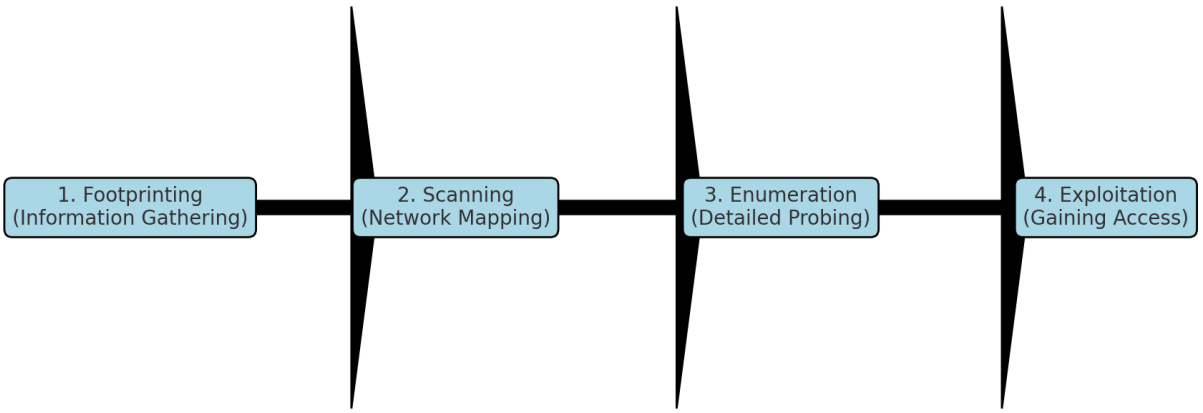
CEH Footprinting & Reconnaissance – Zero to Hero Guide



1. Introduction – What is Footprinting?

Imagine you are planning to enter a locked building.
Before touching the door, you:

- **Look where CCTV cameras are.**
- **Count the floors.**
- **Note the side windows.**
- **Watch when people enter or leave.**

This "collecting information before acting" is called Footprinting in hacking.

In CEH, Footprinting & Reconnaissance is the first step of hacking — gathering maximum information about a target before touching their systems.

Footprinting:

Footprinting is the process of collecting information related to the target network. Footprinting helps in identifying Various ways to intrude into an Organization's network system.

In this step attacker tries to gather publicly available sensitive information, using which he/she can carry out social engineering, perform system or network level attacks, that can cause substantial financial loss or damage the

reputation of an individual or organization. This step helps an attacker in gaining a basic idea of network structure and organization's infrastructure details.

Example:

A hacker researching a company may look at its website, LinkedIn employee profiles, and old archived pages to find clues about technology used.

2. Why is Footprinting Important?

🛠️ For Hackers – Helps find weak spots before launching an attack.
🛡️ For Security Teams – Helps discover and fix leaks before hackers find them.
🎯 For Both – Reduces guesswork by knowing the target's setup.

Example:

If you know a building has a side door without a guard, you'll plan your approach there instead of the main gate.

3. Types of Footprinting

3.1 Passive Footprinting –{*Silent Observation*} :

Involves gathering information about the target without direct interaction.

Collecting info without directly interacting with the target.

- Searching on Google.
- Reading news articles.
- Checking social media.

Example:

You watch a shop from across the street to see customer flow — no contact, no risk.

3.2 Active Footprinting – *{Direct Interaction}:* Involves gathering information about the target with direct interaction. The target may recognize the ongoing information gathering process

Directly engaging with the target's systems or people.

- Calling employees (social engineering).
- Running a traceroute to find network hops.

Example:
You walk into the shop and ask the staff about their products.

4. What Information Can Be Collected?

Network Info: Domain names, IP addresses, server locations.

System Info: OS type, open ports, service banners.

Organization Info: Employee names, office address, phone numbers.

Example:
Finding a company's HR email from LinkedIn and then guessing the format of all company emails (e.g., firstname.lastname@company.com)

How to perform Footprinting

● Through search engines

● Through social networking sites

● Through official websites

● Direct communication with the target

● Through job portals

● Through DNS enumeration

5. How to Defend Against Footprinting

- **Review public info before posting online.**
- **Hide WHOIS details with privacy protection.**
- **Avoid exposing sensitive files.**
- **Train employees against social engineering.**
- **Use IDS to detect scanning attempts.**

PRACTICALS

1] Finding domain registration details with Whois tool

What is Whois?

