Table of Contents

Sudomy - Subdomain Enumeration & Analysis – Guide 1.0

Introduction

Sudomy is a subdomain enumeration tool, created using a bash script, to analyze domains and collect subdomains in fast and comprehensive way.

How Sudomy Works

Sudomy is using cURL library in order to get the HTTP Response Body from third-party sites to then execute the regular expression to get subdomains. This process fully leverages multi processors, more subdomains will be collected with less time consumption.

The passive technique uses third party resources such as DNSdumpster, WebArchive, Shodan, Total Virus, Certsh, BinaryEdge, SecurityTrails, Certspotter, Censys, Threatminer, Bufferover, Hackertarget, Entrust, ThereatCrowd, and Riddler. To improve the enumeration results sudomy application needs to add an API Key for Shodan, Censys, Total Virus, BinaryEdge, and SecurityTrails in the sudomy.API section. Whereas Active technique uses a combination of the Gobuster application with the wordlist provided by SecLists. SecLists has a collection of approximately three million wordlists.

Features

For recent time, Sudomy has these 12 features:

- Easy, light, fast and powerful. Bash script is available by default in almost all Linux distributions. By using bash script multiprocessing feature, all processors will be utilized optimally.
- Subdomain enumeration process can be achieved by using **active** method or **passive** method
  - **Active Method**
    - *Sudomy* utilize Gobuster tools because of its highspeed performance in carrying out DNS Subdomain Bruteforce attack (wildcard support). The wordlist that is used comes from combined SecList (Discover/DNS) lists which contains around 3 million entries
  - **Passive Method**
    - By **selecting** the **good** third-party sites, the enumeration process can be **optimized**. More results will be obtained with less time required. *Sudomy* can collect data from these well-curated 18 third-party sites:

```
https://dnsdumpster.com
https://web.archive.org
https://shodan.io
https://virustotal.com
https://crt.sh
https://www.binaryedge.io
https://securitytrails.com
https://sslmate.com/certspotter
https://censys.io
https://threatminer.org
http://dns.bufferover.run
https://hackertarget.com
https://www.entrust.com/ct-search/
https://www.threatcrowd.org
https://riddler.io
https://findsubdomains.com
https://rapiddns.io/
https://https://otx.alienvault.com/
```

- Test the list of collected subdomains and probe for working http or https servers. This feature uses a third-party tool, httprobe.
- Subdomain availability test based on Ping Sweep and/or by getting HTTP status code.
- The ability to detect virtualhost (several subdomains which resolve to single IP Address). Sudomy will resolve the collected subdomains to IP addresses, then classify them if several subdomains resolve to single IP address. This feature will be very useful for the next penetration testing/bug bounty process. For instance, in port scanning, single IP address won't be scanned repeatedly
- Performed port scanning from collected subdomains/virtualhosts IP Addresses
- Testing Subdomain TakeOver attack
- Taking Screenshotsof subdomains
- Identify technologies on websites
- Data Collecting/Scraping open port from 3rd party (Default::Shodan), For right now just using Shodan [Future::Censys,Zoomeye]. More efficient and effective to collecting port from list ip on target [[Subdomain > IP Resolver > Crawling > ASN & Open Port]]
- Collecting & Extract URL Parameter
  Report output in HTML or CSV format

Publication

- Sudomy: Information Gathering Tools for Subdomain Enumeration and Analysis - IOP Conference Series: Materials Science and Engineering, Volume 771, 2nd International Conference on Engineering and Applied Sciences (2nd InCEAS) 16 November 2019, Yogyakarta, Indonesia

Comparison

The following are the results of passive enumeration DNS testing of *Sublist3r, Subfinder*, and *Sudomy*. The domain that is used in this comparison is ***bugcrowd.com***.

https://github.com/Screetsec/Sudomy

Testing is done by comparing the sudomy application with other applications such as subfinder and sublist3r with the target domain bugcrowd.com.

bugcrowd.com Comparation

Tools	Time	Resources (Source)	Results (Subdomain)
subfinder	1m 38.621s	25	25
sublist3r	0m 27.216s	11	23
sudomy	0m 6.946s	16	49

https://iopscience.iop.org/article/10.1088/1757-899X/771/1/012019/meta

The sub finder application uses 25 resources, sublist3r uses 11 resources, and sudomy uses 16 resources. The time needed to search for a subdomain from bugcrowd.com, the sub finder application takes 1 minute 38,621s, sublist3r takes 0 minutes 27,216s, and sudomy takes 0 minutes 6,946s. The subdomain results from bugcrowd.com found by the sub finder application are 25 subdomains, sublist3r are 23 subdomains, and sudomy is 49 subdomains. The results of enumeration looking for the bugcrowd.com subdomain using the sub finder, sublist3r, and sudomy applications can be seen in table 3. To further speed up the enumeration process and save CPU, RAM, and bandwidth, you can use third party resources as needed.

Installation

Sudomy is currently extended with the following tools. Instructions on how to install & use the application are linked below.

Tools	License	Info
Gobuster	Apache License 2.0	not mandatory
httprobe	Tom Hudson -	mandatory
nmap	GNU General Public License v2.0	not mandatory

Download Sudomy From Github

```
# Clone this repository
git clone --recursive https://github.com/screetsec/Sudomy.git
```

Install Dependencies

```
$ pip install -r requirements.txt
```

Sudomy requires jq to run and parse. Information on how to download and install jq can be accessed here

Linux Installation

```
# Linux
apt-get update
```

```
apt-get install jq nmap phantomjs golang npm
npm i -g wappalyzer
```

Mac Installation

```
# Mac
brew cask install phantomjs
brew install jq nmap go npm
npm i -g wappalyzer
```

If you already have a Go environment, then follow this instruction:

Add the following lines to ~/.bashrc (Of your user)

```
nano ~/.bashrc
export GOPATH=$HOME/go
export PATH=$PATH:$GOROOT/bin:$GOPATH/bin
source ~/.bashrc
```

Then Install the dependencies

```
go get -u github.com/tomnomnom/httprobe
go get -u github.com/OJ/gobuster
```

Post Installation

API Key is needed before querying on third-party sites, such as `Shodan, Censys, SecurityTrails, Virustotal,` and `BinaryEdge .`

- The API key setting can be done in sudomy.api file.

https://github.com/Screetsec/Sudomy

```
# Shodan
# URL :  http://developer.shodan.io
# Example :
#- SHODAN_API="VGhpc1M0bXBsZWwKVGhmcGxlbAo"

SHODAN_API=""

# Censys
# URL : https://censys.io/register

CENSYS_API=""
CENSYS_SECRET=""

# Virustotal
# URL : https://www.virustotal.com/gui/
VIRUSTOTAL=""


# Binaryedge
# URL : https://app.binaryedge.io/login
BINARYEDGE=""


# SecurityTrails
# URL : https://securitytrails.com/
SECURITY_TRAILS=""
```

Testing Application

```
sudomy -d hackerone.com
```

Running in Docker

Docker Container Sudomy v1.1.2

Pull an image from DockerHub

```
docker pull screetsec/sudomy:v1.1.2

```

Run an image, you can run the image on custom directory but you must copy/download config sudomy.api on current directory

```
docker run -v "${PWD}/output:/usr/lib/sudomy/output" -v "${PWD}/sudomy.api:/
```

or define variable when execute

```
docker run -v "${PWD}/output:/usr/lib/sudomy/output" -e "SHODAN_API=xxxx" -e
```

Detail Features

For recent time, Sudomy has these 12 features:

