

子域枚举的意义

这不是一个新鲜的技术，它的存在是为了增加发现漏洞的概率，服务于一次渗透测试的成功。

- 子域往往运行着许多应用程序，增加漏洞发现的机会
- 相同的漏洞往往会出现在不同的子域之中
- 隐藏的子域经常会存在重要的应用程序，如果发现关键漏洞可以直击目标核心

子域枚举技术详解

1.通过搜索引擎

Google语法例如" site:* " 是一种众所周知的方法，它可以用在所有搜索引擎上，但在Google上支持运算符可以帮助我们排除不感兴趣的子域，

```
1 site:*.google.com -www -search -chrome -news
```

site:*.google.com -www -search -chrome -news



乃木坂46 白石麻衣、「美は卒業を認識したのは...」『パナママン』の ...

2020年2月8日 - 乃木坂46を卒業する白石麻衣が、2月11日（火）放送のテレビ朝日『パナママンのドライブスリー』に出演する。

sites.google.com > site > ykleikkhkhwmthrusmskwnci - 翻译此页

[ยกเลิกข้อความ SMS กวนใจ เครือข่าย truemove H - truemove H](#)

2018年6月20日 - 'ไซต์นี้จัดทำขึ้นเพื่อแนะนำแพ็คเกจเสริมของเครือข่ายอินเทอร์เน็ต truemove h ให้เข้าถึงผู้ใช้งานในเครือข่าย truemove h และ ...

console.cloud.google.com > ...

[Google云端平台](#)

借助Google 云端平台，您可以利用Google 所用的基础架构构建、部署以及调整应用、网站和服务。

feedproxy.google.com > noticiasveja ▾ 翻译此页

[Mané: 'Não preciso de Ferraris, relógios e aviões, quero ...](#)

2019年10月17日 - Astro senegalês do Liverpool falou sobre suas origens humildes e contou que gasta a maior parte de seu dinheiro com caridade.

feedproxy.google.com > trdmiami ▾ 翻译此页

[Puttshack Signs Miami Lease At Brickell City Centre](#)

2020年2月12日 - A London mini-golf company signed its first lease in Miami and its largest to date, at Brickell City Centre.

feedproxy.google.com > trdmiami ▾ 翻译此页

[Boston Considers Eliminating Broker Fees - The Real Deal](#)

2020年2月7日 - Boston Mayor Martin Walsh is forming a working group to study broker fees, following New York State's move to nix them.

2.通过第三方服务的DNS数据集检索给定域的子域

- 1 VirusTotal:<https://www.virustotal.com/gui/home/search>
- 2 DNSdumpster:<https://dnsdumpster.com/>

virustotal最初由Hispacec维护是一个免费对可疑文件和网址进行快速检索的在线应用，它检索出的信息比搜索引擎查找的更加直观和全面，不仅可以找到子域还可以找例如whois之类的其它对于网站重要的信息，对于信息侦察阶段具有参考意义。

Passive DNS Replication ⓘ

Date resolved	IP
2020-02-19	172.217.22.142
2020-02-19	216.58.215.46
2020-02-19	172.217.18.206
2020-02-19	216.58.198.206
2020-02-19	216.58.204.110
2020-02-19	172.217.19.238
2020-02-15	216.58.206.238
2020-02-15	216.58.204.142
2020-02-13	216.58.201.238
2020-02-13	172.217.172.142