When someone buys a domain name (like example.com), they must give details such as:

- **Owner's name or organization**
- **Contact email and phone**
- **Registration date & expiry date**
- **Domain registrar (the company that registered the domain)**

All this data is stored in a public database called WHOIS.
The Whois tool allows us to search this database and get information about domain

Why is it useful in Footprinting?

- **Reveals the organization or person owning the domain.**
- **Shows technical contacts who manage the domain.**

- Gives creation and expiry dates — useful for planning attacks or knowing if a domain is abandoned.

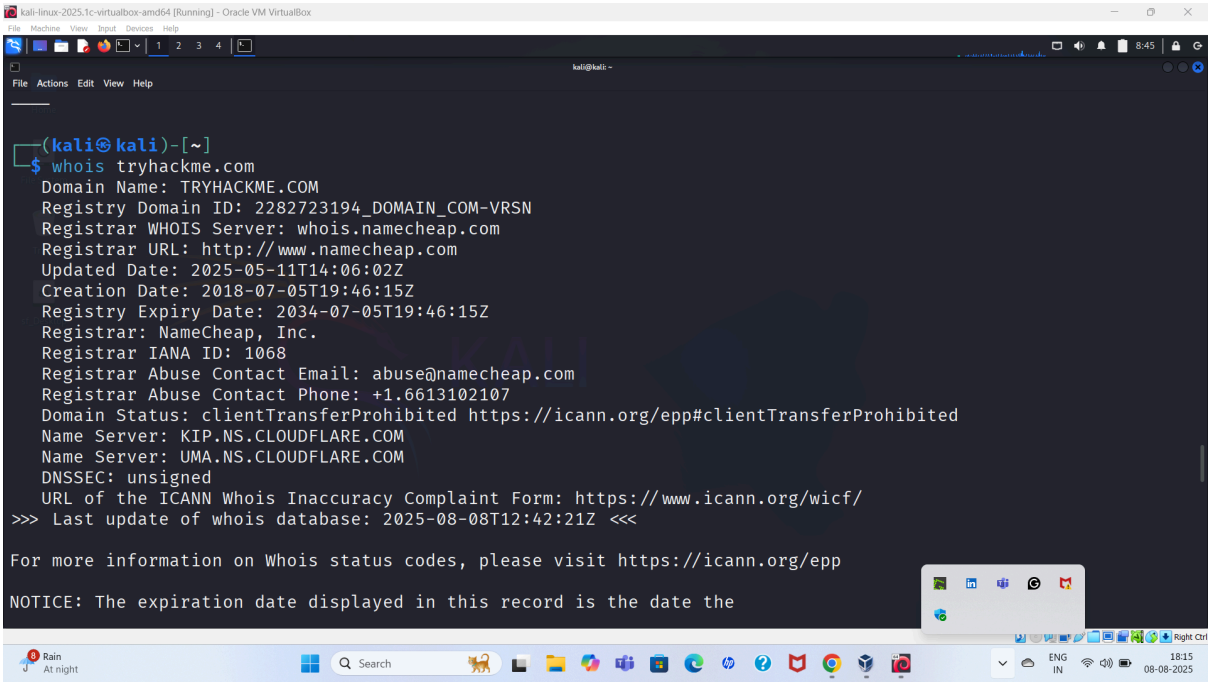
- Can lead to discovering other related domains owned by the same company.

Steps to Perform Whois Lookup

Example: our target is tryhackme.com

1.Open the kali terminal.
2.Type the command:

whois tryhackme.com



Finding Target's IP Address using IP Tracking Technique

What is IP Tracking?

IP tracking is a method of finding the public IP address of a person's device when they click on a specially prepared link.
Once you know the IP address, you can also get extra details like:

- **Approximate location (city, country)**
- **Internet Service Provider (ISP)**
- **Operating System & Browser**
- **Device type**

Why is it useful in Footprinting?

