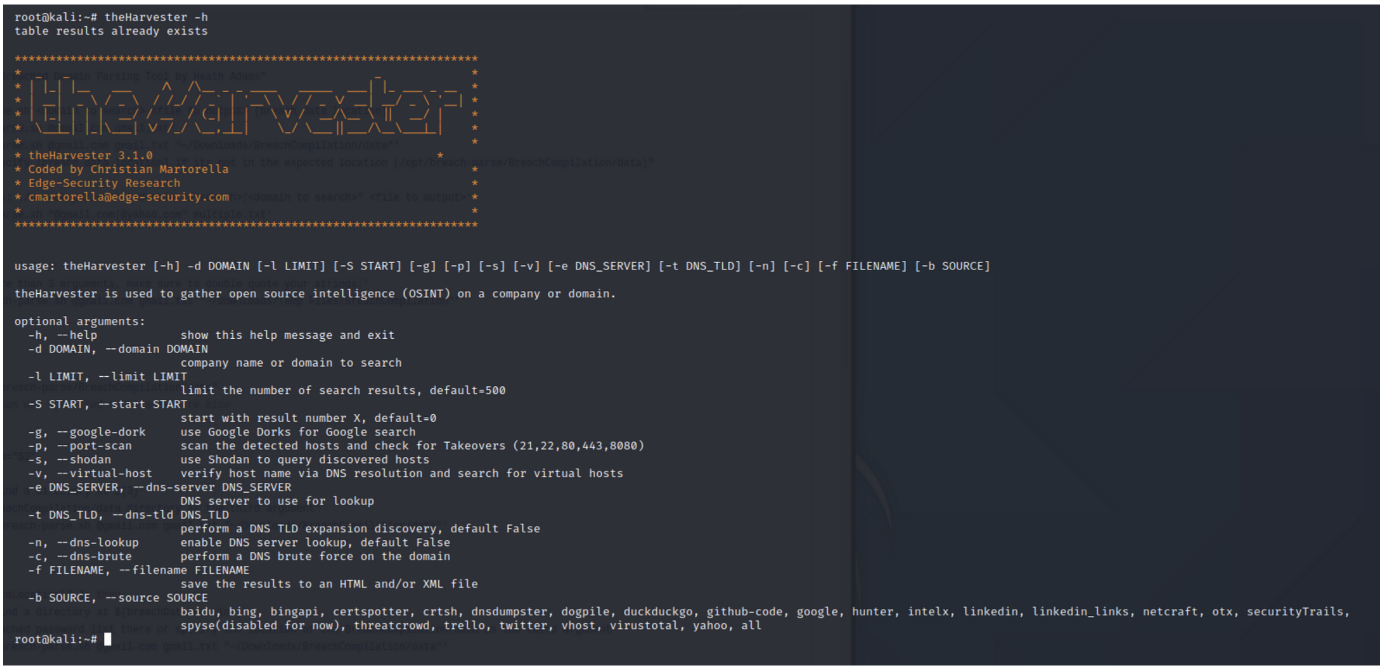
Utilizing theHarvester

---

theHarvester

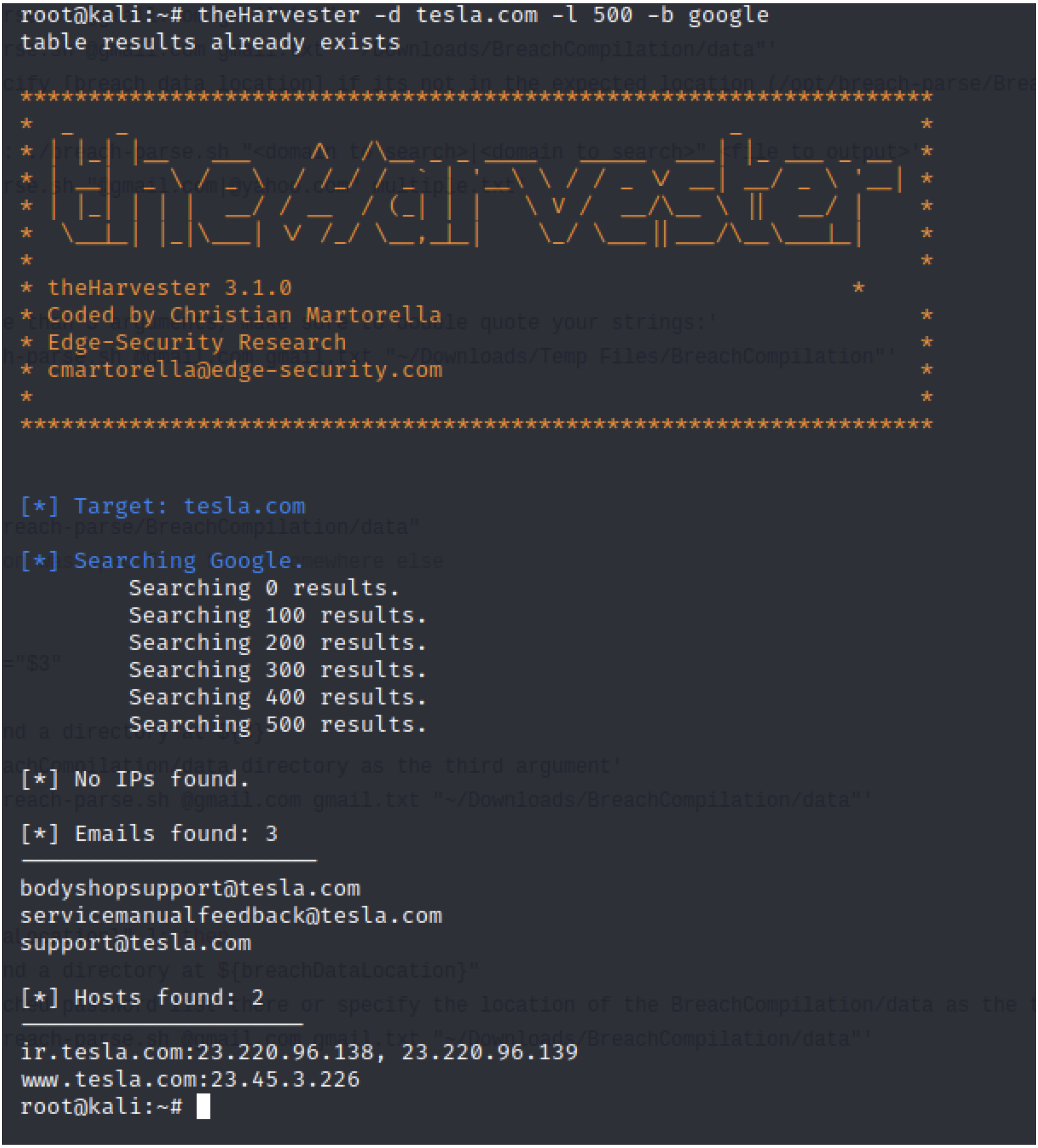
This tool is similar to `breach-parser`. However, it has more data sources which can be enabled and used with the appropriate API keys.

The following are examples of how `theHarvester` works:



```
root@kali:~# theHarvester -h
table results already exists

*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 3.1.0                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s] [-v] [-e DNS_SERVER] [-t DNS_TLD] [-n] [-c] [-f FILENAME] [-b SOURCE]

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

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        company name or domain to search
  -l LIMIT, --limit LIMIT
                        limit the number of search results, default=500
  -S START, --start START
                        start with result number X, default=0
  -g, --google-dork     use Google Dorks for Google search
  -p, --port-scan       scan the detected hosts and check for Takeovers (21,22,80,443,8080)
  -s, --shodan          use Shodan to query discovered hosts
  -v, --virtual-host    verify host name via DNS resolution and search for virtual hosts
  -e DNS_SERVER, --dns-server DNS_SERVER
                        DNS server to use for lookup
  -t DNS_TLD, --dns-tld DNS_TLD
                        perform a DNS TLD expansion discovery, default False