- Easy, light, fast and powerful. Bash script is available by default in almost all Linux distributions. By using bash script multiprocessing feature, all processors will be utilized optimally.
- Subdomain enumeration process can be achieved by using **active** method or **passive** method
  - **Active Method**
    - *Sudomy* utilize Gobuster tools because of its highspeed performance in carrying out DNS Subdomain Bruteforce attack (wildcard support). The wordlist that is used comes from combined SecList (Discover/DNS) lists which contains around 3 million entries
  - **Passive Method**
    - By **selecting** the **good** third-party sites, the enumeration process can be **optimized**. More results will be obtained with less time required. *Sudomy* can collect data from these well-curated 18 third-party sites:

```
https://dnsdumpster.com
https://web.archive.org
https://shodan.io
https://virustotal.com
https://crt.sh
https://www.binaryedge.io
https://securitytrails.com
https://sslmate.com/certspotter
https://censys.io
https://threatminer.org
http://dns.bufferover.run
https://hackertarget.com
https://www.entrust.com/ct-search/
https://www.threatcrowd.org
https://riddler.io
https://findsubdomains.com
https://rapiddns.io/
https://https://otx.alienvault.com/
```

- Test the list of collected subdomains and probe for working http or https servers. This feature uses a third-party tool, httprobe.
- Subdomain availability test based on Ping Sweep and/or by getting HTTP status
- code. The ability to detect virtualhost (several subdomains which resolve to single IP Address). Sudomy will resolve the collected subdomains to IP addresses, then classify them if several subdomains resolve to single IP address. This feature will be very useful for the next penetration testing/bug bounty process. For instance, in port scanning, single IP address won't be scanned repeatedly
- Performed port scanning from collected subdomains/virtualhosts IP Addresses
- Testing Subdomain TakeOver attack
- Taking Screenshotsof subdomains
- Identify technologies on websites
- Data Collecting/Scraping open port from 3rd party (Default::Shodan), For right now just using Shodan [Future::Censys,Zoomeye]. More efficient and effective to collecting port from list ip on target [[Subdomain > IP Resolver > Crawling > ASN & Open Port]]
- Collecting & Extract URL Parameter
- Report output in HTML or CSV format

https://github.com/Screetsec/Sudomy

How to use Engine/Resource

To use all 20 Sources and Probe for working http or https servers:

```
$ sudomy -d bugcrowd
```

If one of the engines give sign [x] , it's mean the engine is inactive. Remember to setup post installation and check the API Key, maybe your API Key limite or missing

To use one or more source:

```
sudomy -d bugcrowd.com -s alienvault,dnsdumpster
```

https://github.com/Screetsec/Sudomy

https://github.com/Screetsec/Sudomy

How to use Plugin

To use one or more plugins:

```
sudomy -d hackerone.com -pS -sC -tO
```

To use all plugins:

You can **run** all plugins by entering commands

```
sudomy -d bugcrowd.com --all
```

In this case, plugin for Nmap, Gobuster and wappalyzer is not Included. So you can add more arguments for that plugin, example

```
sudomy -d bugcrowd.com –all -eP
```

https://github.com/Screetsec/Sudomy

Extract & Collecting Path, Parameter & Endpoint

Collecting Juicy URL & Scraping URL Parameter from Passive scan. Default Source Using Web Archive, CommonCrawl, UrlScan.

- Regex using DFA Engine (awk,sed)-
- Support and Collecting URL with multi Parameter to Fuzzing-
- Removing Duplicate Parameter

```
[+] Collecting URL Parameter from Engine
-----------------------------------------

    Total Juicy URL                 [12479]
    Total Full Parameter            [982]
    Total Uniq Parameter            [487]

[+] Sudomy has been sucessfully completed
-----------------------------------------
```

There will be 3 files in output:

```
-rw-r--r-- 1 root root 830651 May  9 14:25 Passive_Collecting_JuicyURL.txt
-rw-r--r-- 1 root root 114902 May  9 14:25 Passive_Collecting_URLParamter_Full.txt
-rw-r--r-- 1 root root  72325 May  9 14:25 Passive_Collecting_URLParamter_Uniq.txt
```

Passive_Collecting_URLParamter_Full.txt : This File is original collecting URL Parameter without Parsing (Original URL & Parameter Value)

```
https://bugcrowd.com/?rel=startups-list.com
https://www.bugcrowd.com/?rel=startups-list.com
https://www.bugcrowd.com/?utm_source=paid_advertising&utm_medium=website&utm_content=podcast&utm_campaign=cyberwire
https://bugcrowd.com/crowdstream?page=2
https://bugcrowd.com/crowdstream?page=3
https://www.bugcrowd.com/privacy?utm_source=https://integrations.complianceboard.io&utm_campaign=integrations&utm_content=bugcrowd&utm_medium=
https://www.bugcrowd.com/privacy/?utm_source=https://integrations.complianceboard.io&utm_campaign=integrations&utm_content=bugcrowd&utm_medium=
https://bugcrowd.com/programs?hidden%5B%5D=false&pending_invite%5B%5D=true&sort%5B%5D=promoted-desc
https://bugcrowd.com/programs?sort%5B%5D=promoted-desc&search%5B%5D=walmart
https://bugcrowd.com/socrata?utm_source=the-list&utm_medium=list-link&utm_campaign=socrata
https://www.bugcrowd.com/terms-and-conditions?utm_source=https://integrations.complianceboard.io&utm_campaign=integrations&utm_content=bugcrowd&utm_medium=
https://www.bugcrowd.com/terms-and-conditions/?utm_source=https://integrations.complianceboard.io&utm_campaign=integrations&utm_content=bugcrowd&utm_medium=
https://bugcrowd.com/twilio?utm_source=redirect&utm_medium=bounty&utm_term=c018
https://bugcrowd.com/user/sign_up?__hstc=153879591.0e7e5e7d8ada6c3c080dbc2819cc9702.1516752290422.1516752290422.1516752290422.1&__hssc=153879591.1.1516752290423&__hsfp=1995992257
https://bugcrowd.com/westernunion?utm_source=redirect&utm_medium=bounty&utm_term=c006
https://docs.bugcrowd.com/changelog/?page=2
https://docs.bugcrowd.com/changelog/?page=3
https://docs.bugcrowd.com/changelog/?page=4
https://docs.bugcrowd.com/changelog/?page=5
https://docs.bugcrowd.com/changelog/?page=6
https://events.bugcrowd.com/cyberinnovationwinedown?calendar-iCal&u=53174a7e636c77d3
https://forum.bugcrowd.com/?__hstc=153879591.0e7e5e7d8ada6c3c080dbc2819cc9702.1516752290422.1516752290422.1516752290422.1&__hssc=153879591.1.1516752290423&__hsfp=1995992257
https://forum.bugcrowd.com/c/ask-a-hacker/34?page=1
```

