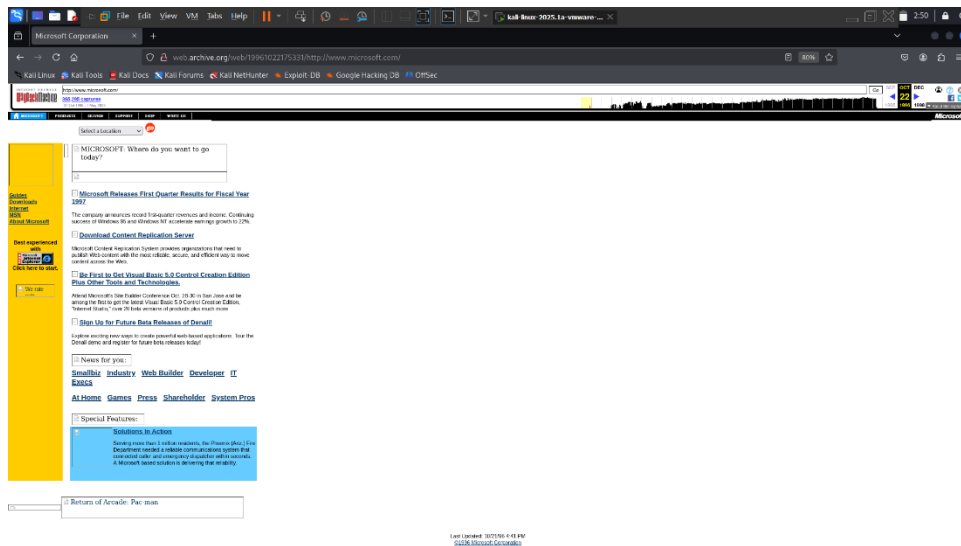
- What is a Whois domain lookup?
- What does the Whois domain database contain?
- What is a Whois IP lookup?
- How do I conduct a Whois search?
- How do I keep my Whois information updated?
- What steps can I take to ensure my domain privacy is protected?
- Why are some entries hidden in my Whois Domain lookup?
- My information doesn't match the Whois results, how do I change my Whois information?
- Can I register for new domains via Whois domain lookup?
- How do I find available domains through the Whois database?

Enter The IP/Domain Of
WebSite you wanna info
about

The screenshot shows a Kali Linux terminal window with a Whois query for IP 142.250.67.174. The terminal output displays Whois data for the IP, including registrant information (Google LLC), contact details, and nameservers. To the right of the terminal, there are three promotional banners: 'space' for \$1.18, 'fun' for \$1.48, and 'WORDPRESS HOSTING' for \$5.48. A red arrow points from the 'space' banner to the terminal output.

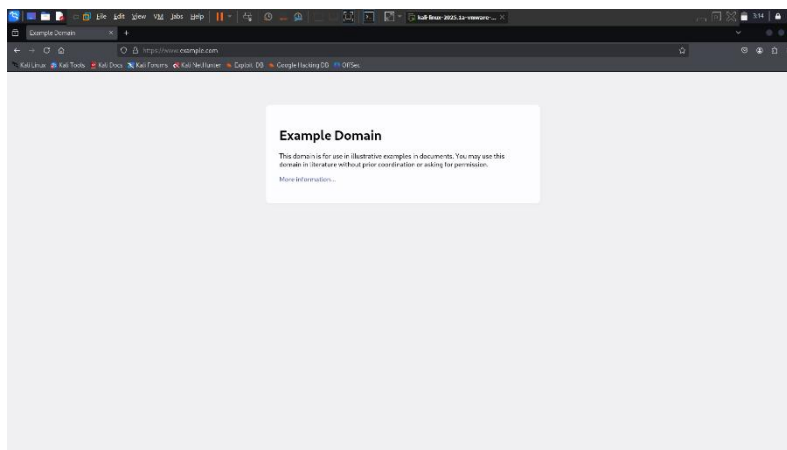
B. **Waybackmachine:** - You can enter a domain name in the search box to find out how the website was looking at a given point of time and what were the pages available on the website on different dates.

[illegible]



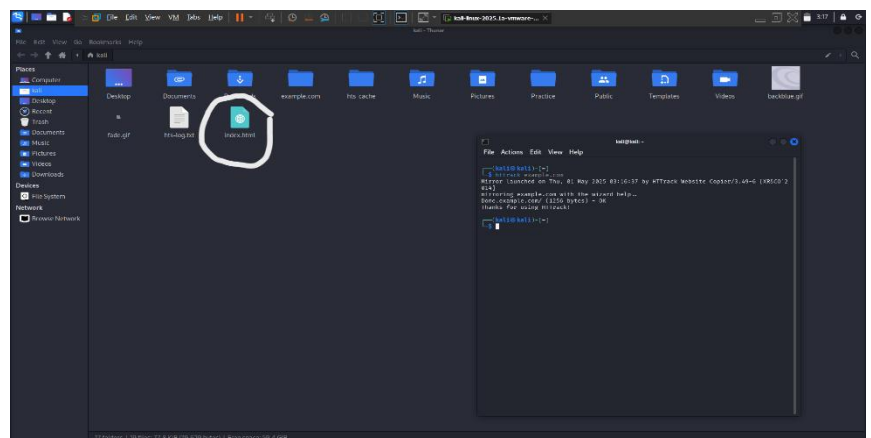
This is The October 22 1996 Microsoft Website Snapshot through wayback machine :

C. Mirroring Website: In This we create a mirror Website of Targeted Website using (httrack).



If Suppose we want to mirror this webpage open terminal in linux and type (httrack) and websites name for example like this httrack example.com