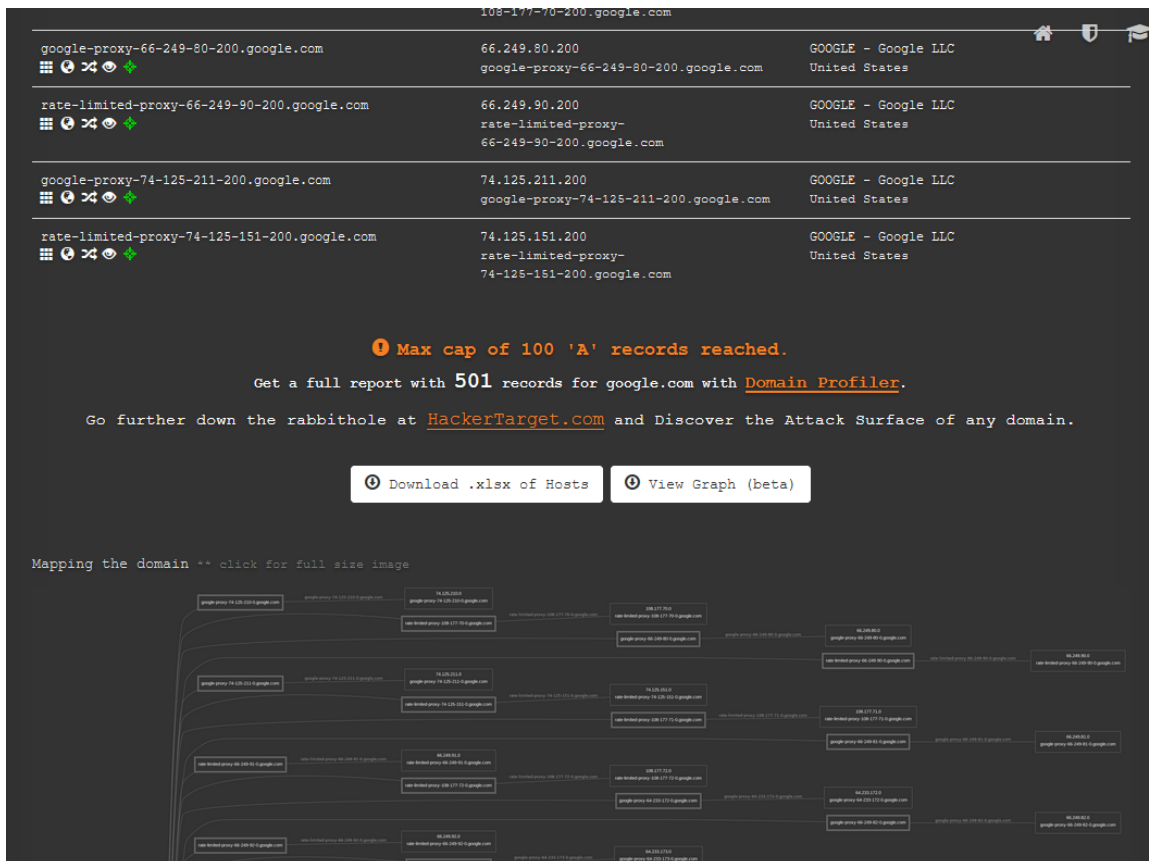
...

Subdomains ⓘ

get.google.com	172.217.219.101	172.217.219.139	172.217.219.102	...
www.google.com	216.58.209.228	172.217.18.196	216.58.213.132	...
services.google.com	209.85.146.113	172.217.18.238	172.217.212.100	...
consent.google.com	192.55.83.30	192.41.162.30	192.52.178.30	...
fundingchoicesmessages.google.com	173.194.194.138	216.58.198.46	172.217.23.14	...
youtube-ui.l.google.com	108.177.96.91	172.253.120.198	172.253.123.190	...
ads.google.com	142.250.9.101	142.250.9.102	142.250.9.100	...
lh3.google.com	216.58.207.174	216.58.198.78	172.217.214.139	...
mt.google.com	172.217.219.100	172.217.219.102	172.217.219.138	...
sb-ssl.google.com	216.58.213.142	172.217.23.110	216.58.207.238	...

DNSdumpster的好处是有一个Mapping,

<https://dnsdumpster.com/static/map/google.com.png>



3.工具枚举

1 Sublist3r: <https://github.com/aboul31a/Sublist3r>

Sublist3r是一款优秀的工具，它不仅枚举子域，还添加了搜索引擎如"Google"、“Yahoo”、“Bing”、“Ask”、甚至是“Baidu”，如果你熟悉网络防火墙在这里可以意识到你需要挂载一个流量代理，或者使用海外的远程服务器才能发挥它所有的功能，同时它还使用了Netcraft,Virus total,ThreatCrowd,DNSdumpster,ReverseDNS来枚举子域，所以这是一个“all in one”的工具。

1 python sublist3r.py -e google,bing,yahoo,virustotal -d example.com -b -p 80,443

```

root@kali:~/Sublist3r# python sublist3r.py -e google,bing,yahoo,virustotal,baidu
-d google.com -b -p 80,443

          _____
         /  _  _  \
        /  _  _  \
       /  _  _  \
      /  _  _  \
     /  _  _  \
    /  _  _  \
   /  _  _  \
  /  _  _  \
 /  _  _  \
/  _  _  \

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for google.com
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Yahoo..
[-] Searching now in Virustotal..
[-] Searching now in Baidu..

```

- 1 -e:是指定搜索引擎
- 2 -b:是Brute俗称爆破
- 3 -p:是指定端口

Usage

Short Form	Long Form	Description
-d	--domain	Domain name to enumerate subdomains of
-b	--bruteforce	Enable the subbrute bruteforce module
-p	--ports	Scan the found subdomains against specific tcp ports
-v	--verbose	Enable the verbose mode and display results in realtime
-t	--threads	Number of threads to use for subbrute bruteforce
-e	--engines	Specify a comma-separated list of search engines
-o	--output	Save the results to text file
-h	--help	show the help message and exit

我建议阅读项目的说明文档，这样便于真正的灵活使用它。

```

1 assetfinder (https://github.com/tomnomnom/assetfinder)
2 https://github.com/tomnomnom/assetfinder/releases
3 assetfinder [--subs-only] <domain>