Passive_Collecting_URLParamter_Uniq.txt : This File is original collecting URL Parameter with Unique URL for Fuzzing

```
https://bugcrowd.com/purevpn?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/?ref=FUZZ
https://bugcrowd.com/?rel=FUZZ
https://bugcrowd.com/resources?utm_campaign=FUZZ&Bugcrowd%20Resources%20Web%20Page=FUZZ&utm_medium=FUZZ&CTA=FUZZ&utm_source=FUZZ
https://bugcrowd.com/riskio?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/sendsafely?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/sendsafely?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ&%22onmouseover=FUZZ
https://bugcrowd.com/servicerocket?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/silentcircle?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/socrata?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/sophos?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/splashid?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/sproutsocial?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/statuspage?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/sunrise?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/tagged?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/twilio?utm_campaign=FUZZ&Twitter%20Link%20Sharing=FUZZ&utm_content=FUZZ&21550266=FUZZ&utm_medium=FUZZ&social=FUZZ&utm_source=FUZZ
https://bugcrowd.com/twilio?utm_source=FUZZ&redirect=FUZZ&utm_medium=FUZZ&bounty=FUZZ&utm_term=FUZZ
https://bugcrowd.com/twilio?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/user/sign_up?__hstc=FUZZ&153879591.0e7e5e7d8ada6c3c080dbc2819cc9702.1516752290422.1516752290422.1516752290422.1=FUZZ&__hssc=FUZZ&153879591.1.1516752290423=FU
ZZ&__hsfp=FUZZ
https://bugcrowd.com/volusion?utm_source=FUZZ&the-list=FUZZ&utm_medium=FUZZ&list-link=FUZZ&utm_campaign=FUZZ
https://bugcrowd.com/vulnerability-rating-taxonomy?search=FUZZ
https://bugcrowd.com/westernunion?utm_source=FUZZ&redirect=FUZZ&utm_medium=FUZZ&bounty=FUZZ&utm_term=FUZZ
```

Passive_Collecting_JuicyURL.txt: This is a huge list of urls associated with the domain. Here we can get and extract relative paths, endpoint, url and interest strings.

https://github.com/Screetsec/Sudomy

```
cat Passive_Collecting_JuicyURL.txt | grep --colour=always -e "\.js"
```

Like filtering the javascript for found a sensitive data from JS Files

```
https://forum.bugcrowd.com/assets/virtual-hyperscript/index.js
https://forum.bugcrowd.com/assets/vnode/vnode.js
https://forum.bugcrowd.com/assets/vnode/vtext.js
https://forum.bugcrowd.com/assets/vtree/diff.js
https://forum.bugcrowd.com/highlight-js/forum.bugcrowd.com/133b1767dbeecf92cad6dfc38d42cde22195db05.js
https://forum.bugcrowd.com/javascripts/jquery.magnific-popup-min.js
https://forum.bugcrowd.com/javascripts/pikaday.js
https://forum.bugcrowd.com/manifest.json
https://forum.bugcrowd.com/service-worker.js
https://forum.bugcrowd.com/vnode/handle-thunk.js
https://forum.bugcrowd.com/vnode/is-vhook.js
https://forum.bugcrowd.com/vnode/is-vnode.js
https://forum.bugcrowd.com/vnode/is-vtext.js
https://forum.bugcrowd.com/vnode/is-widget.js
https://forum.bugcrowd.com/vnode/vnode.js
https://forum.bugcrowd.com/vnode/vpatch.js
https://forum.bugcrowd.com/vnode/vtext.js
https://pages.bugcrowd.com/hs-fs/hub/1549768/hub_generated/style_manager/1444893419764/custom/page/Bugcrowd-Oct2015-theme/Bugcrowd-Oct2015-main.min.js
https://pages.bugcrowd.com/js/forms2/js/forms2.min.js
https://pages.bugcrowd.com/js/LpSocialRenderer.js
https://portal.bugcrowd.com/assets/application-416aaa0cb1ef6df17195a78ec95e434a.js
https://researcherdocs.bugcrowd.com/js/bundle-hub.js?1457745572785
https://researcherdocs.bugcrowd.com/js/bundle-hub.js?1458349958067
http://status.bugcrowd.com/tweets.js
https://ww2.bugcrowd.com/js/forms2/js/forms2.min.js
https://ww2.bugcrowd.com/js/stripmktto.js
```

cat Passive_Collecting_JuicyURL.txt | grep --colour=always -e "\.pdf"

```
https://bugcrowd.com/sites/55bbaabe2c1cc446360044ef/assets/560af9945918ad9d6702f2dd/WinkCaseStudy.pdf
https://bugcrowd.com/sites/55bbaabe2c1cc446360044ef/assets/560af9e25918ad9d952e6013/Aruba_Private_Bug_Bounty_Story.pdf
https://bugcrowd.com/vulnerability-rating-taxonomy/1.0.pdf
https://bugcrowd.com/vulnerability-rating-taxonomy/1.1.pdf
https://bugcrowd.com/vulnerability-rating-taxonomy/1.2.pdf
https://bugcrowd.com/vulnerability-rating-taxonomy/1.3.pdf
https://bugcrowd.com/vulnerability-rating-taxonomy/1.4.pdf
https://bugcrowd.com/vulnerability-rating-taxonomy/1.5.pdf
https://bugcrowd.com/vulnerability-rating-taxonomy/1.6.pdf
https://bugcrowd.com/vulnerability-rating-taxonomy/1.7.pdf
https://bugcrowd.com/vulnerability-rating-taxonomy/1.8.pdf
https://www.bugcrowd.com/wp-content/plugins/wonderplugin-pdf-embed/pdfjs/web/viewer.html?file=https%3A%2F%2Fwww.bugcrowd.com%2Fwp-content%2Fuploads%2F2018%2F12%2Fbugcrowd_insidet
hemindofahacker_2019.pdf
https://pages.bugcrowd.com/hubfs/2017%20Spring%20Release%20Notes.pdf
https://pages.bugcrowd.com/hubfs/Bugcrowd-2017-State-of-Bug-Bounty-Report.pdf
https://pages.bugcrowd.com/hubfs/PDFs/Bugcrowd-Vulnerability-Rating-Taxonomy.pdf
https://pages.bugcrowd.com/hubfs/PDFs/state-of-bug-bounty-2016.pdf
https://pages.bugcrowd.com/hubfs/PDFs/Twilio-Case-Study.pdf
https://pages.bugcrowd.com/hubfs/Vuln_Data_to_Collect.pdf?t=1471894251601
http://pages.bugcrowd.com/rs/601-RSA-253/images/GuidetoHackerSummerCamp.pdf
http://pages.bugcrowd.com/rs/601-RSA-253/images/MobileAppResourceKit.pdf
https://pages.bugcrowd.com/rs/601-RSA-253/images/state-of-bug-bounty-08-2015.pdf
https://pages.bugcrowd.com/rs/601-RSA-253/images/state-of-bug-bounty-08-2015.pdf?mkt_tok=3RkMMJWWfF9wsRonvKXNZKXonjHpfsX56eUpUa63lMI%2F0ER3fOvrPUfGjI4AS8BjI%2BSLDwEYGJlv6SgFTLDEM
bJz27gPXhI%3D
https://ww2.bugcrowd.com/rs/453-IJC-858/images/bugcrowd_insidethemindofahacker_2019.pdf
```

NOTE : As it fetches the parameters from WebArchive, CommonCrawl, URLscan data , so chances of false positives are high.