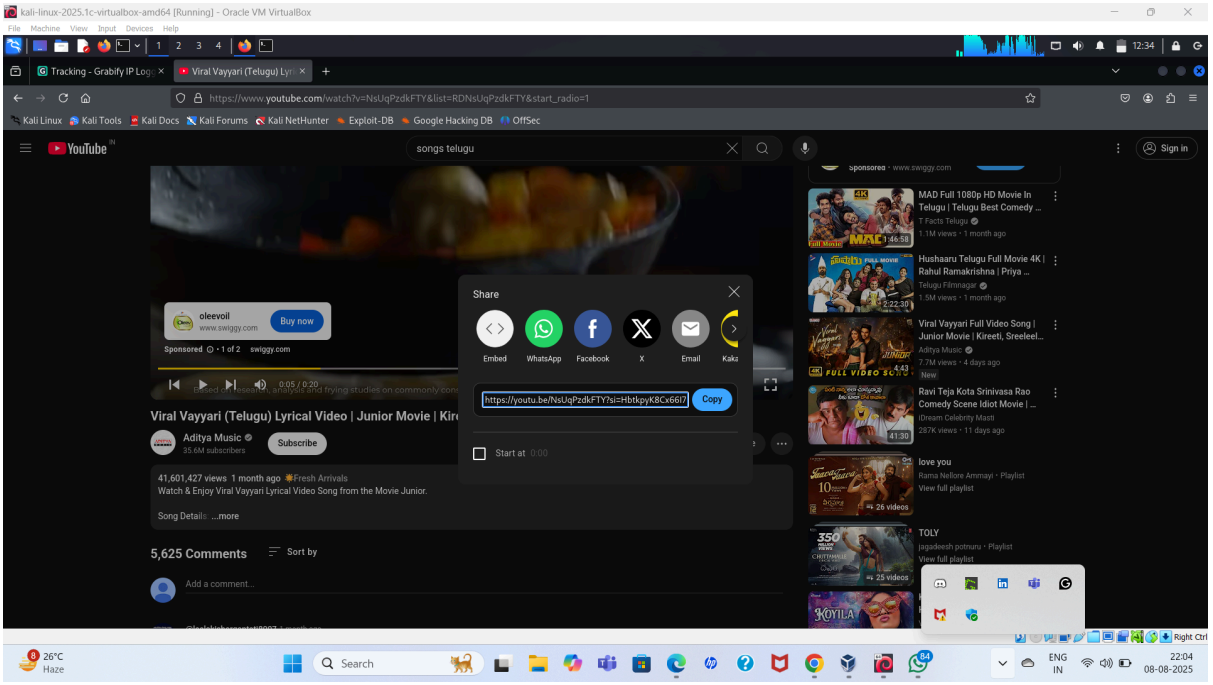
- **Helps understand where the target is located.**
- **Can identify the type of device and OS the target uses.**
- **Can be the first step for further reconnaissance.**

Example:
If you learn that an employee uses Windows 7 and is located in Hyderabad, you might target known vulnerabilities in that OS.

Steps to Perform IP Tracking

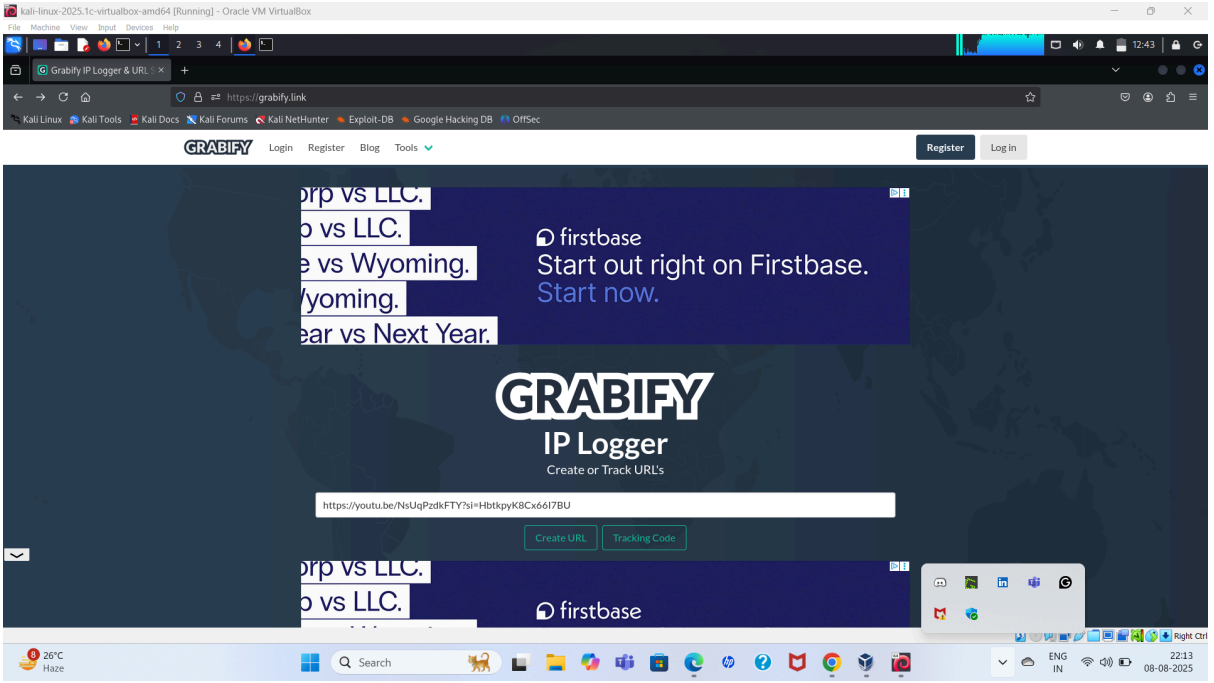
Open the Grabify website:
Go to https://grabify.link/.