```

▼ Assets 10

-  [assetfinder-darwin-386-0.1.0.tgz](#)
-  [assetfinder-darwin-amd64-0.1.0.tgz](#)
-  [assetfinder-freebsd-386-0.1.0.tgz](#)
-  [assetfinder-freebsd-amd64-0.1.0.tgz](#)
-  [assetfinder-linux-386-0.1.0.tgz](#)
-  [assetfinder-linux-amd64-0.1.0.tgz](#)
-  [assetfinder-windows-386-0.1.0.zip](#)
-  [assetfinder-windows-amd64-0.1.0.zip](#)
-  [Source code \(zip\)](#)
-  [Source code \(tar.gz\)](#)

这款子域枚举工具的平台支持性十分良好，而且速度十分优异，我下载了二进制文件直接可以在Windows下使用，

 C:\Windows\system32\cmd.exe

```
E:\>assetfinder.exe -subs-only github.com
ns1.github.com
ns2.github.com
glb-db52c2cf8be544.github.com
1b-192-30-255-110-sea.github.com
1b-192-30-255-120-sea.github.com
1b-192-30-255-170-sea.github.com
1b-192-30-255-1-sea.github.com
1b-192-30-255-111-sea.github.com
1b-192-30-255-121-sea.github.com
1b-192-30-255-171-sea.github.com
1b-192-30-255-2-sea.github.com
1b-192-30-255-112-sea.github.com
1b-192-30-255-82-sea.github.com
1b-192-30-254-192-sea.github.com
1b-192-30-255-113-sea.github.com
```

```
1 altdns: https://github.com/infosec-au/altdns
```

Altdns是一个DNS侦查工具,通过变更和排列允许发现符合模式的子域的工具

#2 DNS Pattern Identification Results (Altdns)

```
>> ~/altdns ./altdns.py -i data/subdomains.txt -o april_output -w wordtest.txt -r -s resolved_results
[+] 500/48972 completed
[+] 1000/48972 completed
[+] 1500/48972 completed
[+] 2000/48972 completed
[+] 2500/48972 completed
[+] 3000/48972 completed
[+] 3500/48972 completed
```

```
>> ~/altdns cat resolved_results
acs.elb.us-west-2.elb.amazonaws.com.
test.com.us-west-1.compute.amazonaws.com.
apollo.com.us-west-2.elb.amazonaws.com.
enigma.com.us-west-2.elb.amazonaws.com.
an.com.us-west-2.elb.amazonaws.com.
cn.us-east-1.elb.amazonaws.com.
events.com.events.s3-website-us-west-2.amazonaws.com.
ava.com.us-west-2.elb.amazonaws.com.
cdn.com.us-west-2.elb.amazonaws.com.
fantasy.com.us-west-2.elb.amazonaws.com.
ee.com.us-west-2.elb.amazonaws.com.
dev.com.
test.com.cloudflare.net.
livestats.com.us-west-2.elb.amazonaws.com.
```

类似的工具还有dnsrecon:<https://github.com/darkoperator/dnsrecon>作为一个dns枚举脚本

4.Certificate Transparency(CT)

证书透明度 (CT) 旨在记录、审核和监视证书颁发机构 (CA)

(https://en.wikipedia.org/wiki/Certificate_authority)颁发的证书,

CT允许网站用户和域所有者识别错误的或者被恶意修改的颁发证书,

这有助于识别未授权的CA, CA是受信任的第三方, 受数字证书的所有者和依赖证书的一方的信任,

证书颁发机构CA会颁发每个SSL/TLS证书发布到公共日志中,

SSL/TLS证书通常会包含域名、子域、电子邮件这些对攻击者有价值的信息,

如果你要成为理论专家, 我建议你阅读 (<https://blog.appsecco.com/certificate-transparency-the-bright-side-and-the-dark-side-8aa47d9a6616>)

(1)crt.sh

```
1 https://crt.sh/?q=%25.example.com
```

crt.sh Identity Search						Group by Issuer
Criteria						Search: 'google.com'
Certificates	crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
	2381394777	2020-01-27	2011-07-13	2012-07-13	*.docs.google.com *.mail.google.com *.plus.google.com *.sites.google.com *.talkgadget.google.com	C=US, O=Google Inc, CN=Google Internet Authority
	2380986199	2020-01-26	2011-02-16	2012-02-16	*.docs.google.com *.mail.google.com *.sites.google.com *.talkgadget.google.com	C=US, O=Google Inc, CN=Google Internet Authority
	2380850988	2020-01-26	2012-02-29	2013-02-28	onex.wifi.google.com	C=US, O=Google Inc, CN=Google Internet Authority
	2380841885	2020-01-26	2011-07-13	2012-07-13	accounts.google.com	C=US, O=Google Inc, CN=Google Internet Authority
	2380681291	2020-01-26	2013-11-22	2013-11-24	hosted-id.google.com	C=US, O=Google Inc, CN=Google Internet Authority G2
	2380579544	2020-01-26	2011-05-11	2012-05-11	accounts.google.com	C=US, O=Google Inc, CN=Google Internet Authority
	2379825238	2020-01-26	2011-05-11	2012-05-11	adwords.google.com adwords.google.com.ar	C=US, O=Google Inc, CN=Google Internet Authority