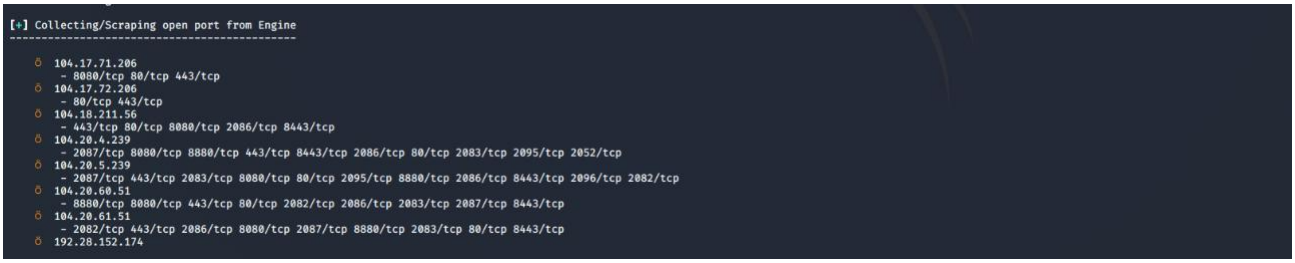
Collecting DB Port & ASN from Engine (Passive)

Data Collecting/Scraping open port from 3rd party (Default::Shodan), For right now just using Shodan [Future::Censys,Zoomeye] . So we do not perfom active scan, who collect the port ? Third-party sites (Shodan,Zoomeye,Censys) doing that and perfom active scan and then, we just collected the port from their result

- More efficient and effective to collecting port from list ip on target [[Subdomain > IP Resolver > Crawling > ASN & Open Port]]
- Here we can further narrow the targeting port for checking in port
- scanning List ASN From IP List [running auto on db_port::ip_dbasn.txt]

Must running with argument -rS | --resolver

```
./sudomy -d bugcrowd.com -rs --db-port
```



Result file :

Here we also get ASN information from all IPs

https://github.com/Screetsec/Sudomy

Resolving: Subdomains & Domains

The ability to detect virtualhost (several subdomains which resolve to single IP Address), for this plugin using argument -rS

```
Sudomy -d bugcrowd.com -rS | --resolver
```

Results :

List IP from all subdomains without duplicates:

```
cat ip_resolver.txt
```

https://github.com/Screetsec/Sudomy

```
104.17.74.206
104.18.210.56
104.20.4.239
104.20.5.239
104.20.60.51
104.20.61.51
192.28.152.174
3.222.95.161
3.230.87.225
34.194.216.57
34.198.111.148
52.44.177.143
52.5.214.175
52.6.24.219
54.84.134.174
```

Sudomy will resolve the collected subdomains to IP addresses, then classify them if several subdomains resolve to single IP address

```
cat pars_subdomain_resolver.txt
```

```
104.18.210.56
 - docs.bugcrowd.com
 - researcherdocs.bugcrowd.com
54.84.134.174
 - events.bugcrowd.com
104.20.5.239
 - blog.bugcrowd.com
 - www.bugcrowd.com
52.5.214.175
 - stargate.a.bugcrowd.com
52.6.24.219
 - tableau.a.bugcrowd.com
3.230.87.225
 - production-sandbox.a.bugcrowd.com
104.20.4.239
 - bugcrowd.com
 - tracker.bugcrowd.com
104.20.61.51
 - api.bugcrowd.com
 - assetinventory.bugcrowd.com
 - concourse.bugcrowd.com
 - email.crowdcontrol.bugcrowd.com
 - email.submit.bugcrowd.com
 - hooks.bugcrowd.com
52.44.177.143
 - gemstash-mattress.a.bugcrowd.com
192.28.152.174
 - bounce.bugcrowd.com
66.220.12.139
 - forum.bugcrowd.com
3.222.95.161
 - proxilate.a.bugcrowd.com
 - proxilate.bugcrowd.com
34.194.216.57
 - collateral.bugcrowd.com
104.17.74.206
 - go.bugcrowd.com
 - ww2.bugcrowd.com
34.198.111.148
 - tracker.production-sandbox.a.bugcrowd.com
104.20.60.51
 - email.assetinventory.bugcrowd.com
 - email.bugcrowd.com
 - email.bugs.bugcrowd.com
 - email.forum.bugcrowd.com
 - gslink.bugcrowd.com
 - pages.bugcrowd.com
```

https://github.com/Screetsec/Sudomy

Web Screenshots from Domain List

Screenshots a list of website, arguments :

```
Sudomy -d bugcrowd.com -sS | --screenshot
```

```
[+] Web Screenshots: from domain list
---------------------------------------------

[+] 45 URLs to be screenshot

[ERROR][http://email.assetinventory.bugcrowd.com:80] Shell command PID 27074 returned an abnormal error code: '1'
[ERROR][http://email.assetinventory.bugcrowd.com:80] Screenshot somehow failed

[ERROR][http://email.bugcrowd.com:80] Shell command PID 27107 returned an abnormal error code: '1'
[ERROR][http://email.bugcrowd.com:80] Screenshot somehow failed

[ERROR][http://email.bugs.bugcrowd.com:80] Shell command PID 27117 returned an abnormal error code: '1'
[ERROR][http://email.bugs.bugcrowd.com:80] Screenshot somehow failed

[ERROR][https://concourse.bugcrowd.com:443] Shell command PID 27154 returned an abnormal error code: '1'
[ERROR][https://concourse.bugcrowd.com:443] Screenshot somehow failed

[ERROR][http://email.crowdcontrol.bugcrowd.com:80] Shell command PID 27205 returned an abnormal error code: '1'
[ERROR][http://email.crowdcontrol.bugcrowd.com:80] Screenshot somehow failed

[ERROR][http://email.forum.bugcrowd.com:80] Shell command PID 27226 returned an abnormal error code: '1'
[ERROR][http://email.forum.bugcrowd.com:80] Screenshot somehow failed

[ERROR][http://email.submit.bugcrowd.com:80] Shell command PID 27234 returned an abnormal error code: '1'
[ERROR][http://email.submit.bugcrowd.com:80] Screenshot somehow failed

[ERROR][https://api.bugcrowd.com:443] Shell command PID 27224 returned an abnormal error code: '1'
[ERROR][https://api.bugcrowd.com:443] Screenshot somehow failed

[ERROR][https://hooks.bugcrowd.com:443] Shell command PID 27426 returned an abnormal error code: '1'
[ERROR][https://hooks.bugcrowd.com:443] Screenshot somehow failed

[ERROR][http://events.bugcrowd.com:80] Screenshot somehow failed

[ERROR][https://events.bugcrowd.com:443] Screenshot somehow failed

[+] 34 actual URLs screenshot
[+] 11 error(s)
    http://email.assetinventory.bugcrowd.com:80
    http://email.bugcrowd.com:80
    http://email.bugs.bugcrowd.com:80
    https://concourse.bugcrowd.com:443
    http://email.crowdcontrol.bugcrowd.com:80
    https://api.bugcrowd.com:443
    http://email.forum.bugcrowd.com:80
    http://email.submit.bugcrowd.com:80
    http://events.bugcrowd.com:80
    https://hooks.bugcrowd.com:443
    https://events.bugcrowd.com:443
```

Resutlts :

The output in screenshots folder :

