

TheHarvester

TheHarvester是一个非常简单易用，但是功能强大而有效的工具。该工具早期用国家渗透测试或红队所参与设计。

将用于其开源情报（OSINT）进行搜集，以帮助确定公司在互联网上的外部威胁情况。该工具可使用多个公共数据源搜集电子邮件，姓名，子域，个人信息网址，DNS暴力枚举等，这些数据源可以包括：

描述	域名
百度搜索引擎	www.baidu.com
微软搜索引擎	www.bing.com
使用Rapid7项目声纳的数据	www.rapid7.com/research/project-sonar/
bingapi	微软搜索引擎，通过api
证书观察员监控证书透明度日志	https://sslmate.com/certspotter/
常见证书搜索	https://crt.sh/
DNSdumpster搜索引擎	https://dnsdumpster.com/
狗桩搜索引擎	www.dogpile.com
DuckDuckGo搜索引擎	www.duckduckgo.com
元搜索引擎	www.exalead.com/search
GitHub代码搜索引擎(需要GitHub个人访问令牌，见下文。)	www.github.com
谷歌搜索引擎(可选谷歌呆子。)	www.google.com
亨特搜索引擎(需要一个应用编程接口的关键，见下文。)	www.hunter.io
英特尔搜索引擎(需要一个应用编程接口密钥，见下文。)	www.intelx.io
谷歌搜索引擎，专门为领英用户搜索	www.linkedin.com
互联网安全与数据挖掘	www.netcraft.com
陌生人开放威胁交换	otx.alienvault.com
安全跟踪:安全跟踪搜索引擎，世界上最大的历史域名系统数据库(需要一个应用编程接口密钥，见下文。)	www.securitytrails.com
shodan: Shodan搜索引擎，将从发现的主机中搜索端口和横幅	www.shodanhq.com

描述	域名
专业人员的网络研究工具(需要一个应用编程接口密钥。)	spyse.com
运行网络研究工具可能需要10分钟以上，但值得等待	Suip
开源威胁情报	www.threatcrowd.org
搜索特雷洛板(使用谷歌搜索。)	trello
与特定领域相关的推特账户(使用谷歌搜索。)	twitter
Bing虚拟主机搜索	vhost
virustotal.com域名搜索	virustotal
雅虎搜索引擎	yahoo

声明

```
root@parrot: ~/home/kun
#theharvester
The command theharvester is deprecated. Please use theHarvester instead.
root@parrot: ~/home/kun
```

在非正常的情况下，TheHarvester是会提示“The command theharvester is deprecated. Please use theHarvester instead.”，不推荐使用服务器命令。请改用服务器”。

所以本次实验使用以下系统进行相关方面的实验或测试

```
Linux sif 4.19.0-kali4-amd64 #1 SMP Debian 4.19.28-2kali1 (2019-03-18) x86_64 GNU/Linux
```

一，帮助文档

sage:服务器选项

- d 要搜索的域名或公司名称
- b 数据来源:baidu, bing, bingapi, censys, crtsh, dogpile, google, google-certificates, googleCSE, googleplus, google-profiles, hunter, linkedin, netcraft, pgp, threatcrowd, twitter, vhost, virustotal, yahoo, all
- g 用谷歌工作代替普通的谷歌搜索
- s 从结果号X开始(默认:0)
- v 通过DNS解析验证主机名，并搜索虚拟主机
- f 将结果保存到一个超文本标记语言和一个可扩展标记语言文件中
- n 对发现的所有范围执行DNS反向查询
- c 对域名进行域名解析
- t 执行域名系统TLD扩展发现

- e 使用此域名服务器
- p 端口扫描检测到的主机并检查接管(80, 443, 22, 21, 8080)
- l 限制要处理的结果数量(Bing从50个结果到50个结果, 谷歌100到100, 而PGP不使用这个选项)
- h 使用SHODAN数据库查询发现的主机