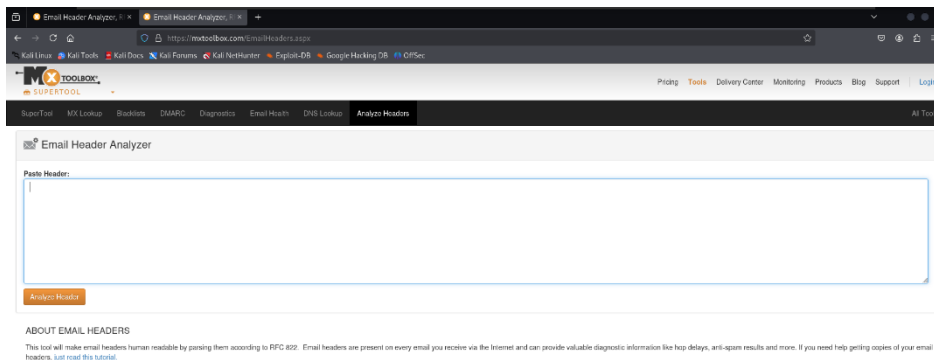
In this index.html folder now the website runs through you pc not through server httrack copies whole webpage in your machine



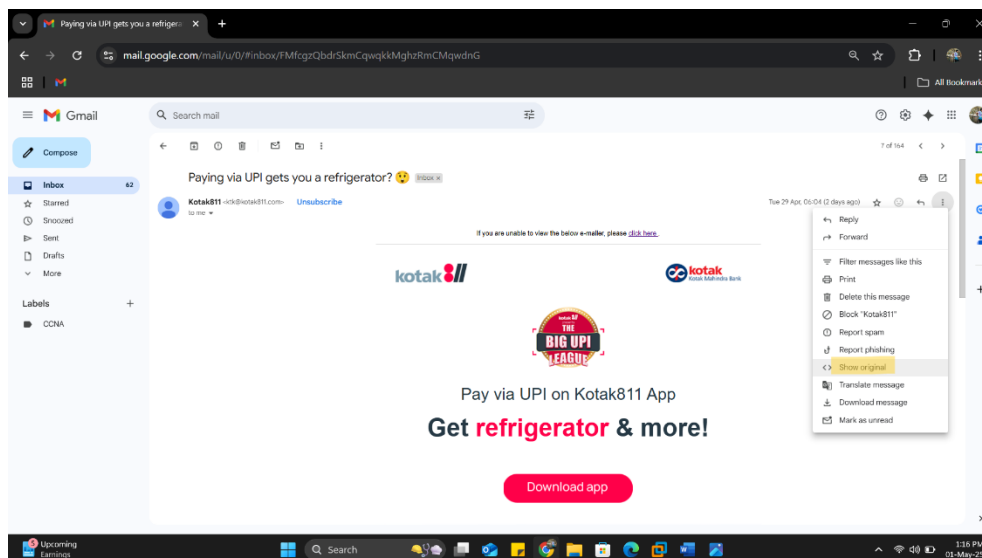
2) Email Foot printing

In this method, a hacker can trace an email and get information from it. Email foot printing gives us information regarding the sender's email, name, location, IP etc.

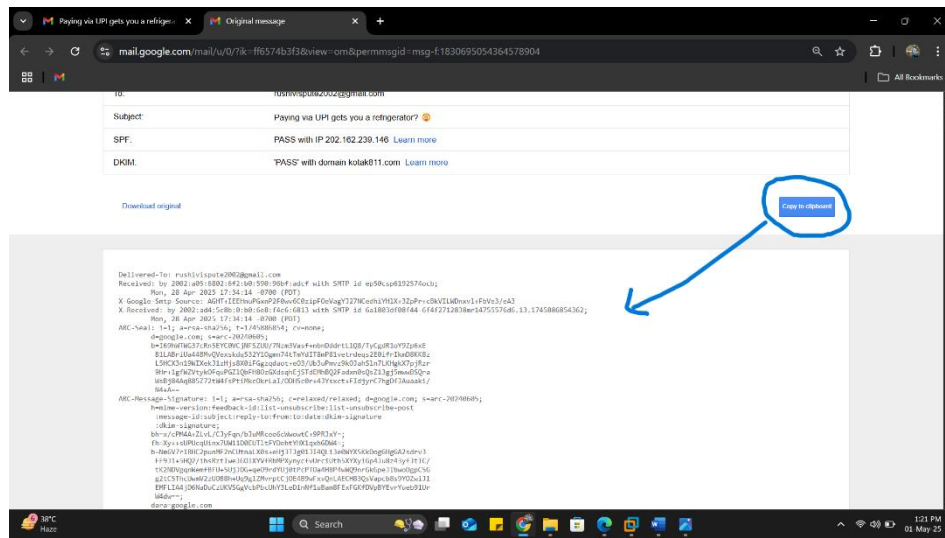
- A. **Email Header Analyzer:** - Tracing an email address by analyzing the header provides useful data in cases of malicious messages, such as in phishing attacks.



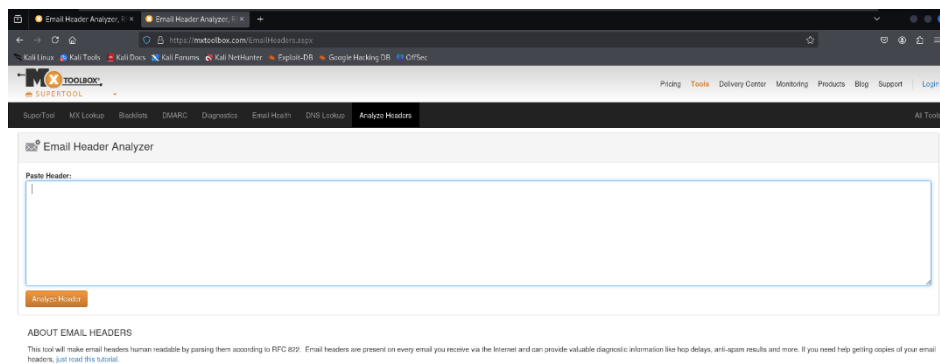
Step 1: Open Email, Click on 3 dots and then click on show originals.



