



theHarvester

theHarvester

theHarvester is an open source intelligence (OSINT) tool which gathers information about email address, domain names and network infrastructure. It is a very useful tool for pentesters and security professionals to collect information about target to find out the potential vulnerabilities and assess overall security posture.

FEATURES OF TheHarvester

1. **Email Address Enumeration:** TheHarvester can search for email address for the associated with particular domain. It uses various search engines and public resources to gather information.
2. **Domain Information Collection:** This tool collects the information regarding domain, subdomain, DNS information and virtual hosts. It is a valuable information for pentesters and other security professionals to understand the online presence of the target.
3. **Network Infrastructure:** This tool provides information about network infrastructure and IP addresses of related domains which helps security professionals to build a plan for potential attack on target.
4. **Data Source:** TheHarvester tool supports various tools to gather information from public source i.e., Shodan, Google, Bing, public servers and various public repositories.



GUIDE TO INSTALL TheHarvester ON KALI LINUX

1. Open Terminal.

- You can open the terminal in kali linux by clicking on terminal icon or open using the keyboard shortcut **Ctrl + Alt + T**.

2. Update & Upgrade.

- Make sure that your system is up-to-date by following the below commands.

```
Sudo apt update  
Sudo apt upgrade
```

3. Install Required Dependencies.

- TheHarvester tool require some python libraries in order to extract information properly from the sources. Follow the below command to install python3 on your machine.

```
Apt install python3
```

4. Install TheHarvester Tool.

- Type the following command to install the tool in your linux machine.

```
git clone https://github.com/laramies/theHarvester.git
```

5. Change the directory to TheHarvester.

- After installation you need to change the directory by following command.

```
cd theHarvester
```

6. Install the requirements file for TheHarvester.

- After changing the directory, pull the list of the current directory and then install the requirements.txt file by following command.

```
Ls  
pip3 install -r requirements.tx
```

7. Run TheHarvester Tool.

- Run TheHarvester tool by following command.

```
theHarvester --help
```

INSTALLATION SCREENSHOTS

```
(root@kali)-[~]
# git clone https://github.com/laramies/theHarvester.git
Cloning into 'theHarvester' ...
remote: Enumerating objects: 14123, done.
remote: Counting objects: 100% (2678/2678), done.
remote: Compressing objects: 100% (289/289), done.
remote: Total 14123 (delta 2517), reused 2440 (delta 2389), pack-reused 11445
Receiving objects: 100% (14123/14123), 7.58 MiB | 1.49 MiB/s, done.
Resolving deltas: 100% (8942/8942), done.
```

INSTALLATION STEP: 1 & 4.

We have skipped the 2 & 3 step of installation because the system is already updated and upgraded. Also, the dependencies are already installed.

```
(root@kali)-[/home/kali]
# cd theHarvester
(root@kali)-[/home/kali/theHarvester]
# ls
bin          Dockerfile  pyproject.toml  README      requirements  restfulHarvest.py  tests          theHarvester-logo.png  theHarvester.py
docker-compose.yml  mpyy.ini      pytest.ini      README.md   requirements.txt  setup.cfg          theHarvester
(root@kali)-[/home/kali/theHarvester]
# pip3 install -r requirements.txt
Requirement already satisfied: aiohttp==3.1.1 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 1)) (3.1.1)
Requirement already satisfied: aiofiles==23.2.1 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 2)) (23.2.1)
Requirement already satisfied: aiohttp==3.9.1 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 3)) (3.9.1)
Requirement already satisfied: aiomultiprocess==0.9.0 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 4)) (0.9.0)
Requirement already satisfied: aioslite==0.19.0 in /usr/local/lib/python3.11/dist-packages (from -r requirements/base.txt (line 5)) (0.19.0)
Requirement already satisfied: beautifulsoup4==4.12.2 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 6)) (4.12.2)
Requirement already satisfied: census==2.2.10 in /usr/local/lib/python3.11/dist-packages (from -r requirements/base.txt (line 7)) (2.2.10)
Requirement already satisfied: certifi==2023.11.17 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 8)) (2023.11.17)
Requirement already satisfied: dnspython==2.4.2 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 9)) (2.4.2)
Requirement already satisfied: fastapi==0.108.0 in /usr/local/lib/python3.11/dist-packages (from -r requirements/base.txt (line 10)) (0.108.0)
Requirement already satisfied: lxml==5.0.1 in /usr/local/lib/python3.11/dist-packages (from -r requirements/base.txt (line 11)) (5.0.1)
Requirement already satisfied: netaddr==0.10.1 in /usr/local/lib/python3.11/dist-packages (from -r requirements/base.txt (line 12)) (0.10.1)
Requirement already satisfied: ujson==5.9.0 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 13)) (5.9.0)
Requirement already satisfied: pyppeteer==1.0.2 in /usr/local/lib/python3.11/dist-packages (from -r requirements/base.txt (line 14)) (1.0.2)
Requirement already satisfied: PyYAML==6.0.1 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 15)) (6.0.1)
Requirement already satisfied: python-dateutil==2.8.2 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 16)) (2.8.2)
Requirement already satisfied: requests==2.31.0 in /usr/local/lib/python3.11/dist-packages (from -r requirements/base.txt (line 17)) (2.31.0)
Requirement already satisfied: retrying==1.3.4 in /usr/local/lib/python3.11/dist-packages (from -r requirements/base.txt (line 18)) (1.3.4)
Requirement already satisfied: setuputils==69.0.3 in /usr/local/lib/python3.11/dist-packages (from -r requirements/base.txt (line 19)) (69.0.3)
Requirement already satisfied: shodan==1.31.0 in /usr/local/lib/python3.11/dist-packages (from -r requirements/base.txt (line 20)) (1.31.0)
Requirement already satisfied: slowapi==0.1.8 in /usr/local/lib/python3.11/dist-packages (from -r requirements/base.txt (line 21)) (0.1.8)
Requirement already satisfied: uvicorn==0.25.0 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 22)) (0.25.0)
Requirement already satisfied: uvloop==0.19.0 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 23)) (0.19.0)
Requirement already satisfied: soupsieve==1.2 in /usr/lib/python3/dist-packages (from beautifulsoup4==4.12.2-->-r requirements/base.txt (line 6)) (2.5)
```

