

Forum:[Hack Forums](#)

Thread: [Information Gathering using theHarvester in Kali Linux](#)

Decryption/Critical - February 14, 2024, 12:59 am

Today we will learn about Information Gathering using theHarvester in Kali Linux. Good information gathering can make the difference between a successful penetration test and one that has failed to provide maximum benefit to the client.

TheHarvester has been developed in Python by Christian Martorella. It is a tool which provides us information about e-mail accounts, user names and hostnames/subdomains from different public sources like search engines and PGP key server.

This tool is designed to help the penetration tester on an earlier stage; it is an effective, simple and easy to use. The sources supported are:

Google – emails, subdomains

Google profiles – Employee names

Bing search – emails, subdomains/hostnames, virtual hosts

Pgp servers – emails, subdomains/hostnames

LinkedIn – Employee names

Exalead – emails, subdomain/hostnames

New features:

Time delays between requests

XML results export

Search a domain in all sources

Virtual host verifier

Let's get started,

If you are using Kali Linux, open the terminal and type theharvester

If not then it can be easily downloaded from here: <https://github.com/laramies/theHarvester>

Simply Download and extract it

Provide execute permission to: theHarvester.py by [chmod 755 theHavester.py]

Then simply run `./theharvester`

Method:1

You can simply use the command `theHarvester -d [url] -l 300 -b [search engine name]`

For example: `theHarvester -d sixthstartech.com -l 300 -b google`

Method:2

To get all the information about the website u can use the command as:

`theHarvester -d sixthstartech.com -l 300 -b all`

Method:3

To save the result in HTML file you can use `-f` option followed by a file name,

Example:

`theHarvester.py -d sixthstartech.com -l 300 -b all -f test`

The result in HTML File: