

INFORMATION GATHERING USING THEHARVESTER.

TOOL: THEHARVESTER

theHarvester is an open-source tool used for gathering information (reconnaissance) about a target during the early stages of penetration testing or ethical hacking. It helps security professionals collect publicly available data about domains, email addresses, employee names, IP addresses, subdomains, and other details that can be useful in mapping a target's attack surface.

The tool works by querying various public search engines, such as Google, Bing, and specialized databases like LinkedIn or Shodan

Task 1

```
sudo apt-get install python3-pip
sudo pip3 install virtualenv
virtualenv venv
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt-get install python3-pip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3-pip is already the newest version (24.2+dfsg-1).
The following packages were automatically installed and are no longer required:
 fonts-liberation2 freerdp2-x11 hydra-gtk ibverbs-providers libassuan0 libavfilter9 libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2
 libdaxctl1 libfreerdp-client2-2t64 libfreerdp2-2t64 libgail-common libgail18t64 libgeos3.12.1t64 libgeos3.12.2 libgfpapi0 libgfrpc0 libgfxdr0
 libglusterfs0 libgspell-1-2 libgtk2.0-0t64 libgtk2.0-bin libgtk2.0-common libibverbs1 libimobiledevice6 libiniparser1 libjim0.82t64
 libjsoncpp25 libjxl0.7 libmfx1 libndctl6 libplacebo338 libplist3 libpmem1 libpostproc57 librados2 librav1e0 librdmacm1t64 libre2-10 libroc0.3
 libsvtaviencl1 libu2f-udev libusbmuxd6 libwinpr2-2t64 libx265-199 linux-image-6.6.15-amd64 openjdk-17-jre openjdk-17-jre-headless
 python3-diskcache python3-hatch-vcs python3-hatchling python3-mistune0 python3-pathspect python3-pendulum python3-pluggy python3-pytzdata
 python3-setuptools-scm python3-trove-classifiers rwho rwho-d samba-ad-provision samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 178 not upgraded.
```

```
(kali@kali)-[~]
$ virtualenv venv
created virtual environment CPython3.11.9.final.0-64 in 1245ms
creator CPython3Posix(dest=/home/kali/venv, clear=False, no_vcs_ignore=False, global=False)
seeder FromAppData(download=False, pip=24.2, setuptools=74.1.2, wheel=0.44.0)
activators BashActivator, CShellActivator, FishActivator, NushellActivator, PowerShellActivator, PythonActivator
```

```
(kali@kali)-[~]
$ sudo pip3 install virtualenv
Requirement already satisfied: virtualenv in /usr/lib/python3/dist-packages (20.26.2)
Requirement already satisfied: distlib<1, >=0.3.7 in /usr/lib/python3/dist-packages (from virtualenv) (0.3.8)
Requirement already satisfied: filelock<4, >=3.12.2 in /usr/lib/python3/dist-packages (from virtualenv) (3.15.4)
Requirement already satisfied: platformdirs<5, >=3.9.1 in /usr/lib/python3/dist-packages (from virtualenv) (4.3.6)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager, possibly rendering your system unusable. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv. Use the --root-user-action option if you know what you are doing and want to suppress this warning.
```

Clone the git repo:

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

```
(kali@kali)-[~]
$ git clone https://github.com/laramies/theHarvester.git
Cloning into 'theHarvester'...
remote: Enumerating objects: 15093, done.
remote: Counting objects: 100% (2944/2944), done.
remote: Compressing objects: 100% (471/471), done.
remote: Total 15093 (delta 2711), reused 2605 (delta 2473), pack-reused 12149 (from 1)
Receiving objects: 100% (15093/15093), 7.76 MiB | 1.85 MiB/s, done.
Resolving deltas: 100% (9598/9598), done.
```

cd theHarvester pip3 install -r requirements.txt

```
(kali@kali)-[~]
$ cd theHarvester

(kali@kali)-[~/theHarvester]
$ pip3 install -r requirements.txt
```

./theHarvester.py -v

```
(kali@kali)-[~/theHarvester]
$ ./theHarvester.py -v
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*****
*
*
*
*
*
*
* theHarvester 4.7.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
usage: theHarvester.py [-h] -d DOMAIN [-l LIMIT] [-s START] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t] [-r [DNS_RESOLVE]]
                        [-n] [-c] [-f FILENAME] [-b SOURCE]
theHarvester.py: error: the following arguments are required: -d/--domain
```

Task 2

To launch an information gathering campaign on a target, type the following:

./theHarvester.py -d hackaday.com -l 300 -b yahoo

This will start theHarvester. It will begin searching Google for the top 300 results related to hackaday.com.

For this target, we could not find any information on Google. Let us dig deeper.

```
[*] Target: hackaday.com

An exception has occurred: Cannot connect to host search.yahoo.com:443 ssl:<ssl.SSLContext object at 0x7fc22471c4d0> [None]
An exception has occurred: Cannot connect to host search.yahoo.com:443 ssl:<ssl.SSLContext object at 0x7fc2252fbda0> [None]
An exception has occurred: Cannot connect to host search.yahoo.com:443 ssl:<ssl.SSLContext object at 0x7fc2252fbc80> [None]
[*] Searching Yahoo.

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 0
```

```
[*] Hosts found: 142
```

```
1000.hackaday.com  
_dmarc.hackaday.com  
_mta-sts.hackaday.com  
activities.hackaday.com  
adobe-dns.hackaday.com  
als.hackaday.com  
answers.hackaday.com  
apc4.hackaday.com  
api.hackaday.com  
aurora.hackaday.com  
back2.hackaday.com  
bbs.hackaday.com  
blog.hackaday.com  
blogs.hackaday.com  
boutique.hackaday.com  
broker.wip3.hackaday.com  
browseusers.hackaday.com  
bz2.hackaday.com  
careers.hackaday.com  
cdn.hackaday.com  
cellphon.hackaday.com  
cellphones.hackaday.com  
citrix.hackaday.com  
cname.hackaday.com  
confluence.hackaday.com  
cosmic.hackaday.com  
day.hackaday.com  
de.hackaday.com
```

Task 3

If we want to gather even more information about our target, we can specify the following:

```
./theHarvester.py -d hackaday.com -l 300 -b all
```

```
[*] IPs found: 111
```

```
104.112.163.37  
104.21.5.216  
104.236.6.220  
104.80.89.115  
141.136.42.129  
144.126.218.153  
149.154.164.13  
157.238.74.72  
162.243.127.7  
165.254.206.8  
165.254.207.90  
165.254.245.32  
165.254.26.50  
165.254.94.154  
165.254.94.162  
167.172.237.176  
172.66.44.87  
172.67.135.103  
172.67.149.67  
172.67.157.76  
172.67.164.88  
172.67.177.64  
172.67.209.120  
184.25.102.89  
185.176.43.98  
185.199.108.153  
185.199.111.153
```

Task 4