crt.sh提供PostgreSQL接口来提权给定域名的子域

```
1 #!/bin/sh
2
3 # Script by Hanno Bock - https://github.com/hannob/tlshelpers/blob/master/getsut
domain
4
5 query="SELECT ci.NAME_VALUE NAME_VALUE FROM certificate_identity ci WHERE ci.NAM
E_TYPE = 'dNSName' AND reverse(lower(ci.NAME_VALUE)) LIKE reverse(lower('%.$1')));"
6
7 echo $query | \
8 psql -t -h crt.sh -p 5432 -U guest certwatch | \
9 sed -e 's:^ *::g' -e 's:^*\.:g' -e '/^$/d' | \
10 sort -u | sed -e 's:*::g'
```

也可以使用python脚本

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# python crtsh.py github.com
*.github.com
porter2.github.com
importer2.github.com
import2.github.com
cla.github.com
jira.github.com
lab.github.com
staging-lab.github.com
*.staging-lab.github.com
review-lab.github.com
*.review-lab.github.com
vpn-ca.iad.github.com
id.github.com
*.id.github.com
cloud.github.com
f.cloud.github.com
brandguide.github.com
styleguide.github.com
enterprise.github.com
support.enterprise.github.com
pkg.github.com
*.pkg.github.com
stg.github.com
```

优秀的研究人员把更多的ct搜索脚本放在这里

(<https://github.com/appsecco/the-art-of-subdomain-enumeration>)

(2)massdns(<https://github.com/blechschmidt/massdns>)

该项目使用前需要进行编译，在根目录下运行make即可

massdns支持crt.sh使用


```
1 ./scripts/ct.py github.com | ./bin/massdns -r lists/resolvers.txt -t A -o S -w results.txt
```

```
root@kali: ~/massdns
File Edit View Search Terminal Help
root@kali:~/massdns# ./scripts/ct.py github.com | ./bin/massdns -r lists/resolvers.txt -t A -o S -w results.txt
Reading domain list from stdin.
Privileges have been dropped to "nobody:nogroup" for security reasons.

Processed queries: 0
Received packets: 0
Progress: 0.00% (00 h 00 min 00 sec / 00 h 00 min 00 sec)
Current incoming rate: 0 pps, average: 0 pps
Current success rate: 0 pps, average: 0 pps
Finished total: 0, success: 0 (0.00%)
Mismatched domains: 0 (0.00%), IDs: 0 (0.00%)
Failures: 0: 0.00%, 1: 0.00%, 2: 0.00%, 3: 0.00%, 4: 0.00%, 5: 0.00%, 6: 0.00%, 7: 0.00%, 8: 0.00%, 9: 0.00%, 10: 0.00%, 11: 0.00%, 12: 0.00%, 13: 0.00%, 14: 0.00%, 15: 0.00%, 16: 0.00%, 17: 0.00%, 18: 0.00%, 19: 0.00%, 20: 0.00%, 21: 0.00%, 22: 0.00%, 23: 0.00%, 24: 0.00%, 25: 0.00%, 26: 0.00%, 27: 0.00%, 28: 0.00%, 29: 0.00%, 30: 0.00%, 31: 0.00%, 32: 0.00%, 33: 0.00%, 34: 0.00%, 35: 0.00%, 36: 0.00%, 37: 0.00%, 38: 0.00%, 39: 0.00%, 40: 0.00%, 41: 0.00%, 42: 0.00%, 43: 0.00%, 44: 0.00%, 45: 0.00%, 46: 0.00%, 47: 0.00%, 48: 0.00%, 49: 0.00%, 50: 0.00%,

Response: | Success: | Total:
OK: | 0 ( 0.00%) | 0 ( 0.00%)
NXDOMAIN: | 0 ( 0.00%) | 0 ( 0.00%)
SERVFAIL: | 0 ( 0.00%) | 0 ( 0.00%)
```

保存结果的文件在目录下