  -n, --dns-lookup      enable DNS server lookup, default False
  -c, --dns-brute       perform a DNS brute force on the domain
  -f FILENAME, --filename FILENAME
                        save the results to an HTML and/or XML file
  -b SOURCE, --source SOURCE
                        baidu, bing, bingapi, certspotter, crtsh, dnsdumpster, dogpile, duckduckgo, github-code, google, hunter, intelx, linkedin, linkedin_links, netcraft, otx, securityTrails,
                        spyse(disabled for now), threatcrowd, trello, twitter, vhost, virustotal, yahoo, all
root@kali:~# 
```

The above image shows the "help" option that gives you instructions on how to use the tool.



```
root@kali:~# theHarvester -d tesla.com -l 500 -b google
table results already exists
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 3.1.0                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: tesla.com

[*] Searching Google.
        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
        Searching 300 results.
        Searching 400 results.
        Searching 500 results.

[*] No IPs found.

[*] Emails found: 3
----------------------
bodyshopsupport@tesla.com
servicemanualfeedback@tesla.com
support@tesla.com

[*] Hosts found: 2
---------------------
ir.tesla.com:23.220.96.138, 23.220.96.139
www.tesla.com:23.45.3.226
root@kali:~# 
```

The above image shows a sample test of the `tesla.com` domain using `google` as the data source.