INSTALLATION STEPS: 5 & 6.

```
(root@kali)-[~]
# theHarvester --help
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
*                               *
*  theHarvester                 *
*                               *
* theHarvester 4.5.0            *
* Coded by Christian Martorella *
* Edge-Security Research        *
* cmartorella@edge-security.com *
*                               *
*****
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-s START] [-p] [-s] [--screenshot SCREENSHOT]
                  [-e DNS_SERVER] [-t] [-r [DNS_RESOLVE]] [-n] [-c] [-f FILENAME] [-b SOURCE]

theHarvester is used to gather open source intelligence (OSINT) on a company or domain.

options:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Company name or domain to search.
  -l LIMIT, --limit LIMIT
                        Limit the number of search results, default=500.
  -s START, --start START
                        Start with result number X, default=0.
  -p, --proxies          Use proxies for requests, enter proxies in proxies.yaml.
  -s, --shodan           Use Shodan to query discovered hosts.
  --screenshot SCREENSHOT
                        Take screenshots of resolved domains specify output directory: --screenshot
                        output_directory
  -v, --virtual-host     Verify host name via DNS resolution and search for virtual hosts.
  -e DNS_SERVER, --dns-server DNS_SERVER
                        DNS server to use for lookup.
  -t, --take-over        Check for takeovers.
```

STEP: 7

STEPS TO ADDING API-KEY TO .YAML FILE

1. Open Terminal.

- Type the below command in the terminal to open the .Yaml file.

```
sudo mousepad /etc/theHarvester/api-keys.yaml
```

2. Navigate to Websites.

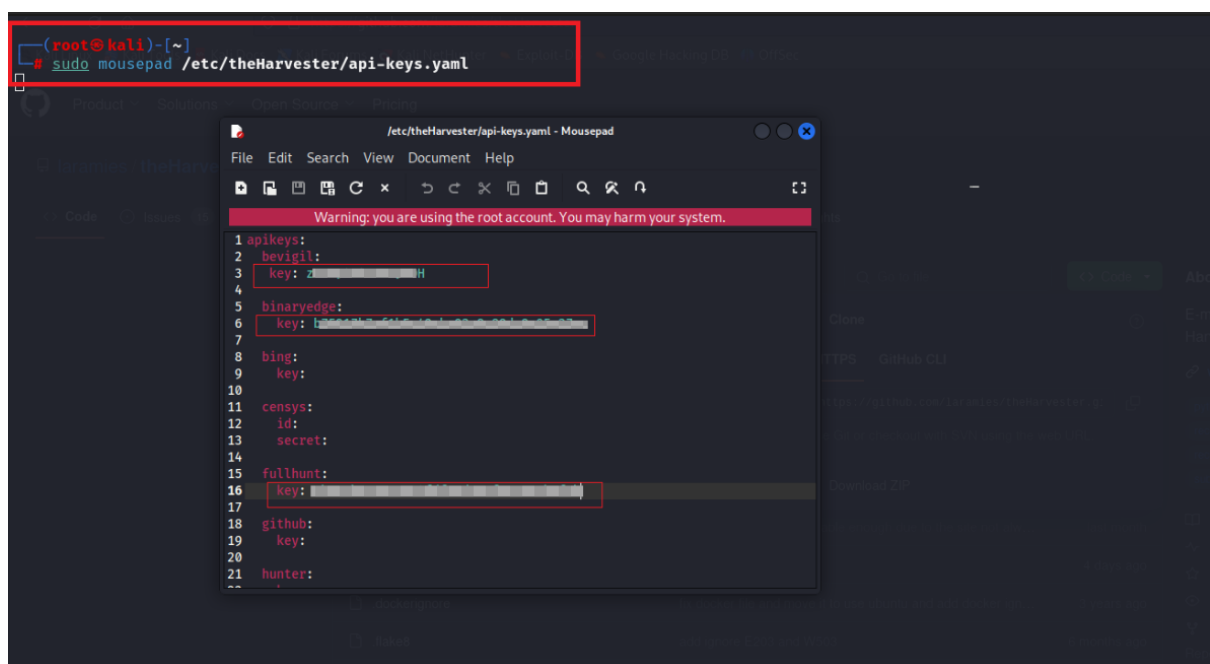
- Once you hit enter by following the above command, you'll see one dialogue box opened which contains websites name and API key field empty. Now navigate to those websites and sign-up using any dummy email credentials and then copy the API key from the specific website and paste it in the box under the respective website.