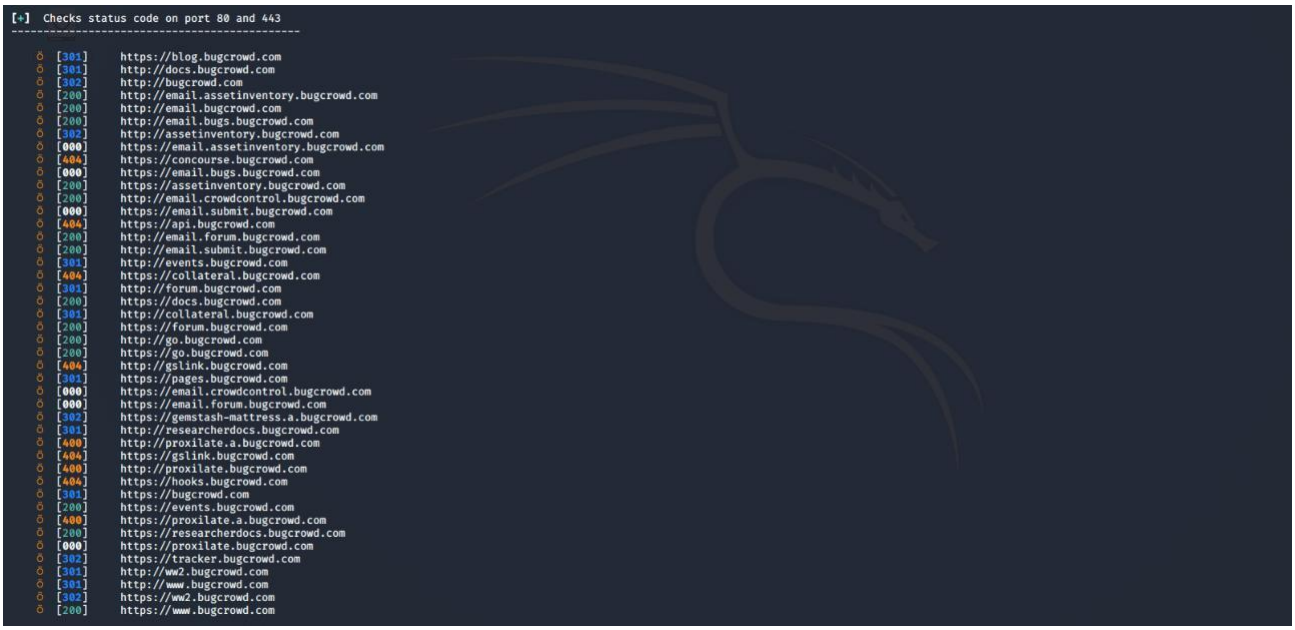
```
http_assetinventory.bugcrowd.com_80.png   http_researcherdocs.bugcrowd.com_80.png   https_email.crowdcontrol.bugcrowd.com_443.png   https_proxilate.bugcrowd.com_443.png
http_bugcrowd.com_80.png                  https_assetinventory.bugcrowd.com_443.png  https_email.forum.bugcrowd.com_443.png          https_researcherdocs.bugcrowd.com_443.png
http_collateral.bugcrowd.com_80.png       https_blog.bugcrowd.com_443.png            https_email.submit.bugcrowd.com_443.png          https_tracker.bugcrowd.com_443.png
http_docs.bugcrowd.com_80.png             https_bugcrowd.com_443.png                 https_forum.bugcrowd.com_443.png                 https_ww2.bugcrowd.com_443.png
http_forum.bugcrowd.com_80.png            https_collateral.bugcrowd.com_443.png      https_gemstash-mattress.a.bugcrowd.com_443.png   https_www.bugcrowd.com_443.png
http_go.bugcrowd.com_80.png               https_docs.bugcrowd.com_443.png            https_go.bugcrowd.com_443.png                    http_ww2.bugcrowd.com_80.png
http_gslink.bugcrowd.com_80.png           https_email.assetinventory.bugcrowd.com_443.png  https_gslink.bugcrowd.com_443.png          http_www.bugcrowd.com_80.png
http_proxilate.a.bugcrowd.com_80.png      https_email.bugcrowd.com_443.png           https_pages.bugcrowd.com_443.png
http_proxilate.bugcrowd.com_80.png        https_email.bugs.bugcrowd.com_443.png      https_proxilate.a.bugcrowd.com_443.png
```

https://github.com/Screetsec/Sudomy

Getting Status Code from Domain List

Get status codes, response from domain list, argument

```
Sudomy -d bugcrowd.com -pS
```



Results :

```
cat HTTP_Status_Code.txt
```

https://github.com/Screetsec/Sudomy

```
https://blog.bugcrowd.com                    301   Redirection:Moved-Permanently
http://docs.bugcrowd.com                     301   Redirection:Moved-Permanently
http://bugcrowd.com                          302   Redirection:Found:Residing
http://email.assetinventory.bugcrowd.com     200   Successful:OK
http://email.bugcrowd.com                    200   Successful:OK
http://email.bugs.bugcrowd.com               200   Successful:OK
http://assetinventory.bugcrowd.com           302   Redirection:Found:Residing
https://email.assetinventory.bugcrowd.com    000   Not-responding
https://concourse.bugcrowd.com               404   ClientError:NotFound
https://email.bugs.bugcrowd.com              000   Not-responding
https://assetinventory.bugcrowd.com          200   Successful:OK
http://email.crowdcontrol.bugcrowd.com       200   Successful:OK
https://email.submit.bugcrowd.com            000   Not-responding
https://api.bugcrowd.com                     404   ClientError:NotFound
http://email.forum.bugcrowd.com              200   Successful:OK
http://email.submit.bugcrowd.com             200   Successful:OK
http://events.bugcrowd.com                   301   Redirection:Moved-Permanently
https://collateral.bugcrowd.com              404   ClientError:NotFound
http://forum.bugcrowd.com                    301   Redirection:Moved-Permanently
https://docs.bugcrowd.com                    200   Successful:OK
http://collateral.bugcrowd.com               301   Redirection:Moved-Permanently
https://forum.bugcrowd.com                   200   Successful:OK
http://go.bugcrowd.com                       200   Successful:OK
https://go.bugcrowd.com                      200   Successful:OK
http://gslink.bugcrowd.com                   404   ClientError:NotFound
https://pages.bugcrowd.com                   301   Redirection:Moved-Permanently
https://email.crowdcontrol.bugcrowd.com      000   Not-responding
https://email.forum.bugcrowd.com             000   Not-responding
https://gemstash-mattress.a.bugcrowd.com     302   Redirection:Found:Residing
http://researcherdocs.bugcrowd.com           301   Redirection:Moved-Permanently
http://proxilate.a.bugcrowd.com              400   ClientError:Bad-Request
https://gslink.bugcrowd.com                  404   ClientError:NotFound
http://proxilate.bugcrowd.com                400   ClientError:Bad-Request
https://hooks.bugcrowd.com                   404   ClientError:NotFound
https://bugcrowd.com                         301   Redirection:Moved-Permanently
https://events.bugcrowd.com                  200   Successful:OK
https://proxilate.a.bugcrowd.com             400   ClientError:Bad-Request
https://researcherdocs.bugcrowd.com          200   Successful:OK
https://proxilate.bugcrowd.com               000   Not-responding
https://tracker.bugcrowd.com                 302   Redirection:Found:Residing
http://ww2.bugcrowd.com                      301   Redirection:Moved-Permanently
http://www.bugcrowd.com                      301   Redirection:Moved-Permanently
https://ww2.bugcrowd.com                     302   Redirection:Found:Residing
https://www.bugcrowd.com                     200   Successful:OK
```