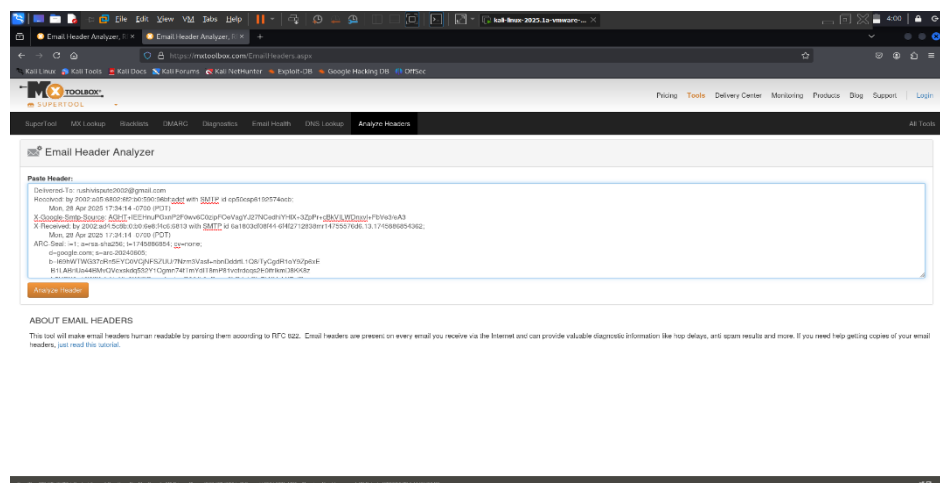
Step 2: This showing information copy this.



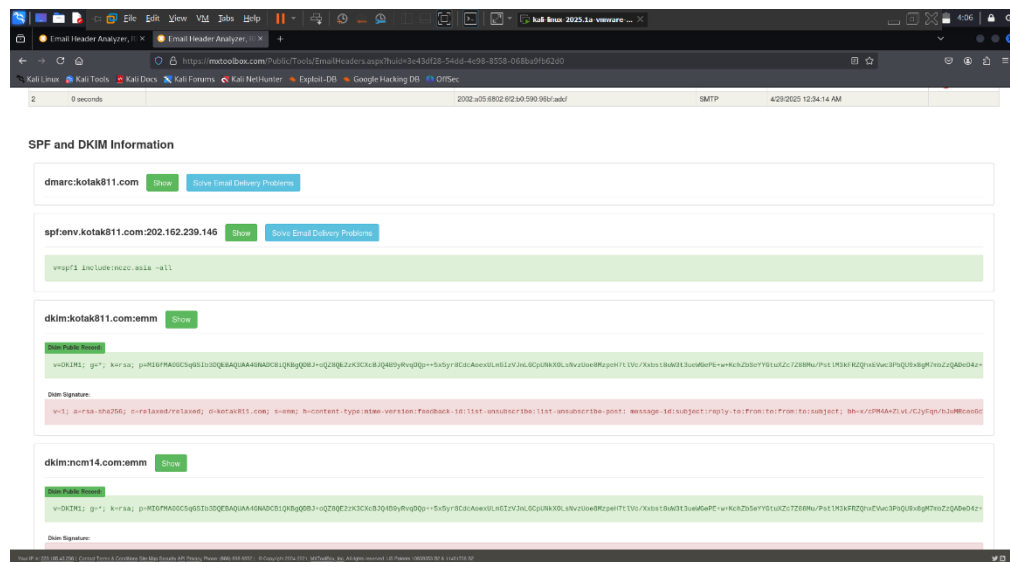
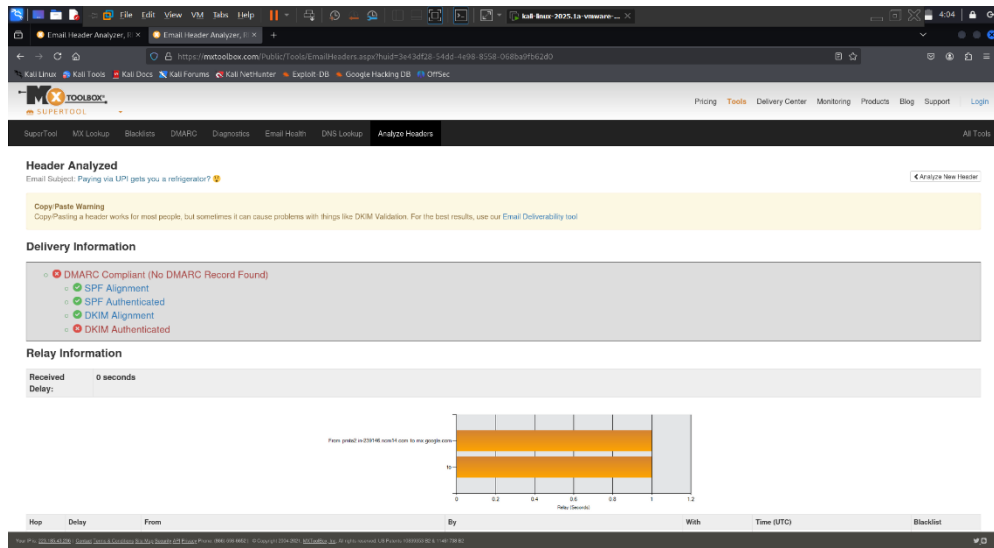
Step 3: Open a Mx Toolbox & go on analyze headers.



Step 4: Paste copy information on this given box.