“Make sure you hit space bar once and then paste the API key”

3. Save the API Key.

- Once you paste the API key then click on **“file”** option and click on save.

API-KEY ADDING SCREENSHOTS



STEP: 1,2 & 3

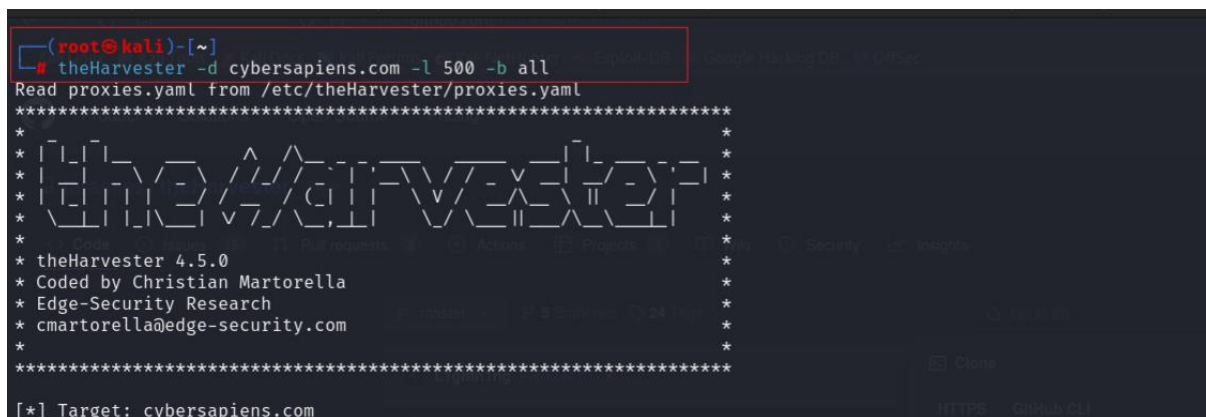
ADVANTAGES OF TheHarvester TOOL

1. **Community Support:** This tool is widely used in cyber security to gather information from different source which is publicly available. The community has created a documentation on this tool about its command and usage. Also the make sure the tool is up-to-date.
2. **OSINT (Open-Source Intelligence):** This tool builds a details profile of the target system which gives an idea of the online presence of the target.

LIVE USAGE OF TheHarvester TOOL WITH SCREENSHOT

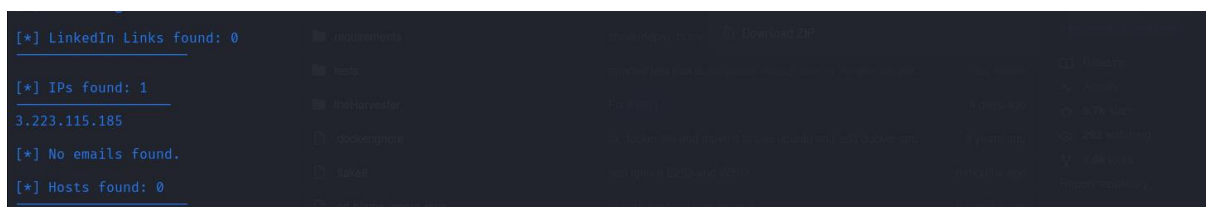
By following the below given command you can extract the details of the domain, email address of that particular domain (If existing) and add the source from where do you want to extract that information. (The master command is always to search with “all”) to get detail results.

theHarvester -d domain -l 500 -b all



```
(root@kali)~# theHarvester -d cybersapiens.com -l 500 -b all
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
*                               *
* theHarvester 4.5.0            *
* Coded by Christian Martorella *
* Edge-Security Research        *
* cmartorella@edge-security.com *
*                               *
*****
[*] Target: cybersapiens.com
```

SCREENSHOT: TARGET DOMAIN “CYBERSAPIENS”



```
[*] LinkedIn Links found: 0
[*] IPs found: 1
3.223.115.185
[*] No emails found.
[*] Hosts found: 0
```

SCREENSHOT: RESULTS

REFERENCES

<https://github.com/laramies/theHarvester>

https://www.youtube.com/watch?v=XKyjadN_Pmg

<https://chat.openai.com/>

<https://www.kali.org/tools/theharvester/>