https://github.com/Screetsec/Sudomy

Chek Live Host - Ping Sweep

Check live host using methode Ping Sweep, run with arguments

```
Sudomy -d bugcrowd.com -pS
```

```
[+] Check Live Host: Ping Sweep - ICMP PING
--------------------------------------------

    [DEAD]    a.bugcrowd.com
    [LIVE]    api.bugcrowd.com
    [LIVE]    assetinventory.bugcrowd.com
    [LIVE]    blog.bugcrowd.com
    [LIVE]    bounce.bugcrowd.com
    [LIVE]    bugcrowd.com
    [DEAD]    collateral.bugcrowd.com
    [LIVE]    concourse.bugcrowd.com
    [DEAD]    crowdcontrol.bugcrowd.com
    [LIVE]    docs.bugcrowd.com
    [DEAD]    email.assetinventory.bugcrowd.com
    [LIVE]    email.bugcrowd.com
    [LIVE]    email.bugs.bugcrowd.com
    [LIVE]    email.crowdcontrol.bugcrowd.com
    [LIVE]    email.forum.bugcrowd.com
    [DEAD]    email.submit.bugcrowd.com
    [DEAD]    events.bugcrowd.com
    [LIVE]    forum.bugcrowd.com
    [DEAD]    forum-new.bugcrowd.com
    [DEAD]    gemstash-mattress.a.bugcrowd.com
    [LIVE]    go.bugcrowd.com
    [LIVE]    gslink.bugcrowd.com
    [DEAD]    hello.bugcrowd.com
    [LIVE]    hooks.bugcrowd.com
    [DEAD]    otter.bugcrowd.com
    [LIVE]    pages.bugcrowd.com
    [DEAD]    p.bugcrowd.com
    [DEAD]    portal.bugcrowd.com
    [DEAD]    production-sandbox.a.bugcrowd.com
    [DEAD]    proxilate.a.bugcrowd.com
    [DEAD]    proxilate.bugcrowd.com
    [LIVE]    researcherdocs.bugcrowd.com
    [DEAD]    stargate.a.bugcrowd.com
    [DEAD]    status.bugcrowd.com
    [DEAD]    submissions.bugcrowd.com
    [DEAD]    support.bugcrowd.com
    [DEAD]    swag.bugcrowd.com
    [DEAD]    tableau.a.bugcrowd.com
    [LIVE]    tracker.bugcrowd.com
    [DEAD]    tracker.production-sandbox.a.bugcrowd.com
    [DEAD]    wiki.bugcrowd.com
    [DEAD]    wordpress.bugcrowd.com
    [LIVE]    ww2.bugcrowd.com
    [LIVE]    www.bugcrowd.com
```

Results :

```
a.bugcrowd.com                              DEAD
api.bugcrowd.com                            LIVE
assetinventory.bugcrowd.com                 LIVE
blog.bugcrowd.com                           LIVE
bounce.bugcrowd.com                         LIVE
bugcrowd.com                                LIVE
collateral.bugcrowd.com                     DEAD
concourse.bugcrowd.com                      LIVE
crowdcontrol.bugcrowd.com                   DEAD
docs.bugcrowd.com                           LIVE
email.assetinventory.bugcrowd.com           DEAD
email.bugcrowd.com                          LIVE
email.bugs.bugcrowd.com                     LIVE
email.crowdcontrol.bugcrowd.com             LIVE
email.forum.bugcrowd.com                    LIVE
email.submit.bugcrowd.com                   DEAD
events.bugcrowd.com                         DEAD
forum.bugcrowd.com                          LIVE
forum-new.bugcrowd.com                      DEAD
gemstash-mattress.a.bugcrowd.com            DEAD
go.bugcrowd.com                             LIVE
gslink.bugcrowd.com                         LIVE
hello.bugcrowd.com                          DEAD
hooks.bugcrowd.com                          LIVE
otter.bugcrowd.com                          DEAD
pages.bugcrowd.com                          LIVE
p.bugcrowd.com                              DEAD
portal.bugcrowd.com                         DEAD
production-sandbox.a.bugcrowd.com           DEAD
proxilate.a.bugcrowd.com                    DEAD
proxilate.bugcrowd.com                      DEAD
researcherdocs.bugcrowd.com                 LIVE
stargate.a.bugcrowd.com                     DEAD
status.bugcrowd.com                         DEAD
submissions.bugcrowd.com                    DEAD
support.bugcrowd.com                        DEAD
swag.bugcrowd.com                           DEAD
tableau.a.bugcrowd.com                      DEAD
tracker.bugcrowd.com                        LIVE
tracker.production-sandbox.a.bugcrowd.com   DEAD
wiki.bugcrowd.com                           DEAD
wordpress.bugcrowd.com                      DEAD
ww2.bugcrowd.com                            LIVE
www.bugcrowd.com                            LIVE
www.pages.bugcrowd.com                      DEAD
www.portal.bugcrowd.com                     DEAD
www.submissions.bugcrowd.com                DEAD
```

https://github.com/Screetsec/Sudomy

Recognises Web Technologies

Identify technologies on websites from domain list, like detects content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and many more

```
./sudomy -d bugcrowd.com -aI / --apps-identifier
```

```
https://forum.bugcrowd.com
     - Discourse 2.5.0
     - Ember.js 3.12.2
     - Google Font API
     - Handlebars 4.7.6
     - Moment.js 2.24.0
     - Nginx
     - jQuery 3.4.1
     - jQuery UI 1.12.1
     - Ruby on Rails
     - Ruby

https://api.bugcrowd.com
     - CloudFlare

http://www.bugcrowd.com
     - CloudFlare
     - Google Font API
     - Google Tag Manager
     - New Relic
     - Pantheon
     - Segment
     - Varnish
     - WordPress 5.3.1
     - jQuery 3.4.1
     - jQuery Migrate 3.1.0
     - PHP
     - Nginx
     - MariaDB
     - MySQL

http://go.bugcrowd.com
     - CloudFlare

https://go.bugcrowd.com
     - CloudFlare

https://hooks.bugcrowd.com
     - CloudFlare
```

Results in CSV Formats :

```
root@kali:~/Enumeration/Subdomain/version/Sudomy-1.1.5#dev/output/05-07-2020/bugcrowd.com# cat wappalyzer.txt
http://docs.bugcrowd.com;Algolia 3.35.1, AngularJS 1.3.20, Chart.js, CloudFlare, CodeMirror 5.48.2, Google Analytics, Intercom, Lodash 2.4.2, Marked, Segment, jQuery 2.1.4, jQuery-pjax, jQuery UI 1
.1
https://docs.bugcrowd.com;Algolia 3.35.1, AngularJS 1.3.20, Chart.js, CloudFlare, CodeMirror 5.48.2, Google Analytics, Intercom, Lodash 2.4.2, Marked, Segment, jQuery 2.1.4, jQuery-pjax, jQuery UI
2.1
http://email.bugcrowd.com;CloudFlare
http://assetinventory.bugcrowd.com;Babel, CloudFlare, Google Analytics, Google Tag Manager, Moment.js 2.18.1, jQuery 3.3.1
https://email.bugcrowd.com;CloudFlare
http://forum.bugcrowd.com;Discourse 2.5.0, Google Analytics, Google Font API, Nginx, Ruby on Rails, Ruby
http://events.bugcrowd.com;Nginx
http://researcherdocs.bugcrowd.com;Algolia 3.35.1, AngularJS 1.3.20, Chart.js, CloudFlare, CodeMirror 5.48.2, Google Analytics, Lodash 2.4.2, Marked, jQuery 2.1.4, jQuery-pjax, jQuery UI 1.12.1
https://researcherdocs.bugcrowd.com;Algolia 3.35.1, AngularJS 1.3.20, Chart.js, CloudFlare, CodeMirror 5.48.2, Google Analytics, Lodash 2.4.2, Marked, jQuery 2.1.4, jQuery-pjax, jQuery UI 1.12.1
https://pages.bugcrowd.com;CloudFlare, Google Font API, Google Tag Manager, New Relic, Pantheon, Segment, Varnish, WordPress 5.3.1, jQuery 3.4.1, PHP, Nginx, MariaDB, MySQL
http://collateral.bugcrowd.com;Nginx
https://assetinventory.bugcrowd.com;Babel, CloudFlare, Google Analytics, Google Tag Manager, Moment.js 2.18.1, jQuery 3.3.1
https://forum.bugcrowd.com;Discourse 2.5.0, Ember.js 3.12.2, Google Font API, Handlebars 4.7.6, Moment.js 2.24.0, Nginx, jQuery 3.4.1, jQuery UI 1.12.1, Ruby on Rails, Ruby
https://api.bugcrowd.com;CloudFlare
http://www.bugcrowd.com;CloudFlare, Google Font API, Google Tag Manager, New Relic, Pantheon, Segment, Varnish, WordPress 5.3.1, jQuery 3.4.1, jQuery Migrate 3.1.0, PHP, Nginx, MariaDB, MySQL
http://go.bugcrowd.com;CloudFlare
https://go.bugcrowd.com;CloudFlare
https://hooks.bugcrowd.com;CloudFlare
http://ww2.bugcrowd.com;CloudFlare, Varnish
https://ww2.bugcrowd.com;CloudFlare, Varnish
https://tracker.bugcrowd.com;CloudFlare, Google Analytics, React, Ruby on Rails, jQuery 3.5.0, Ruby
https://collateral.bugcrowd.com;Nginx
https://events.bugcrowd.com;Nginx
https://www.bugcrowd.com;CloudFlare, Google Font API, Google Tag Manager, New Relic, Pantheon, Segment, Varnish, WordPress 5.3.1, jQuery 3.4.1, jQuery Migrate 3.1.0, PHP, Nginx, MariaDB, MySQL
```