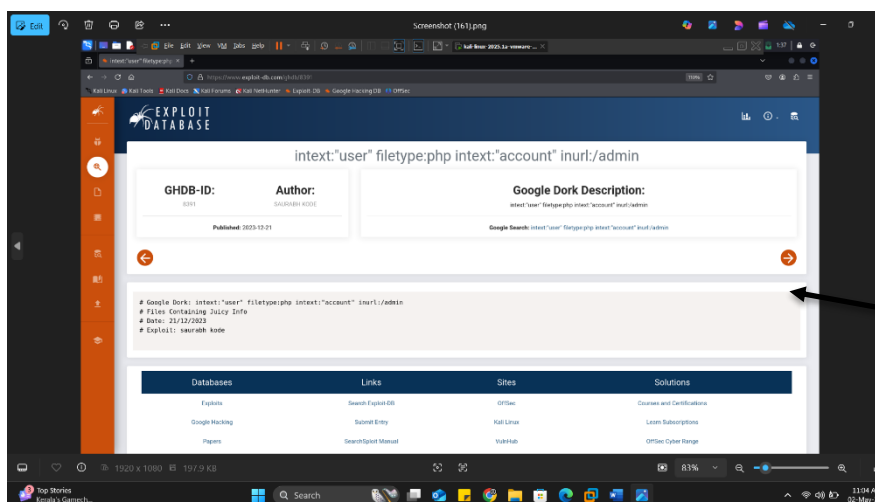
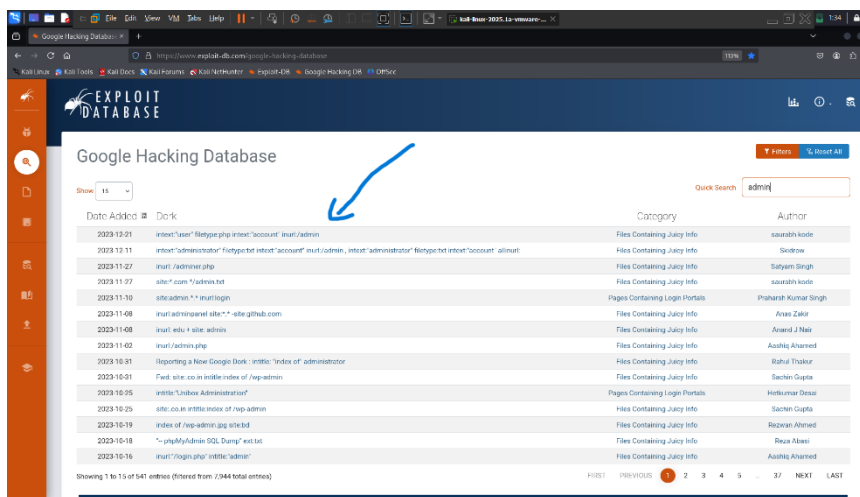
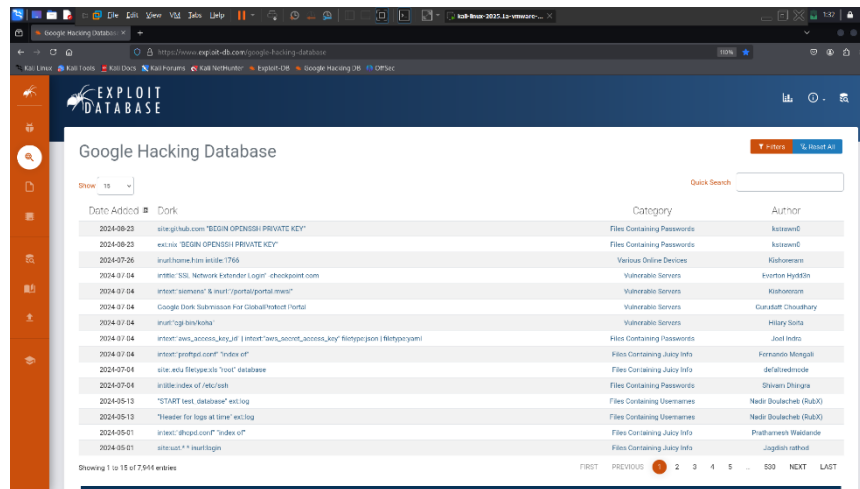
This is a Result :