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

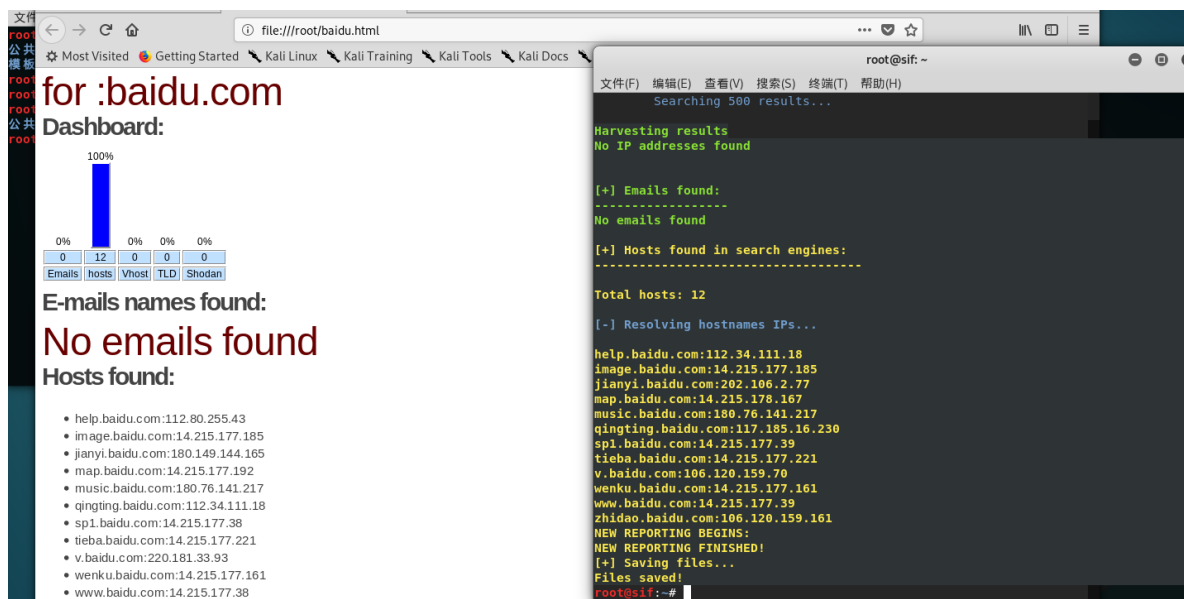
theharvester -d microsoft.com -l 200 -g -b google

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

theharvester -d cornell.edu -l 100 -b bing -h

```

二, 命令实例



The screenshot shows a web browser window displaying the theharvester dashboard for the domain **baidu.com**. The dashboard includes a progress bar showing 100% completion for the search. Below the progress bar, it states "E-mails names found: No emails found" and "Hosts found:" followed by a list of 12 hosts. To the right, a terminal window shows the output of the theharvester command, displaying the same list of hosts found in search engines.

for :baidu.com

Dashboard:

100%

0% 0% 0% 0%

0 12 0 0 0

Emails hosts Vhost TLD Shodan

E-mails names found:

No emails found

Hosts found:

- help.baidu.com:112.80.255.43
- image.baidu.com:14.215.177.185
- jianyi.baidu.com:180.149.144.165
- map.baidu.com:14.215.177.192
- music.baidu.com:180.76.141.217
- qingting.baidu.com:112.34.111.18
- sp1.baidu.com:14.215.177.38
- tieba.baidu.com:14.215.177.221
- v.baidu.com:220.181.33.93
- wenku.baidu.com:14.215.177.161
- www.baidu.com:14.215.177.38

Terminal Output:

```

root@osif: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
Searching 500 results...

Harvesting results
No IP addresses found

[+] Emails found:
-----
No emails found

[+] Hosts found in search engines:
-----

Total hosts: 12

[-] Resolving hostnames IPs...

help.baidu.com:112.34.111.18
image.baidu.com:14.215.177.185
jianyi.baidu.com:202.106.2.77
map.baidu.com:14.215.178.167
music.baidu.com:180.76.141.217
qingting.baidu.com:117.185.16.230
sp1.baidu.com:14.215.177.39
tieba.baidu.com:14.215.177.221
v.baidu.com:106.120.159.70
wenku.baidu.com:14.215.177.161
www.baidu.com:14.215.177.39
zhidao.baidu.com:106.120.159.161
NEW REPORTING BEGINS!
NEW REPORTING FINISHED!
[+] Saving files...
Files saved!
root@osif:~#

```

theharvester -d baidu.com -b baidu -l 10 -f baidu.html

对目标baidu.com进行OSINET进行公开的信息搜集, 扫描间隔为为“10”, 然后生成报告。