https://github.com/Screetsec/Sudomy

Detecting Live HTTP/HTTPS

Resolve the domains and check the protocol http/https how many domains are actually alive. This feature uses a third-party tool, httprobe. By default sudomy check subdomain for working on http/https

```
Total                          [47]

[+] Probe subdomain for working on http/https
----------------------------------------------

        - https://email.assetinventory.bugcrowd.com
        - http://bugcrowd.com
        - https://blog.bugcrowd.com
        - http://docs.bugcrowd.com
        - https://email.bugs.bugcrowd.com
        - http://assetinventory.bugcrowd.com
        - http://email.assetinventory.bugcrowd.com
        - https://email.crowdcontrol.bugcrowd.com
        - https://email.forum.bugcrowd.com
        - https://assetinventory.bugcrowd.com
        - https://email.submit.bugcrowd.com
        - http://collateral.bugcrowd.com
        - http://email.bugcrowd.com
        - http://email.bugs.bugcrowd.com
        - https://email.bugcrowd.com
        - http://email.crowdcontrol.bugcrowd.com
        - http://email.forum.bugcrowd.com
        - http://email.submit.bugcrowd.com
        - https://concourse.bugcrowd.com
        - https://api.bugcrowd.com
        - http://events.bugcrowd.com
        - http://forum.bugcrowd.com
        - https://collateral.bugcrowd.com
        - https://docs.bugcrowd.com
        - https://pages.bugcrowd.com
        - http://gslink.bugcrowd.com
        - https://forum.bugcrowd.com
        - https://go.bugcrowd.com
        - http://go.bugcrowd.com
        - http://researcherdocs.bugcrowd.com
        - https://gslink.bugcrowd.com
        - https://researcherdocs.bugcrowd.com
        - https://gemstash-mattress.a.bugcrowd.com
        - https://hooks.bugcrowd.com
        - https://events.bugcrowd.com
        - http://proxilate.bugcrowd.com
        - https://proxilate.a.bugcrowd.com
        - https://proxilate.bugcrowd.com
        - https://bugcrowd.com
        - http://proxilate.a.bugcrowd.com
        - http://ww2.bugcrowd.com
        - https://tracker.bugcrowd.com
        - http://www.bugcrowd.com
        - https://ww2.bugcrowd.com
```

Or do you want to not perform httprobe, use argument `--no-probe`

```
sudomy -d bugcrowd.com --no-probe
```

Results

https://github.com/Screetsec/Sudomy

```
root@kali:~/Enumeration/Subdomain/version/Sudomy-1.1.5#dev/output/05-07-2020/bugcrowd.com# cat httprobe_subdomain.txt
http://bugcrowd.com
https://blog.bugcrowd.com
https://email.assetinventory.bugcrowd.com
http://docs.bugcrowd.com
https://docs.bugcrowd.com
https://email.bugs.bugcrowd.com
http://assetinventory.bugcrowd.com
https://email.crowdcontrol.bugcrowd.com
http://email.assetinventory.bugcrowd.com
https://email.forum.bugcrowd.com
http://email.bugcrowd.com
https://email.bugcrowd.com
http://email.bugs.bugcrowd.com
https://email.submit.bugcrowd.com
http://email.crowdcontrol.bugcrowd.com
https://assetinventory.bugcrowd.com
http://email.forum.bugcrowd.com
http://collateral.bugcrowd.com
http://email.submit.bugcrowd.com
https://api.bugcrowd.com
http://forum.bugcrowd.com
https://concourse.bugcrowd.com
http://events.bugcrowd.com
https://pages.bugcrowd.com
https://forum.bugcrowd.com
http://gslink.bugcrowd.com
https://collateral.bugcrowd.com
http://go.bugcrowd.com
https://go.bugcrowd.com
http://researcherdocs.bugcrowd.com
https://gslink.bugcrowd.com
https://gemstash-mattress.a.bugcrowd.com
https://events.bugcrowd.com
https://hooks.bugcrowd.com
http://proxilate.a.bugcrowd.com
http://proxilate.bugcrowd.com
https://proxilate.a.bugcrowd.com
https://proxilate.bugcrowd.com
https://bugcrowd.com
https://researcherdocs.bugcrowd.com
http://ww2.bugcrowd.com
https://tracker.bugcrowd.com
http://www.bugcrowd.com
https://ww2.bugcrowd.com
https://www.bugcrowd.com
```

https://github.com/Screetsec/Sudomy

Subdomain Takeover Check

Subdomain TakeOver Vulnerabilty Scanner, its not default so you must run the plugin with the command:

```
sudomy -d bugcrowd.com -tO
```

```
[+] Subdomain TakeOver - Check Possible Vulns
---------------------------------------------

    Ö [FAILS]   En: Unknown  https://blog.bugcrowd.com
    Ö [FAILS]   En: Unknown  http://docs.bugcrowd.com
    Ö [FAILS]   En: Unknown  http://bugcrowd.com
    Ö [FAILS]   En: Unknown  http://email.assetinventory.bugcrowd.com
    Ö [FAILS]   En: Unknown  http://email.bugcrowd.com
    Ö [FAILS]   En: Unknown  http://email.bugs.bugcrowd.com
    Ö [FAILS]   En: Unknown  http://assetinventory.bugcrowd.com
    Ö [FAILS]   En: Unknown  https://email.assetinventory.bugcrowd.com
    Ö [FAILS]   En: Unknown  https://concourse.bugcrowd.com
    Ö [FAILS]   En: Unknown  https://email.bugs.bugcrowd.com
    Ö [FAILS]   En: Unknown  https://assetinventory.bugcrowd.com
    Ö [FAILS]   En: Unknown  https://email.bugcrowd.com
    Ö [FAILS]   En: Unknown  http://email.crowdcontrol.bugcrowd.com
```

