

Usage

theHarvester Usage. [] Specifies [-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s] [--screenshot SCREEN SHOT] [-v] [-e DNS_SERVER] [-t Optional Switch. DNS_TLD] [-r] [-n] [-c] [-f FILENAME] [-b SOURCE]

Options

DESCRIPTION	SWITCH	EXAMPLES IN THIS COLUMN
Show the Help Menu.	-h, --help	theHarvester -h
Specify the Company Name or Domain Name to be Searched.	-d DOMAIN, --domain DOMAIN	theHarvester -d microsoft.com
Limit the Number of Search Results for the Domain. The default is 500.	-l LIMIT, --limit LIMIT	theHarvester -l 200
Specify the Number to Start at for Results. Default is 0.	-S START, --start START	theHarvester --start 5
Specify the Use of Google Dorks if Using Google Search.	-g, --google-dork	theHarvester -g
Specify the Use of Proxies for the Requests. Enter these in the proxies.yaml File.	-p, --proxies	theHarvester --proxies
Specify the Use of Shodan to Query Hosts that are Discovered.	-s, --shodan	theHarvester -s
Capture Screenshots of Resolved Domains, and Send to Output Directory.	--screenshot OUTPUT_DIRECTORY	theHarvester --screenshot DOMAINS
Verify host name using DNS Resolution, and search for Virtual Hosts.	-v, --virtual-host	theHarvester -v
Specify DNS Server to Use for Lookup.	-e DNS_SERVER, --dns-server DNS_SERVER	theHarvester -e 8.8.8.8
Perform a DNS TLD expansion Discovery. Default Value is False.	-t DNS_TLD, --dns-tld DNS_TLD	theHarvester -t .org
Check for Takeovers.	-r, --take-over	theHarvester --take-over
Enable DNS Server Lookup. Default Value is False.	-n, --dns-lookup	theHarvester -n
Perform a DNS Brute Force on the Domain.	-c, --dns-brute	theHarvester -c
Specify a File to Save Results.	-f FILENAME, --filename FILENAME	theHarvester -f Results.html
Specify Data Source for Search. API Key May be Required.	-b SOURCE, --source SOURCE	theHarvester -b bing



By **samossecurity**

cheatography.com/samossecurity/

Published 8th May, 2023.

Last updated 8th May, 2023.

Page 1 of 2.

Sponsored by **ApolloPad.com**

Everyone has a novel in them. Finish Yours!

<https://apollopad.com>

Possible Data Sources

anubis, baidu, bing, binaryedge, bingapi, bufferoverun, censys, certspotter, crtsh, dnsdumpster, duckduckgo, fullhunt, github-code, google, hackertarget, hunter, intelx, linkedin, linkedin_links, n45ht, omnisint, otx, pentesttools, projectdiscovery, qwant, rapiddns, rocketreach, securityT-rails, spyse, sublist3r, threatcrowd, threatminer, trello, twitter, urlscan, virustotal, yahoo, zoomeye



By **samossecurty**

cheatography.com/samossecurty/

Published 8th May, 2023.

Last updated 8th May, 2023.

Page 2 of 2.

Sponsored by **ApolloPad.com**

Everyone has a novel in them. Finish

Yours!

<https://apollopad.com>