```
Open [results.txt] Save
~/massdns
offer.github.com. CNAME github.github.io.
pkg.github.com. A 3.114.74.150
community.github.com. CNAME redirect.github.com.
f.cloud.github.com. CNAME r2.shared.global.fastly.net.
camo.github.com. CNAME github.github.io.
vpn-ca.iad.github.com. CNAME github.github.io.
mac-installer.github.com. CNAME d4hwcs1zqtws.cloudfront.net.
classroom.github.com. CNAME classroom.github.com.herokudns.com.
cloud.github.com. CNAME d24z2fz21y4fag.cloudfront.net.
status.github.com. CNAME octostatus-production-285068721.us-east-1.elb.amazonaws.com.
brandguide.github.com. CNAME github.github.io.
api.security.github.com. A 192.30.253.175
api.security.github.com. A 192.30.253.176
education.github.com. CNAME glb-db52c2cf8be544.github.com.
maintainers.github.com. CNAME maintainers.github.com.herokudns.com.
jira.github.com. CNAME jira.github.com.herokudns.com.
lab.github.com. CNAME lab.github.com.herokudns.com.
atom-installer.github.com. CNAME github.map.fastly.net.
lab-sandbox.github.com. CNAME github.github.io.
talks.github.com. CNAME github.github.io.
styleguide.github.com. CNAME styleguide.github.com.herokudns.com.
dodgeball.github.com. CNAME github.github.io.
helpnext.github.com. CNAME github.github.io.
jobs.github.com. A 192.30.253.176
jobs.github.com. A 192.30.253.175
vscode-auth.github.com. CNAME vscode-auth.github.com.herokudns.com.
support.enterprise.github.com. CNAME redirect.github.com.
```

script目录下的(subbrute.py)支持对子域进行暴力枚举

```
1 ./scripts/subbrute.py lists/names.txt github.com | ./bin/massdns -r lists/resolvers.txt -t A -o S -w results.txt
```

```
root@kali: ~/massdns
File Edit View Search Terminal Help
Processed queries: 20829
Received packets: 1344
Progress: 0.00% (00 h 01 min 28 sec / 00 h 01 min 28 sec)
Current incoming rate: 2 pps, average: 15 pps
Current success rate: 0 pps, average: 9 pps
Finished total: 10829, success: 838 (7.74%)
Mismatched domains: 126 (9.45%), IDs: 0 (0.00%)
Failures: 0: 0.02%, 1: 0.05%, 2: 0.03%, 3: 0.04%, 4: 0.06%, 5: 0.06%, 6: 0.06%,
7: 2.58%, 8: 0.06%, 9: 0.02%, 10: 0.05%, 11: 0.03%, 12: 0.03%, 13: 0.04%, 14:
0.02%, 15: 0.03%, 16: 0.05%, 17: 3.98%, 18: 0.36%, 19: 0.04%, 20: 0.04%, 21: 0.
06%, 22: 0.01%, 23: 0.01%, 24: 0.02%, 25: 0.03%, 26: 0.06%, 27: 0.04%, 28: 3.32
%, 29: 0.93%, 30: 0.03%, 31: 0.04%, 32: 0.03%, 33: 0.02%, 34: 0.05%, 35: 0.03%,
36: 0.03%, 37: 0.04%, 38: 2.37%, 39: 0.23%, 40: 0.06%, 41: 0.06%, 42: 0.06%, 4
3: 0.03%, 44: 0.04%, 45: 0.03%, 46: 83.84%, 47: 0.93%, 48: 0.04%, 49: 0.04%, 50
: 92.26%,
Response: | Success: | Total:
OK: | 794 ( 94.75%) | 890 ( 66.77%)
NXDOMAIN: | 5 ( 0.60%) | 5 ( 0.38%)
SERVFAIL: | 39 ( 4.65%) | 42 ( 3.15%)
REFUSED: | 0 ( 0.00%) | 396 ( 29.71%)
FORMERR: | 0 ( 0.00%) | 0 ( 0.00%)
```

(3)censys

censys是跟shodan同种类的搜索引擎，黑客可以用来做信息侦察，安全人员可以拿来做安全研究