Results :

```
cat TakeOver.txt
```

```
https://blog.bugcrowd.com                    Unknown   Not.Vuln
http://docs.bugcrowd.com                     Unknown   Not.Vuln
http://bugcrowd.com                          Unknown   Not.Vuln
http://email.assetinventory.bugcrowd.com     Unknown   Not.Vuln
http://email.bugcrowd.com                    Unknown   Not.Vuln
http://email.bugs.bugcrowd.com               Unknown   Not.Vuln
http://assetinventory.bugcrowd.com           Unknown   Not.Vuln
https://email.assetinventory.bugcrowd.com    Unknown   Not.Vuln
https://concourse.bugcrowd.com               Unknown   Not.Vuln
https://email.bugs.bugcrowd.com              Unknown   Not.Vuln
https://assetinventory.bugcrowd.com          Unknown   Not.Vuln
https://email.bugcrowd.com                   Unknown   Not.Vuln
http://email.crowdcontrol.bugcrowd.com       Unknown   Not.Vuln
https://email.submit.bugcrowd.com            Unknown   Not.Vuln
https://api.bugcrowd.com                     Unknown   Not.Vuln
http://email.forum.bugcrowd.com              Unknown   Not.Vuln
http://email.submit.bugcrowd.com             Unknown   Not.Vuln
http://events.bugcrowd.com                   Unknown   Not.Vuln
https://collateral.bugcrowd.com              Unknown   Not.Vuln
http://forum.bugcrowd.com                    Unknown   Not.Vuln
https://docs.bugcrowd.com                    Unknown   Not.Vuln
http://collateral.bugcrowd.com               Unknown   Not.Vuln
https://forum.bugcrowd.com                   Unknown   Not.Vuln
http://go.bugcrowd.com                       Unknown   Not.Vuln
https://go.bugcrowd.com                      Unknown   Not.Vuln
http://gslink.bugcrowd.com                   Unknown   Not.Vuln
https://pages.bugcrowd.com                   Unknown   Not.Vuln
https://email.crowdcontrol.bugcrowd.com      Unknown   Not.Vuln
https://email.forum.bugcrowd.com             Unknown   Not.Vuln
https://gemstash-mattress.a.bugcrowd.com     Unknown   Not.Vuln
http://researcherdocs.bugcrowd.com           Unknown   Not.Vuln
http://proxilate.a.bugcrowd.com              Unknown   Not.Vuln
https://gslink.bugcrowd.com                  Unknown   Not.Vuln
http://proxilate.bugcrowd.com                Unknown   Not.Vuln
https://hooks.bugcrowd.com                   Unknown   Not.Vuln
https://bugcrowd.com                         Unknown   Not.Vuln
https://events.bugcrowd.com                  Unknown   Not.Vuln
https://proxilate.a.bugcrowd.com             Unknown   Not.Vuln
https://researcherdocs.bugcrowd.com          Unknown   Not.Vuln
https://proxilate.bugcrowd.com               Unknown   Not.Vuln
https://tracker.bugcrowd.com                 Unknown   Not.Vuln
http://ww2.bugcrowd.com                      Unknown   Not.Vuln
http://www.bugcrowd.com                      Unknown   Not.Vuln
https://ww2.bugcrowd.com                     Unknown   Not.Vuln
https://www.bugcrowd.com                     Unknown   Not.Vuln
```

https://github.com/Screetsec/Sudomy

Generate Report & Output

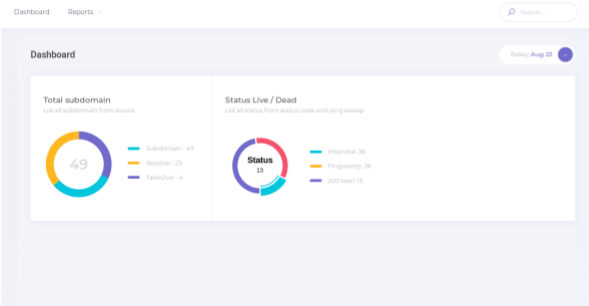
The sudomy application has been equipped with a reporting system with HTML and CSV output format that makes it easy for Cyber Security researchers and / or analyst

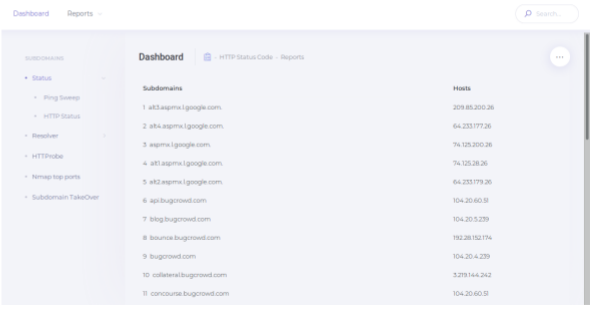
To create report in HTML Format

```
$ sudomy --all -d hackerone.com --html
```

HTML Report Sample:

Dashboard | Reports





Default Location

If the program has finished running, the output and report will be in the `output/reports folder`

```
[+] Generate Reports: Make report into HTML
--------------------------------------------

    Make template for reports
      - output/05-07-2020/bugcrowd.com/reports

    Successful Created ..

[+] Sudomy has been sucessfully completed
--------------------------------------------

    Location output:
      - output/05-07-2020/bugcrowd.com
      - output/05-07-2020/bugcrowd.com/report
      - output/05-07-2020/bugcrowd.com/screenshots
```

https://github.com/Screetsec/Sudomy

You can define path for outputfile (specify an output file when completed) with the argument

```
$ sudomy --all -d hackerone.com --outfile /root
```

```
[+] Sudomy has been sucessfully completed
-----------------------------------------------

    Location output:
      - /root/Sudomy-Output/bugcrowd.com
      - /root/Sudomy-Output/bugcrowd.com/report
      - /root/Sudomy-Output/bugcrowd.com/screenshots
```

Output Folder Structure

```
.
├── 05-07-2020
│   └── bugcrowd.com
│       ├── httprobe_subdomain.txt
│       ├── ip_dbasn.txt
│       ├── ip_dbport.txt
│       ├── ip_resolver.txt
│       ├── pars_subdomain_resolver.txt
│       ├── Passive_Collecting_URLParamter.txt
│       ├── Passive_Collecting_URLParamter_Uniq.txt
│       ├── Subdomain_Resolver.txt
│       ├── subdomain.txt
│       └── wappalyzer.txt
└── 05-08-2020
    └── bugcrowd.com
        ├── httprobe_subdomain.txt
        ├── HTTP_Status_Code.txt
        ├── ip_resolver.txt
        ├── pars_subdomain_resolver.txt
        ├── Pingsweep.txt
        ├── screenshots
        │   ├── http_assetinventory.bugcrowd.com_80.png
        │   ├── http_bugcrowd.com_80.png
        │   ├── http_collateral.bugcrowd.com_80.png
        │   ├── http_docs.bugcrowd.com_80.png
        │   ├── http_forum.bugcrowd.com_80.png
        │   ├── http_go.bugcrowd.com_80.png
        │   ├── http_gslink.bugcrowd.com_80.png
        │   ├── http_proxilate.a.bugcrowd.com_80.png
        │   ├── http_proxilate.bugcrowd.com_80.png
        │   ├── http_researcherdocs.bugcrowd.com_80.png
        │   ├── https_assetinventory.bugcrowd.com_443.png
        │   ├── https_blog.bugcrowd.com_443.png
        │   ├── https_bugcrowd.com_443.png
        │   ├── https_collateral.bugcrowd.com_443.png
        │   ├── https_docs.bugcrowd.com_443.png
        │   ├── https_email.assetinventory.bugcrowd.com_443.png
        │   ├── https_email.bugcrowd.com_443.png
        │   ├── https_email.bugs.bugcrowd.com_443.png
        │   ├── https_email.crowdcontrol.bugcrowd.com_443.png
        │   ├── https_email.forum.bugcrowd.com_443.png
        │   ├── https_email.submit.bugcrowd.com_443.png
        │   ├── https_forum.bugcrowd.com_443.png
        │   ├── https_gemstash-mattress.a.bugcrowd.com_443.png
        │   ├── https_go.bugcrowd.com_443.png
        │   ├── https_gslink.bugcrowd.com_443.png
        │   ├── https_pages.bugcrowd.com_443.png
        │   ├── https_proxilate.a.bugcrowd.com_443.png
        │   ├── https_proxilate.bugcrowd.com_443.png
        │   ├── https_researcherdocs.bugcrowd.com_443.png
```