theHarvester 3.0.0 Cheatsheet (ingenieriainformatica.uniovi.es)

Website OSINT tool

https://tools.kali.org/information-gathering/theharvester

GENERAL USAGE

```
theharvester options
```

NOTES

Installable directly from Kali Linux repositories

OPTIONS

-b: data source: baidu, bing, bingapi, dogpile, google, googleCSE, googleplus, google-profiles, linkedin, pgp, twitter, vhost, virustotal, threatcrowd, crtsh, netcraft, yahoo, all

-c: perform a DNS brute force for the domain name

-d: Domain to search or company name

-e: use this DNS server

-f: save the results into an HTML and XML file (both)

-h: use SHODAN database to query discovered hosts

-l: limit the number of results to work with(bing goes from 50 to 50 results, google 100 to 100, and pgp doesn't use this option)

-n: perform a DNS reverse query on all ranges discovered

-p: port scan the detected hosts and check for Takeovers (80,443,22,21,8080)

-s: start in result number X (default: 0)

-t: perform a DNS TLD expansion discovery

-v: verify host name via dns resolution and search for virtual hosts

EXAMPLES

theharvester -d uniovi.es -l 50 -b google
theharvester -d uniovi.es -b pgp
theharvester -d uniovi -l 200 -b linkedin
theharvester -d uniovi.es -b googleCSE -l 100 -s 300

by José Manuel Redondo López

```
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when f
uzzing SSL sites. Check Wfuzz's documentation for more information.


*******************************************************************
*                                                                 *
* | |_| |_   ___     /\  /\___ _ __ _____   _____ ___| |_ ___ _ __  *
* | __| '_ \ / _ \   / /_/ / _` | '__\ \ / / _ \ __/ _ \ '__| *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/ ||  __/ |    *
*  \__|_| |_|\___|  \/ /_/ \__,_|_|    \_/ \___|\__\___|_|    *
*                                                                 *
* theHarvester Ver. 3.0.6                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: baidu, bing, bingapi, censys, crtsh, dogpile,
                        google, google-certificates, googleCSE, googleplus, google-pro
files,
                        hunter, linkedin, netcraft, pgp, threatcrowd,
                        twitter, vhost, virustotal, yahoo, all
       -g: use Google dorking instead of normal Google search
       -s: start in result number X (default: 0)
       -v: verify host name via DNS resolution and search for virtual hosts
```