```
1 https://censys.io/ipv4?q=example.com
```



IPv4 Hosts

[Results](#) [Map](#) [Metadata](#) [Report](#)

Quick Filters

For all fields, see [Data Definitions](#)

Autonomous System:

83.65K AMAZON-02
36.47K AMAZON-AES
35.41K DIGITALOCEAN-ASN
27.16K CNNIC-ALIBABA-CN-
NET-AP Hangzhou
Alibaba Advertising
Co.,Ltd.
20.01K MICROSOFT-CORP-
MSN-AS-BLOCK

[More](#)

Protocol:

394.55K 80/http
300.64K 443/https
172.91K 22/ssh
57.15K 8080/http
38.19K 3306/mysql

[More](#)

Tag:

491.5K http
278.97K https
172.91K ssh
44.89K database
38.19K mysql

[More](#)

IPv4 Hosts

Page: 1/19,665 Results: 491,620 Time: 136ms

47.114.63.105

🌐 CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd. (37963) 📍 Hangzhou, Zhejiang, China
🐧 Ubuntu ⚙️ 22/ssh, 3306/mysql, 443/https, 80/http, 8080/http, 8888/http
🔍 没有找到站点 📄 github-trending.api.ioslide.com
🔍 8080.http.get.body: `://github.com/twostraws.png`

[DATABASE](#) [MYSQL](#)

193.0.115.200

🌐 UW-AS (8890) 📍 Lucynow Duzy, Mazovia, Poland
🐧 Debian ⚙️ 443/https
🔍 443.https.get.body: `://github.com`

193.0.115.199

🌐 UW-AS (8890) 📍 Lucynow Duzy, Mazovia, Poland
🐧 Debian ⚙️ 443/https
🔍 443.https.get.body: `://github.com`

91.201.213.191 (191-213-201-91.zrh.sportradar.com.)

🌐 SPORTRADAR-AS (51776) 📍 Switzerland
⚙️ 443/https, 80/http
🔍 Matomo 3.13.1 - Analytics Platform - Matomo 📄 vgt.betradar.com, vgt.swiftscore.com

140.82.53.38 (140.82.53.38.vultr.com.)

🌐 AS-CHOOPA (20473) 📍 Aubervilliers, Île-de-France, France
⚙️ 443/https, 80/http
🔍 list of bounties 📄 donate.dumpstack.io
🔍 443.https.get.body: `- <a href="https://github.com/jollheef/appvm/issues/15">github.com`

95.217.8.136 (static.136.8.217.95.clients.your-server.de.)

🌐 HETZNER-AS (24940) 📍 Germany
🐧 Ubuntu ⚙️ 22/ssh, 80/http

同时也可以使用censys python库编写的工具来提取给定域的子域

```
1 https://github.com/christophetd/censys-subdomain-finder
2 https://github.com/0xbharath/censys-enumeration
```

使用这类工具通常都需要设置API，

这里需要先注册一个账户在<https://censys.io/register>

注册是免费的，然后访问<https://censys.io/account/api>

[Details](#) [API](#) [Billing](#)

API Credentials

Below are the credentials that can be used for accessing [authenticated APIs](#):

API ID



Secret



[RESET MY API SECRET](#)

并且使用你注册账户的API ID和API Secret设置两个环境变量

```
1 $ export CENSYS_API_ID="*****"  
2 $ export CENSYS_API_SECRET="*****"
```

值得一提的是censys_enumeration可以枚举子域和邮箱，用法如下：

```
1 $ python censys_enumeration.py domains.txt
```

censys_subdomain_finder:

```
1 $ python censys_subdomain_finder.py example.com  
2 [*] Searching Censys for subdomains of example.com  
3 [*] Found 5 unique subdomains of example.com  
4  
5 - products.example.com  
6 - www.example.com  
7 - dev.example.com  
8 - example.com  
9 - support.example.com
```

5.自治系统/自治域(Autonomous system, AS)

自治系统是指在互联网中，一个或多个实体管辖下的所有IP网络和路由器的组合，它们对互联网执行共同的路由策略,参看RFC 1930中更新的定义。

```
1 https://tools.ietf.org/html/rfc1930  
2 https://en.wikipedia.org/wiki/Autonomous_system_(Internet)  
3 https://www.iana.org/assignments/as-numbers/as-numbers.xhtml
```

通过查找自治系统(AS)编号可以帮助我们识别某个组织的网络块具有的有效域，

```
1 https://asn.cymru.com/cgi-bin/whois.cgi  
2 https://www.ultratools.com/tools/asnInfo  
3 https://nmap.org/nsedoc/scripts/targets-asn.html
```

Family: ☒ IPv4 ☐ IPv6 Methods: ☒ whois ☒ peer-whois
Flags: ☒ prefix ☒ cc ☒ registry ☒ allocated ☒ nottruncate ☒ verbose

Insert your IP or ASN in the textbox above.

IPv4 [OPTIONAL COMMENT]

Eg. '4.2.2.2 2004-12-10 11:33:21 GMT'

AS#

Eg. 'AS23028'

IPv6 [OPTIONAL COMMENT]

--- snip snip ---
2001:5c0:8fff:fffe::ff6 2004-12-10 11:32:01 GMT
2001:5c0:8fff:fffe::ff7 2004-12-10 11:33:21 GMT
--- snip snip ---

Both IPv4 and IPv6 addresses are supported.
However, only one address family is permitted
per query. In other words, you may NOT intermix
IPv4 and IPv6 addresses.

Executing commands. Please be patient!

v4.whois.cymru.com

The server returned 2 line(s).

AS	IP	BGP Prefix	CC	Registry	Allocated	AS Name
16509	13.229.188.59	13.228.0.0/15	US	arin	2016-08-09	AMAZON-02, US

v4-peer.whois.cymru.com

The server returned 3 line(s).

PEER_AS	IP	BGP Prefix	CC	Registry	Allocated	AS Name
2914	13.229.188.59	13.228.0.0/15	US	arin	2016-08-09	NTT-COMMUNICATIONS-2914, US
6453	13.229.188.59	13.228.0.0/15	US	arin	2016-08-09	AS6453, US

 Email  Share

ASN Lookup & Information

The ASN Information tool provides complete autonomous system (AS) information.

Autonomous Systems are routable networks within the public Internet, administered by the local RIRs and assigned to owners of networks. The ASN Information tool displays information about an IP address's Autonomous System Number (ASN) such as: IP owner, registration date, issuing registrar and the max range of the AS with total IPs.

Enter an AS number, IP address, or a Company name.

Related Tools: [CDR/Netmask](#) [What's your IP](#) [Decimal IP Calculator](#)

AS16509

Country: US
Registration Date: 2000-05-04
Registrar: arin
Owner: AMAZON-02, US

找到的ASN编号可以使用nmap脚本来查找域的网块