3) Foot printing using Google

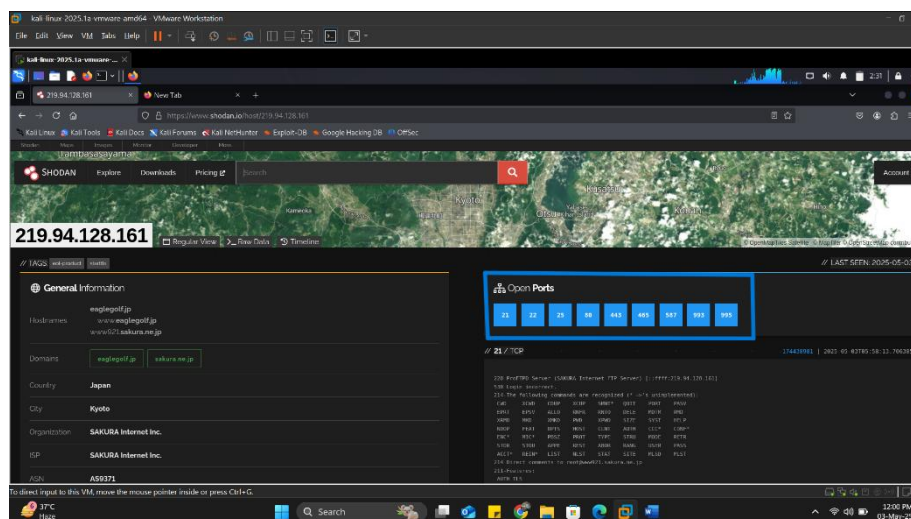
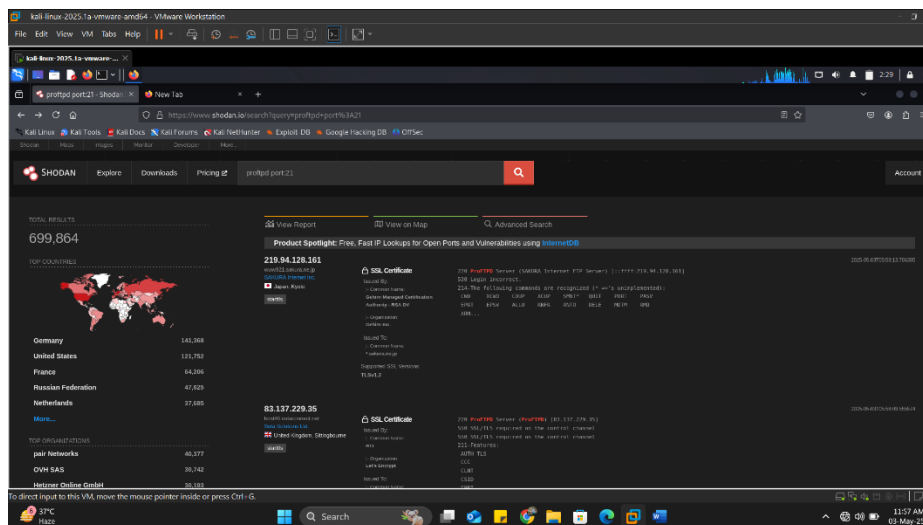
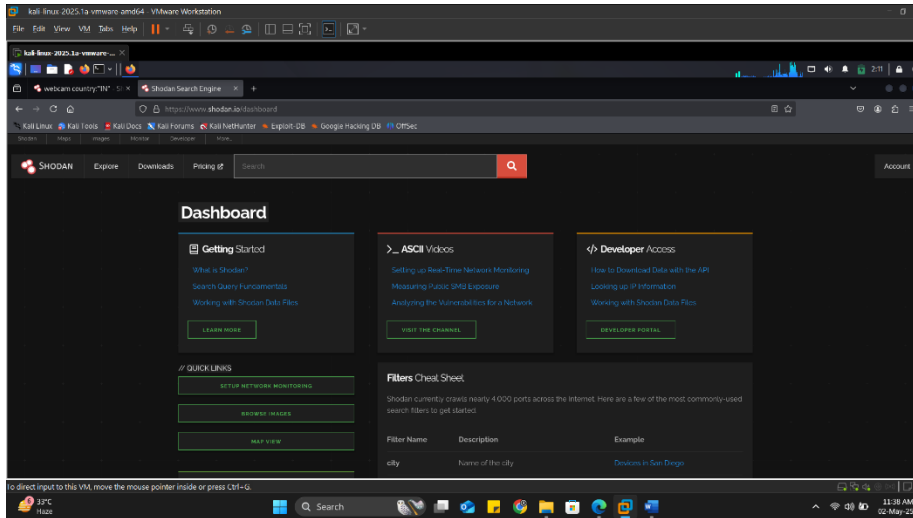
Using google dork: - Google dorks is a search technique that uses advanced operators to search for information that is not typically indexed by search engines.

A. Ghdb: GHDB is an information gathering technique used by an attacker for advanced google searching,



Result

- B. **Shodan.com**: - Shodan (Sentient Hyper-Optimised Data Access Network) is a search engine designed to map and gather information about internet-connected devices and systems. Shodan is sometimes referred to as a search engine for the internet of things (IoT).

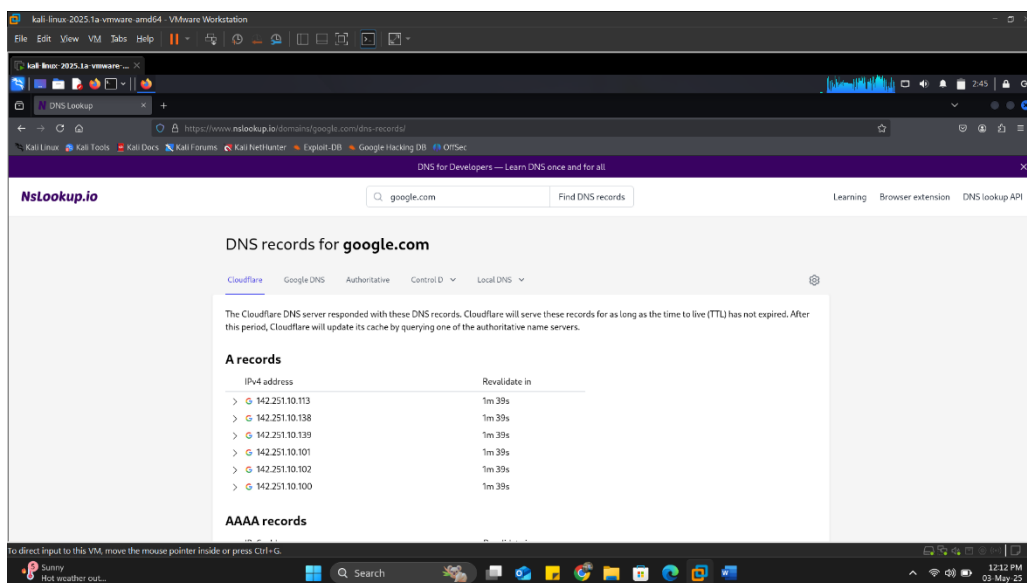
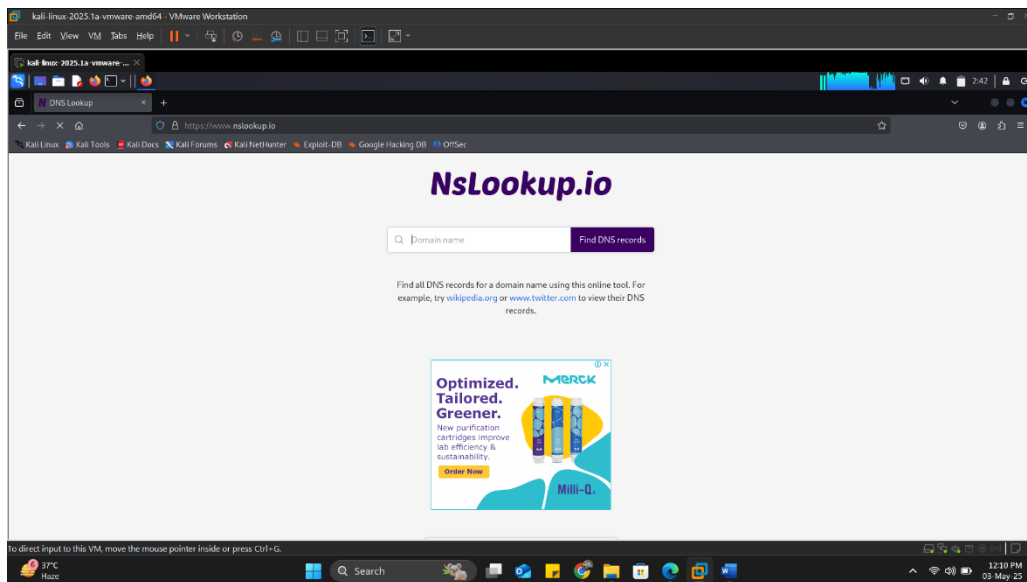


