# theHarvester

**theHarvester** is another tool like sublist3r which is developed using Python. This tool can be used by penetration testers for gathering information of emails, sub-domains, hosts, employee names, open ports, and banners from different public sources like search engines, PGP key servers, and SHODAN computer database. This tool can be used in passive reconnaissance and by anyone who needs to know what an attacker can see about the organization.

theHarvester (purposely spelt with a lower-case 't' at the beginning) is a commandline-based tool made by the team at **Edge-Security**. It is a Python-based tool meant to be used in the initial stages of an investigation by leveraging open source Intelligence (OSINT) to help determine a company's external threat landscape on the internet.

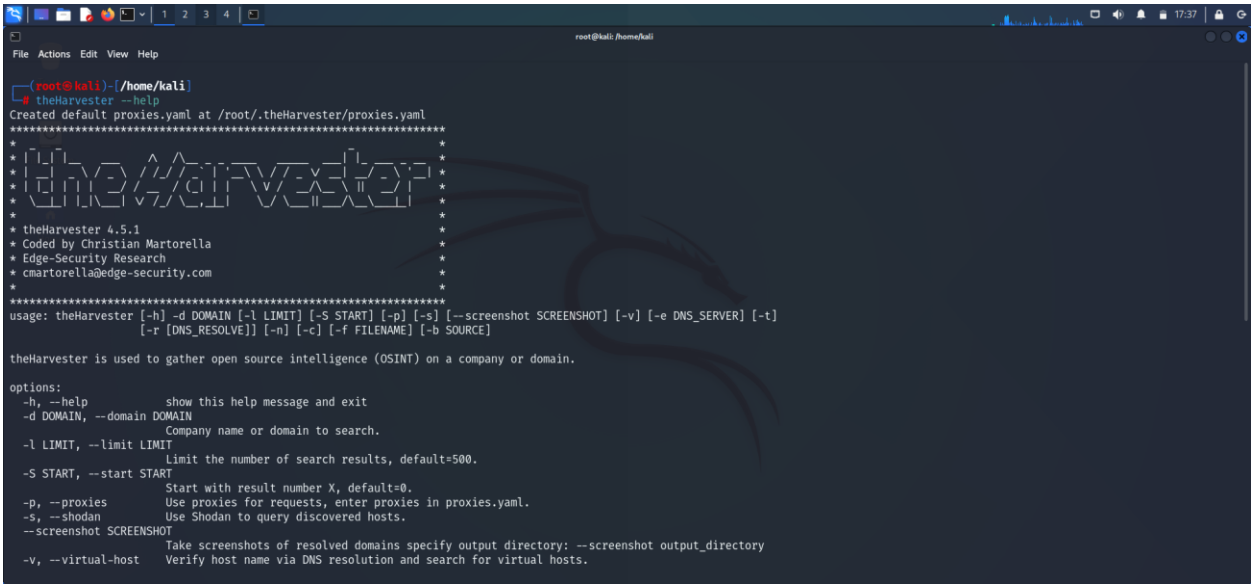
The tool was originally designed to be used in the early stages of a penetration test or red team engagement. However, the passive reconnaissance abilities of theHarvester also make it suitable for blue or purple teams, depending on the situation.

