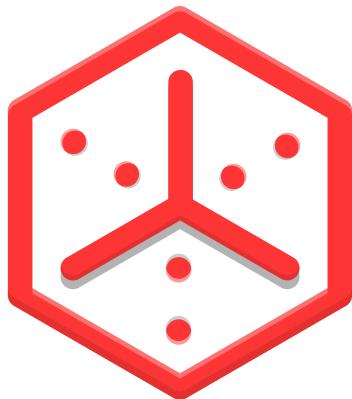


Theharvester



version: 4.8.2 arch: all

[Theharvester Homepage](#) | [Package Tracker](#) | [Source Code Repository](#)
[Edit This Page](#)

Metapackages

default everything large

Tools:

information-g... vulnerability

Tool Documentation

Packages & Binaries

[theharvester](#)

restfulHarvest

theHarvester

theharvester

Learn more with OffSec

[Pen-200](#)

[Sec-100](#)

Tool Documentation:

theharvester Usage Example

Search from email addresses from a domain (`-d kali.org`), limiting the results to 500 (`-l 500`), using DuckDuckGo (`-b duckduckgo`):

Packages and Binaries:

theharvester

The package contains a tool for gathering subdomain names, e-mail addresses, virtual hosts, open ports/ banners, and employee names from different public sources (search engines, pgp key servers).

Installed size: 1.94 MB

How to install: sudo apt install theharvester

Dependencies:

kali-defaults	python3
python3-aiodns	python3-aiofiles
python3-aiohttp	python3-aiomultiprocess
python3-aiosqlite	python3-bs4
python3-censys	python3-certifi
python3-dateutil	python3-dnspython
python3-fastapi	python3-lxml
python3-netaddr	python3-playwright
python3-requests	python3-retrying
python3-shodan	python3-slowapi
python3-starlette	python3-ujson
python3-unicorn	python3-uvloop
python3-yaml	

restfulHarvest

```
root@kali:~# restfulHarvest -h
usage: restfulHarvest [-h] [-H HOST] [-p PORT] [-l LOG_LEVEL] [-r]
```

options:

-h, --help	show this help message and exit
-H, --host HOST	IP address to listen on default is 127.0.0.1
-p, --port PORT	Port to bind the web server to, default is 5000
-l, --log-level LOG_LEVEL	Set logging level, default is info but [critical error warning info debug trace] can be

-r, --reload Enable automatic reload used during development
api

theHarvester

theHarvester is used to gather open source intelligence (OSINT) on a company or domain.

options:

```
-h, --help                  show this help message and exit
-d, --domain DOMAIN        Company name or domain to search.
-l, --limit LIMIT          Limit the number of search results, default=500
-S, --start START          Start with result number X, default=0.
-p, --proxies               Use proxies for requests, enter proxies in
                            proxies.yaml.
-s, --shodan                Use Shodan to query discovered hosts.
--screenshot SCREENSHOT    Take screenshots of resolved domains specify output
                            directory: --screenshot output_directory
-v, --virtual-host          Verify host name via DNS resolution and search
                            virtual hosts.
-e, --dns-server DNS_SERVER DNS server to use for lookup.
-t, --take-over              Check for takeovers.
-r, --dns-resolve [DNS RESOLVE]
```

```
root@kali:~# theharvester -h
(Message from Kali developers)

The command theharvester is deprecated. Please use theHarvester instead
```

Learn more with

Want to learn more about theharvester? get access to in-depth training and hands-on labs:

[PEN-200: 12.1.1. Client-side Attacks: Information Gathering](#)

[MITRE ATT&CK - Resource Development \(TA0042\): 2.1.2. Client-side Attacks: Client Fingerprinting](#)

[SEC-100: 19.1.2. Information Gathering and Enumeration: Client Fingerprinting](#)



PEN-200 course



SEC-100 course

Updated on: 2025-Aug-26

[Edit this page](#)

tetragon

tightvnc

LIGHT

DARK

Links

Home
Download / Get Kali
Blog
OS Documentation
Tool Documentation
System Status
Archived Releases
Partnerships

Platforms

ARM (SBC)
NetHunter (Mobile)
Amazon AWS
Docker

Linode

Microsoft Azure

Microsoft Store (WSL)

Vagrant

Development

Bug Tracker
Continuous Integration

Community

Discord
Support Forum

[Network Mirror](#)

[Package Tracker](#)

[GitLab](#)

Follow Us

[Bluesky](#)

[Facebook](#)

[Instagram](#)

[Mastodon](#)

[Substack](#)

[X](#)

[Newsletter](#)

[RSS](#)

[PeerTube](#)

Policies

[Cookie Policy](#)

[Privacy Policy](#)

[Trademark Policy](#)

© OffSec Services Limited 2025. All rights reserved.

OffSecTM

Kali Linux is part of OffSec's Community Projects
Learn more about OffSec's free, open-source
penetration testing tools for cybersecurity
professionals