```
1 nmap --script targets-asn --script-args targets-asn.asn=ASN编号
```

```
C:\Users\Administrator>nmap --script targets-asn --script-args targets-asn.asn=16509
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-23 23:35 ?D1ú±ê×?ê±??
Pre-scan script results:
  targets-asn:
    16509
      3.0.0.0/15
      3.5.128.0/24
      3.5.129.0/24
      3.5.130.0/24
      3.5.128.0/22
      3.5.131.0/24
      3.5.132.0/24
      3.5.132.0/23
      3.5.133.0/24
      3.5.208.0/24
      3.5.209.0/24
      3.5.210.0/24
      3.5.208.0/22
      3.5.211.0/24
      3.5.212.0/24
      3.5.212.0/23
      3.5.213.0/24
      3.6.0.0/15
      3.8.0.0/14
      2.12.0.0/16
```

还有其它“花哨”的手段可以阅读参考书(<https://hakin9.org/a-penetration-testers-guide-to-subdomain-enumeration/>)进行学习补充, hakin9提供了在线答疑功能, 当你有疑虑的时候可以直击右下角进行询问在线答疑人员。

实例参考:

本例子引用了h1中的一个报告(<https://hackerone.com/reports/770513>)

(1)首先通过crt.sh来查找存在多级子域的目标



Criteria	Type: Identity	Match: ILIKE	Search: '%.%.%.8x8.com'			
ertificates	crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
	1862945263	2019-09-09	2019-08-28	2020-09-28	*.prod.us-east-1.ai.8x8.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	1822044596	2019-08-29	2019-08-22	2020-09-22	*.dev.us-east-1.ai.8x8.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	1817385556	2019-08-28	2019-08-28	2020-09-28	*.prod.us-east-1.ai.8x8.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	1795729913	2019-08-22	2019-08-22	2020-09-22	*.dev.us-east-1.ai.8x8.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	1812431063	2019-08-08	2019-08-08	2019-11-06	*.100.us-east-1.acceptance.cloud.8x8.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1751791851	2019-08-08	2019-08-08	2019-11-06	*.100.us-east-1.acceptance.cloud.8x8.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1812427214	2019-08-08	2019-08-08	2019-11-06	*.01.us-east-1.acceptance.cloud.8x8.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1751788043	2019-08-08	2019-08-08	2019-11-06	*.01.us-east-1.acceptance.cloud.8x8.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1812306711	2019-08-08	2019-08-08	2019-11-06	*.01.us-east-1.acceptance.cloud.8x8.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1751701394	2019-08-08	2019-08-08	2019-11-06	*.01.us-east-1.acceptance.cloud.8x8.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1443087767	2019-05-07	2019-05-07	2020-06-07	*.qa.us-east-1.ai.8x8.com *.stg.us-east-1.ai.8x8.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	804503927	2018-10-01	2018-09-26	2019-10-26	*.prod.us-east-1.ai.8x8.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	803946172	2018-10-01	2018-09-20	2019-10-20	*.dev.us-east-1.ai.8x8.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	788922624	2018-09-26	2018-09-26	2019-10-26	*.prod.us-east-1.ai.8x8.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	770132733	2018-09-20	2018-09-20	2019-10-20	*.dev.us-east-1.ai.8x8.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	315064848	2018-01-28	2018-01-28	2018-04-28	sip1.sw.us-east.chalet.8x8.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	266645760	2017-11-29	2017-11-29	2018-02-27	sip1.sw.us-east.chalet.8x8.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	220666504	2017-09-30	2017-09-30	2017-12-29	sip1.sw.us-east.chalet.8x8.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

315064848	2018-01-28	2018-01-28	2018-04-28	sip1.sw.us-east.chalet.8x8.com
266645760	2017-11-29	2017-11-29	2018-02-27	sip1.sw.us-east.chalet.8x8.com
220666504	2017-09-30	2017-09-30	2017-12-29	sip1.sw.us-east.chalet.8x8.com

(2)接着使用assetfinder配合httprobe来枚举子域

- 1 <https://github.com/tomnomnom/assetfinder/releases>
- 2 <https://github.com/tomnomnom/httprobe/releases>

C:\Windows\system32\cmd.exe