Enter a destination URL:
Example: A YouTube video link.



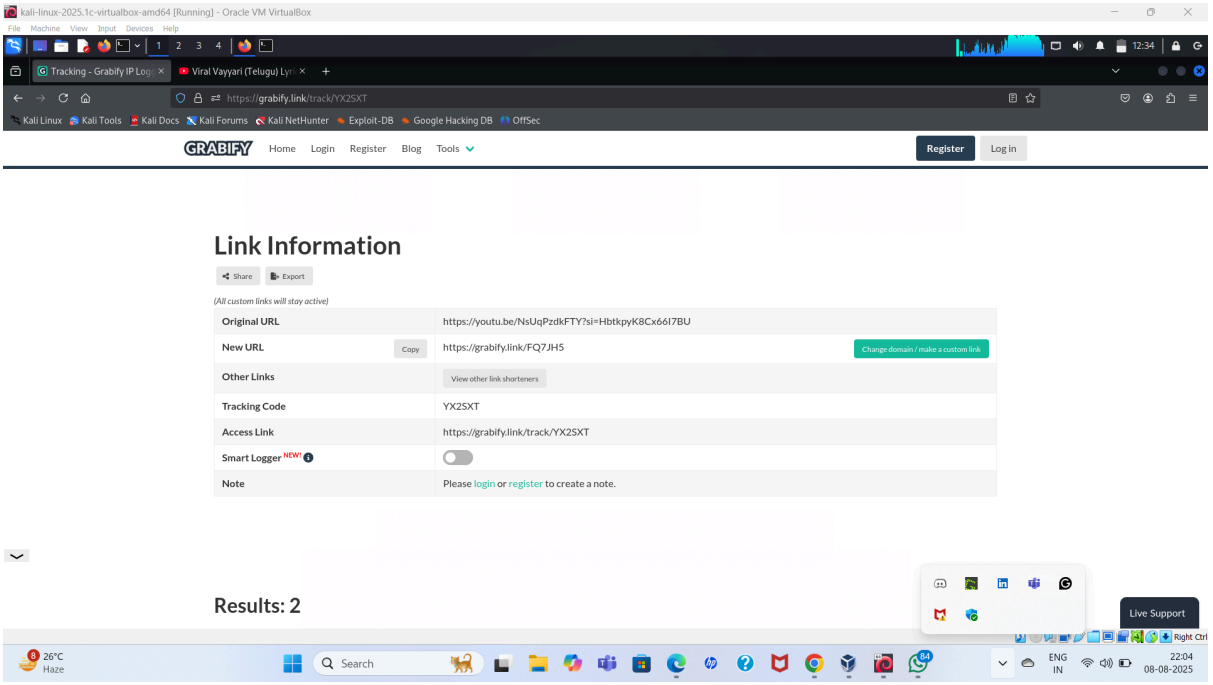
Paste it into the Grabify input box.

Click Create URL.