**TheHarvester can retrieve various types of information, including:**

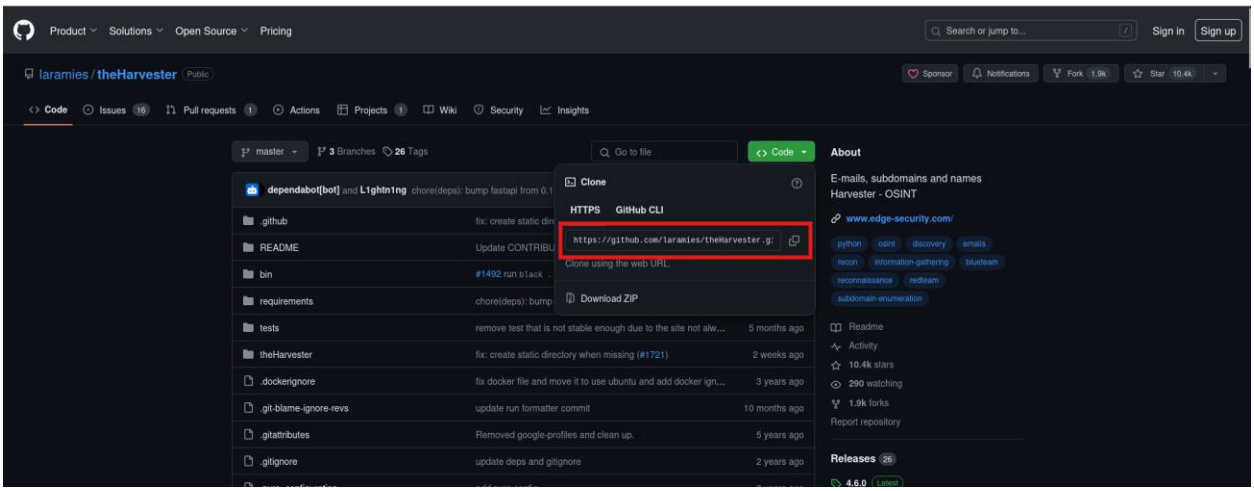
- **Email Addresses:** It can search for email addresses associated with a domain from search engines, social media platforms, and other public sources.
- **Domain Names:** It can enumerate subdomains associated with a target domain.
- **Hostnames:** It can discover hostnames associated with a target domain or IP address.
- **Open Ports:** It can identify open ports on target systems.
- **Virtual Hosts:** It can discover virtual hosts associated with web servers.
- **DNS Information:** It can gather DNS information such as DNS server names, mail exchanger (MX) records, and name server (NS) records.
- **Network Information:** It can retrieve information about the network infrastructure of a target organization.

# Steps to install and run:-

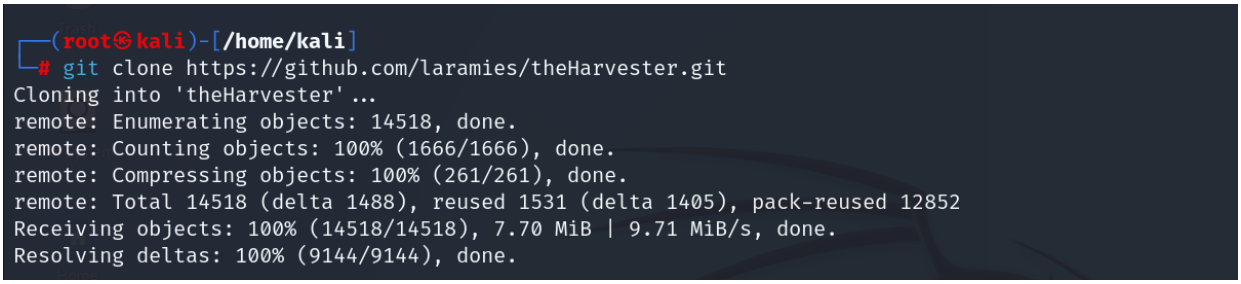
1. theHarvester tool is per-installed in Linux distribution. You can run it by just typing theHarvester inside the terminal.