```
suggestion.baidu.com:220.181.38.138
t1.baidu.com:113.113.73.48
t10.baidu.com:113.113.73.48
t11.baidu.com:113.113.73.48
t12.baidu.com:113.113.73.48
t2.baidu.com:113.113.73.48
t3.baidu.com:113.113.73.48
tag.baidu.com:14.215.177.87
tieba.baidu.com:14.215.177.221
v.baidu.com:220.181.33.93
voice.baidu.com:14.215.178.102
vse.baidu.com:14.215.178.66
wenku.baidu.com:14.215.177.161
www.baidu.com:14.215.177.39
xapp.baidu.com:empty
xiaodu.baidu.com:14.215.178.100
xueshu.baidu.com:14.215.177.38
zhidao.baidu.com:106.120.159.161
zhidaocommit.baidu.com:106.120.159.161
zhidao.baidu.com:106.120.159.161

[-] Scanning ports (active):
- Scanning : 14.215.177.92
  Detected open ports: 80,443
  Searching takeovers for api.map.baidu.com
- Scanning : 14.215.178.31
  Detected open ports: 80,443
  Searching takeovers for api.open.baidu.com
- Scanning : 14.215.177.167
  Detected open ports: 80,443
  Searching takeovers for app.baidu.com
- Scanning : 14.215.178.42
```

theharvester -d baidu.com -b baidu -p -h

对Baidu.com进行OSINT搜索的同时，并对其进行端口扫描和SHODAN

TLD

TLD是顶级域名（Top-level domain）是ICANN在2013年开始实施的全球互联网扩张计划的一部分。

```
Searching 490 results...
Searching 500 results...

Harvesting results
No IP addresses found

[+] Emails found:
-----
No emails found

[+] Hosts found in search engines:
-----
Total hosts: 12

[-] Resolving hostnames IPs...
help.baidu.com:180.149.144.166
image.baidu.com:14.215.177.185
jianyi.baidu.com:117.185.16.213
map.baidu.com:14.215.177.192
music.baidu.com:180.76.141.217
qingting.baidu.com:117.185.16.213
spl.baidu.com:14.215.177.38
tieba.baidu.com:14.215.177.221
v.baidu.com:106.120.159.70
wenku.baidu.com:14.215.177.161
www.baidu.com:14.215.177.38
zhidao.baidu.com:106.120.159.161

[-] Starting DNS brute force:
Resolvers file can't be open
Error opening dns dictionary file
```

theharvester -d baidu.com -b baidu -c -t

对目标进行OSINT进行扫描，并对其进行解析，并对其进行顶级系统的扩展发现。

theharvester -d baidu.com -b baidu -n

查询目标OSINT的同时并对其进行DNS反向解析

music.baidu.com:180.76.141.217
qingting.baidu.com:112.34.111.18
spl.baidu.com:14.215.177.38
tieba.baidu.com:14.215.177.221
v.baidu.com:220.181.33.93
wenku.baidu.com:14.215.177.161
www.baidu.com:14.215.177.39
zhidao.baidu.com:106.120.159.161

[+] Starting active queries:

117.185.16.230

[~]Performing reverse lookup in : 117.185.16.0/24

117.185.16.25514.215.177.185

[~]Performing reverse lookup in : 14.215.177.0/24

14.215.177.255202.106.2.78

[~]Performing reverse lookup in : 202.106.2.0/24

202.106.2.25514.215.178.167

[~]Performing reverse lookup in : 14.215.178.0/24

14.215.178.255180.76.141.217

[~]Performing reverse lookup in : 180.76.141.0/24

180.76.141.255112.34.111.18

[~]Performing reverse lookup in : 112.34.111.0/24

112.34.111.25514.215.177.38

14.215.177.221

220.181.33.93

[~]Performing reverse lookup in : 220.181.33.0/24

220.181.33.25514.215.177.161

14.215.177.39

106.120.159.161

8 KB)