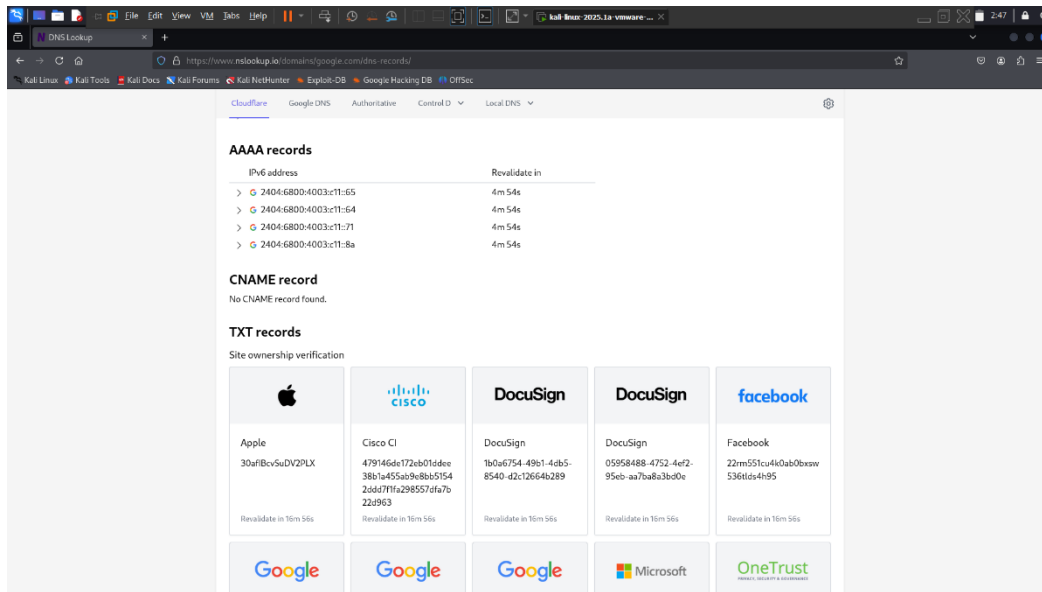
4) DNS Foot printing

DNS Foot printing is a technique that is used by an attacker to gather DNS information about the target system.

A. Nslookup:

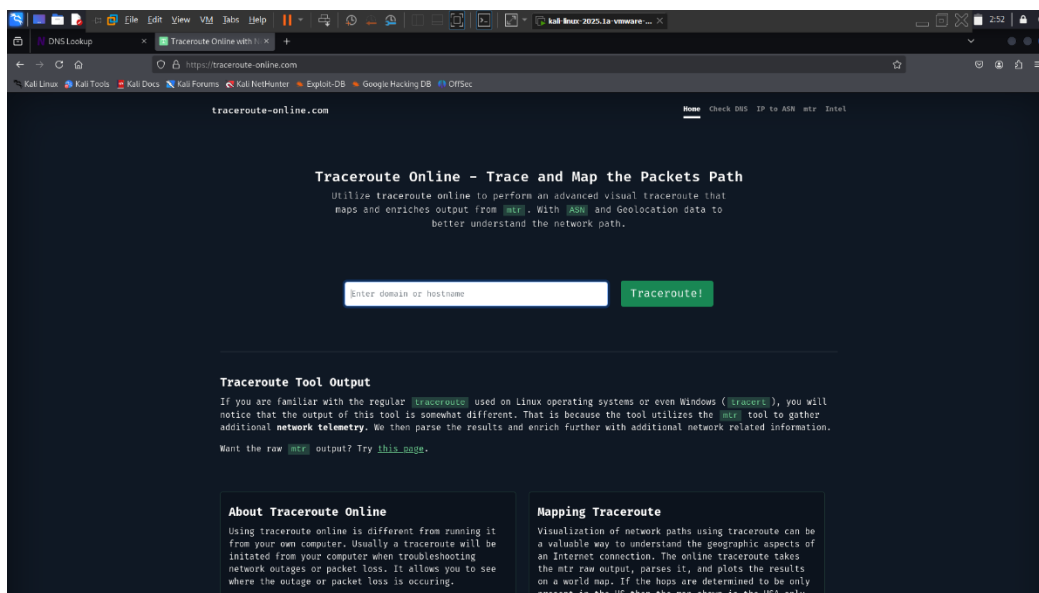
Nslookup is the name of a program that lets users enter a host name and find out the corresponding IP address or domain name system (DNS) record.