2. If its not installed then, you can install it through its Github repository.

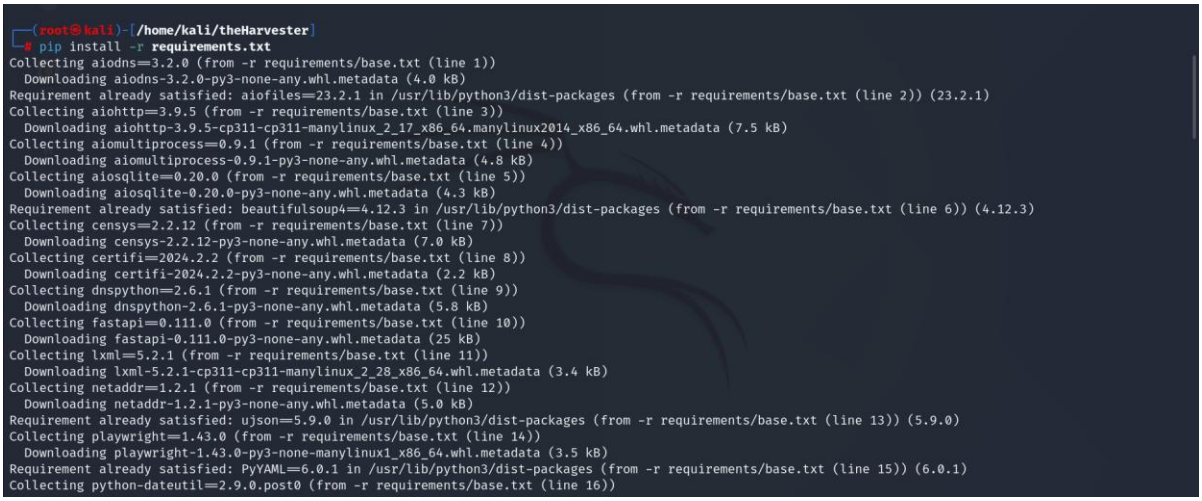


3. Just use git clone command into your terminal with the copied url of the tool.




4. Now after cloning it move towards its directory where you have clone it.

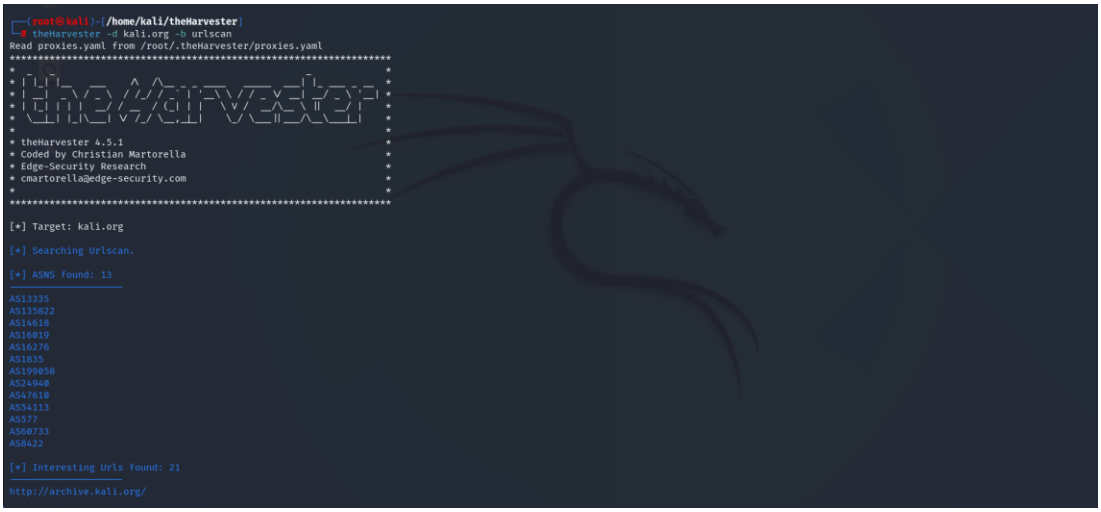

5. Now install the requirements.txt file using pip command.



**Now it is ready to use. theHarvester is available with various switches. I am going to demonstrate few of them.**

1. -d is used to define the target domain while -b is used to define the source of the search. Here I have searched for Microsoft.com in all the available search field by using the all parameter in the -b.


2. Now I just want to search under the scanurl search engine so I have define it inside -b.



# Here are few more commands for the particular purposes:

- **Search for Email Addresses:** theHarvester -d example.com -l 100 -b google
- **Enumerate Subdomains:** theHarvester -d example.com -l 100 -b Baidu
- **Discover Hostnames:** theHarvester -d example.com -l 100 -b bing
- **Identify Open Ports:** theHarvester -d example.com -b shodan
- **Discover Virtual Hosts:** theHarvester -d example.com -l 100 -b bing -f output.txt
- **Gather DNS Information:** theHarvester -d example.com -b all
- **Retrieve Network Information:** theHarvester -d example.com -l 100 -b netcraft