INFORMATION GATHERING USING THEHARVESTER.

TOOL: THEHARVESTER

the Harvester 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⊕ 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 rend ering 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

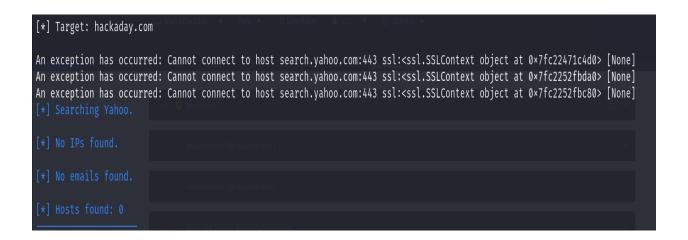
Task 2

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

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

This will start the Harvester. 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.



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

Task 4