5) Network Foot printing

A. Traceroute online.com:



Traceroute Online - Trace and Map the Packets Path

Utilize traceroute online to perform an advanced visual traceroute that maps and enriches output from **tracert**. With **ASNs** and Geolocation data to better understand the network path.

google.com Traceroute!

Hop	Hostname	IP	AS	Network	Country
1	2000:3c8f::808	2000:3c8f::808	AS2001- LINODE-AP Atlanta Connected Cloud, US	2000:3c8f::/48	US
2	2000:3c8f::15:14	2000:3c8f::15:14	AS2001- LINODE-AP Atlanta Connected Cloud, US	2000:3c8f::/48	US
3	2000:3c8f::32:12	2000:3c8f::32:12	AS2001- LINODE-AP Atlanta Connected Cloud, US	2000:3c8f::/48	US
4	linode - Atlanta, GA	2000:3c8f::32:12	AS2001- LINODE-AP Atlanta Connected Cloud, US	2000:3c8f::/48	US
5	2000:3c8f::32:12	2000:3c8f::32:12	AS2001- LINODE-AP Atlanta Connected Cloud, US	2000:3c8f::/48	US
6	2000:3c8f::32:12	2000:3c8f::32:12	AS2001- LINODE-AP Atlanta Connected Cloud, US	2000:3c8f::/48	US
7	2000:3c8f::32:12	2000:3c8f::32:12	AS2001- LINODE-AP Atlanta Connected Cloud, US	2000:3c8f::/48	US
8	2001:468::12:3456	2001:468::12:3456	AS2001- LINODE-AP Atlanta Connected Cloud, US	2001:468::/32	US

Traceroute Online - Trace and Map the Packets Path

Utilize traceroute online to perform an advanced visual traceroute that maps and enriches output from **tracert**. With **ASNs** and Geolocation data to better understand the network path.

google.com Traceroute!

IP: 192.168.1.1

AS: 2001- LINODE-AP

Network: 2001:468::/32

Country: US

ASN Information

AS2001- LINODE-AP Atlanta Connected Cloud, US 15319

7.75 MS

AS2001- LINODE-AP Atlanta Connected Cloud, US 15319

0.80 MS

Traceroute Tool Output

If you are familiar with the regular **tracert** tool used on Linux operating systems or even windows (**tracert**), you will notice that the output of this tool is somewhat different. That is because this tool utilizes the **tracert** tool to gather additional network information, so this gives the results and much further with additional network related information.

Want the raw **tracert** output? Try [this link](#).

About Traceroute Online Mapping Traceroute

6) Eavesdropping

Eavesdropping: An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices. 7)

Shoulder surfing



7) Shoulder surfing

Shoulder surfing: - A shoulder surfing attack describes a situation where the attacker can physically view the device screen and keypad to obtain personal information.



8) Dumpster diving

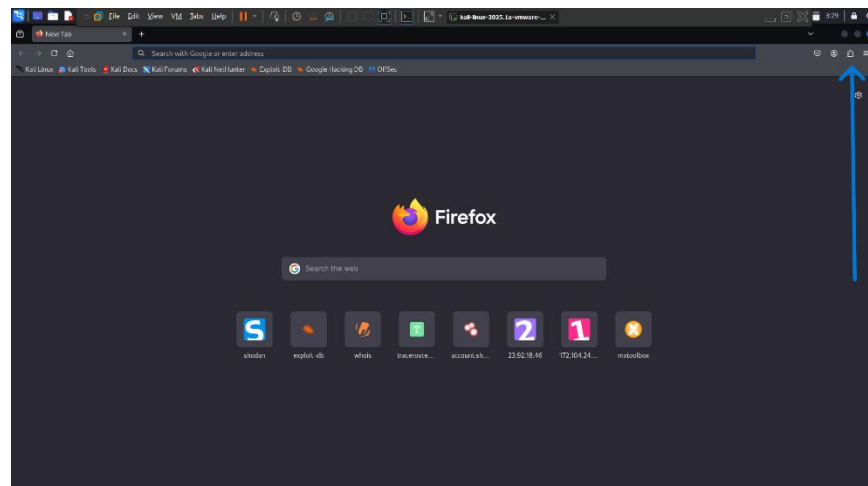
Dumpster diving: - Dumpster diving is the process of searching trash to obtain useful information about a person/company/business that can later be used for the hacking purpose.