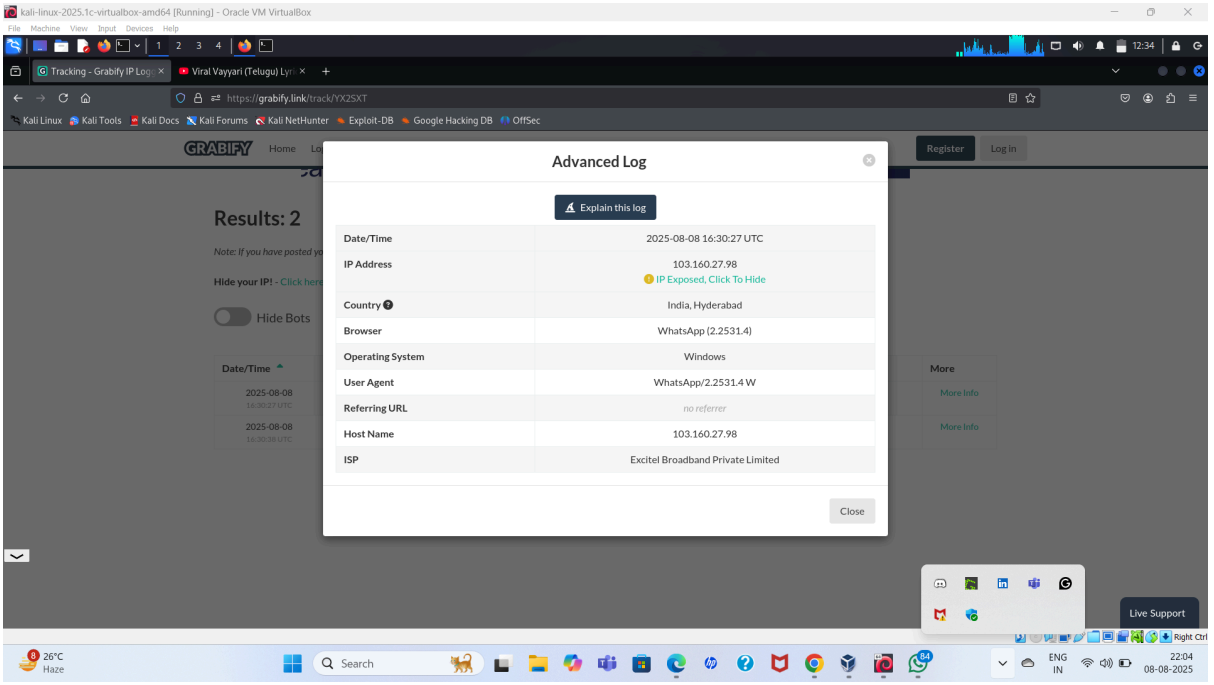
Get your tracking link:

- **Grabify will give you a New URL.**
- **This is the link you share with the target**



Wait for the click:

- **When the target clicks the link, they are taken to the real site (e.g., YouTube).**
- **In the background, Grabify logs their details.**



Understanding the Results:

- **IP Address: Public IP of the target's internet connection.**
- **ISP: The internet provider (e.g., Airtel, Jio).**
- **Location: Approximate city/country.**
- **User Agent: Shows OS and browser version.**

Common Tools for Footprinting & Reconnaissance

(For ethical and legal testing only)

- **Whois – Domain registration details**
- **TheHarvester – Emails, subdomains, hostnames**
- **Nslookup / Dig – DNS records lookup**
- **Recon-ng – Web reconnaissance framework**
- **Sublist3r – Subdomain enumeration**
- **Google Dorks – Advanced search queries**
- **Archive.org – Historical site data**
- **Sherlock – Username search across platforms**
- **Shodan – Search for internet-connected devices**
- **Maltego – Data visualization and link analysis**
- **Censys – Internet scanning and data collection**
- **FOCA – Metadata extraction from documents**
- **Grabify – IP tracking via links**
- **Nmap – Network scanning (for active footprinting)**
- **EmailHunter / Hunter.io – Find professional email addresses**

List of Practicals

Footprinting Domain using Recon-ng Tool

Google Dorks

Gathering Information using Archive.org

Subdomain Enumeration using Sublist3r Tool

Username Enumeration across Social Platforms using Sherlock

Installing and Using Shell GPT (SGPT) for AI-powered Command Line Assistance

Installing tgpt on Linux

If you want this practicals message me on linkedin
www.linkedin.com/in/karthik-reddy-morapelly

Final Note:

This document is for educational purposes only.
All examples and commands are tested on safe domains like `example.com` and `tryhackme.com` to ensure legal and ethical practice.
Never test on live systems without proper permission.