theHarvester Cheat Sheet Cheat Sheet

by ClassAssignment124 via cheatography.com/146937/cs/31875/

Usage:

theHarvester: `[-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s] [--scr eenshot SCREEN SHOT] [-v] [-e DNS_SE R` `[-b SOURCE]`

Optional Arguments:

-d *DOMAIN*	Company name or domain to search
-l *LIMIT*	Limit the number of search results, default=500.
-S *START*	Start with result number X, default=0.
-g	Use Google Dorks for Google search.
-p	Use proxies for requests, enter proxies in proxies.yaml.
-s	Use Shodan to query discovered hosts.
--screenshot *SCREENSHOT*	Take screenshots of resolved domains specify output directory: --screenshot output_directory
-v	Verify host name via DNS resolution and search for virtual hosts.
-e	DNS server to use for lookup.
-t *DNS_TLD*	Perform a DNS TLD expansion discovery, default False.
-r	Check for takeovers.
-n	Enable DNS server lookup, default False.
-c	Perform a DNS brute force on the domain.
-f *FILENAME*	Save the results to an XML and JSON file.
-b *SOURCE*	anubis, baidu, bing, binaryedge, bingapi, bufferoverun, censys, certspotter, crtsh, dnsdumpster, duckduckgo, github-code, google, hackertarget, hunter, intelx, linkedin, linkedin_links, netcraft, omnisint, otx, pentesttools, projectdiscovery, qwant, rapiddns, rocketreach, securityTrails, spyse, sublist3r, threatcrowd, threatminer, trello, twitter, urlscan, virustotal, yahoo, zoomeye, all

Arguments to further control your output, italics are user entered.

Examples:

theHarvester -d microsoft.com -l 500 -b google -f myresults.html

theHarvester -d microsoft.com -b pgp, virustotal

theHarvester -d microsoft -l 200 -b linkedin

theHarvester -d microsoft.com -l 200 -g -b google

theHarvester -d apple.com -b googleCSE -l 500 -s 300

theHarvester -d cornell.edu -l 100 -b bing

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com