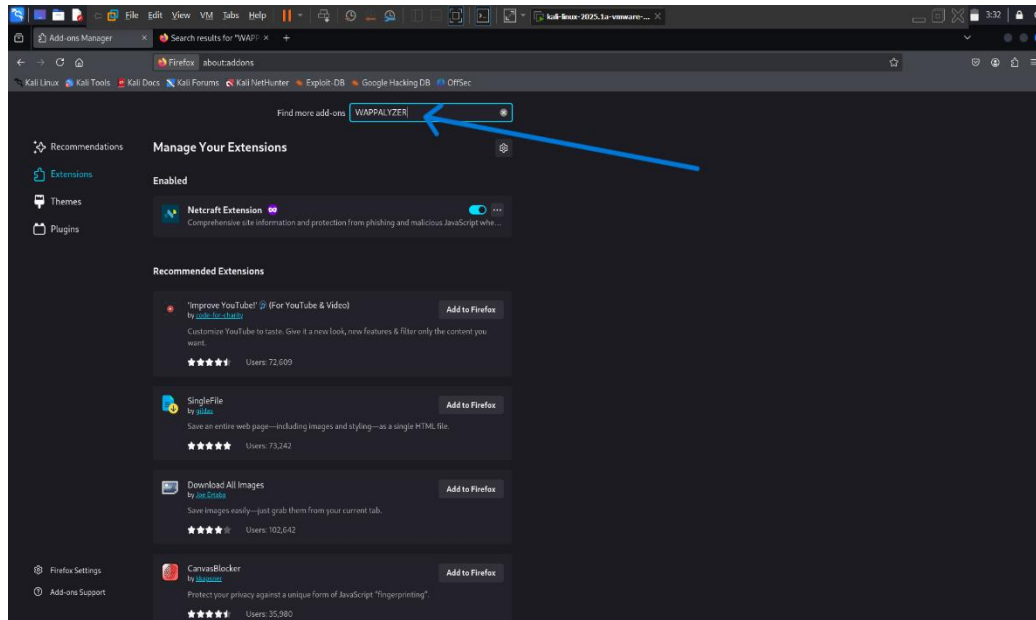
❖ Some important add-on on Fire Fox

WAPPALYZER

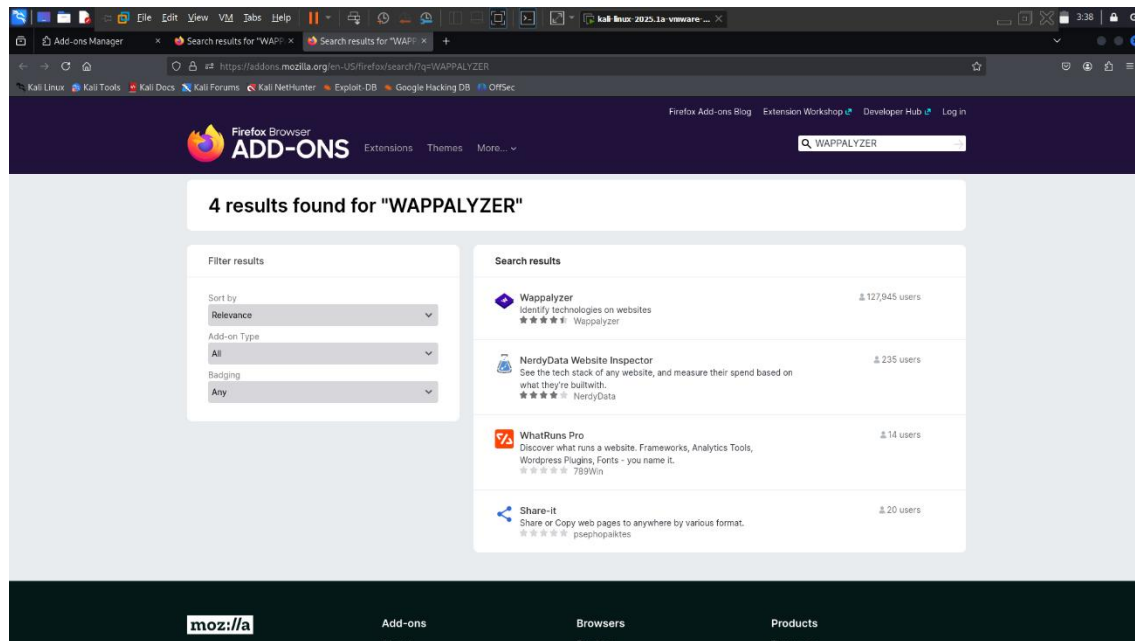
Step 1: Open Firefox and on top right corner click on that puzzle button



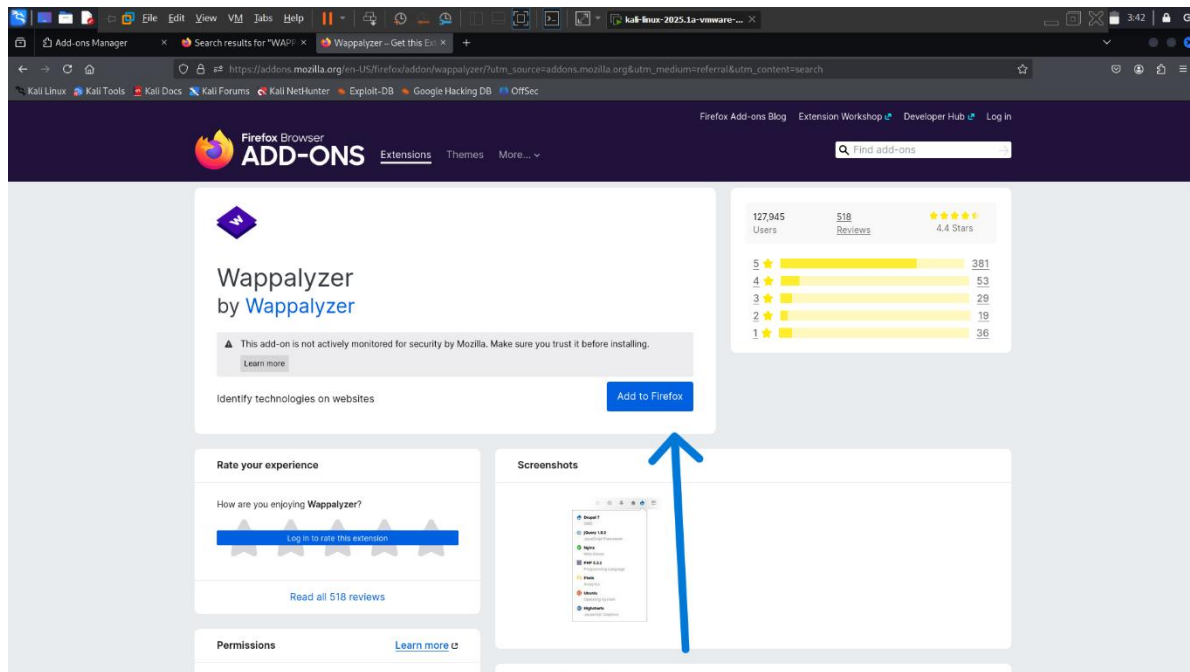
Step 2: Search for Wappalyzer.



Step 3: Click On Wappalyzer.



Step 4: Click to Add on :



NETCRAFT: Follow same process to add an extension of netcraft in your browser.