```
C:\Users\gguze>assetfinder -subs-only chalet.8x8.com | httprobe
http://client-beta.global.chalet.8x8.com
https://client-beta.global.chalet.8x8.com
```

将目标锁定为<https://client-beta.global.chalet.8x8.com/>

(3)用dirsearch来进行目录探测

- 1 <https://github.com/maurosoria/dirsearch>

```
F:\dirsearch>python dirsearch.py -b -u "https://client-beta.global.chalet.8x8.com/" -e html,json
```

dirsearch v0.3.9

Extensions: html, json | HTTP method: get | Threads: 10 | Wordlist size: 6422

Error Log: F:\dirsearch\logs\errors-20-02-23_23-07-30.log

Target: https://client-beta.global.chalet.8x8.com/

[23:07:31] Starting:

[23:07:44] 400 - 915B - /%2e%2e/google.com

[23:07:47] 400 - 277B - /%ff/

[23:12:08] 200 - 15KB - /favicon.ico

[23:12:57] 200 - 5KB - /index.html

[23:13:47] 200 - 412B - /manifest.json

[23:14:16] 200 - 97B - /oauth

[23:17:06] 200 - 0B - /soap/

Task Completed

https://client-beta.global.chalet.8x8.com/oauth

:bad_params

[Back](#)

(4)使用arjun查找隐藏参数

```
1 https://github.com/s0md3v/Arjun
```

C:\Windows\system32\cmd.exe

```
C:\Users\gguze\Desktop\tools\Arjun>arjun.py -u "https://client-beta.global.chalet.8x8.com/oauth" --get
```

```
  _/ _/ _/
 ( _/ _/ _/ ) v1.5
  _/ _/ _/
```

```
Analysing the content of the webpage
Analysing behaviour for a non-existent parameter
Reflections: 0
Response Code: 200
Content Length: 97
Plain-text Length: 20
Parsing webpage for potential parameters
Performing heuristic level checks
Heuristic found 2 potential parameters.
Scan Completed
Valid parameter found: error
Reason: Different number of reflections
```

(5)插入Payload获得xss

```
1 Payload : "<><img onerror=alert(1) src>
```

https://client-beta.global.chalet.8x8.com/oauth?error="<>

client-beta.global.chalet.8x8.com web sitesinin mesajı

1

Tamam

参考来源:

<https://censys.io/>

<https://crt.sh/>
<https://www.virustotal.com/gui/home/search>
<https://dnsdumpster.com/>
<https://github.com/aboul3la/Sublist3r>
<https://github.com/tomnomnom/assetfinder/releases>
<https://github.com/infosec-au/altdns>
<https://github.com/darkoperator/dnsrecon>
https://en.wikipedia.org/wiki/Certificate_authority
<https://blog.appsecco.com/certificate-transparency-the-bright-side-and-the-dark-side-8aa47d9a6616>
<https://docs.google.com/presentation/d/1PCnjzCekIOeGMoWiE2IUzIRGOBxNp8K5hLQuvBNzrFY/edit>
<https://github.com/appsecco/bugcrowd-levelup-subdomain-enumeration>
<https://blog.appsecco.com/open-source-intelligence-gathering-101-d2861d4429e3>
<https://www.databreaches.net/hackers-post-450k-credentials-apparently-pilfered-from-yahoo/>
<http://info.menandmice.com/blog/bid/73645/Take-your-DNSSEC-with-a-grain-of-salt>
<https://hakin9.org/a-penetration-testers-guide-to-subdomain-enumeration/>
<https://medium.com/@gguzelkokar.mdbf15/get-reflected-xss-within-3-minutes-baa314e25489>
<https://www.peerlyst.com/posts/bsideslv-2017-breaking-ground-with-underflow-bsides-las-vegas>
<https://github.com/appsecco/the-art-of-subdomain-enumeration>
<https://github.com/blechschmidt/massdns>
<https://github.com/christophetd/censys-subdomain-finder>
<https://github.com/0xbharath/censys-enumeration>
<https://tools.ietf.org/html/rfc1930>
[https://en.wikipedia.org/wiki/Autonomous_system_\(Internet\)](https://en.wikipedia.org/wiki/Autonomous_system_(Internet))
<https://www.iana.org/assignments/as-numbers/as-numbers.xhtml>
<https://asn.cymru.com/cgi-bin/whois.cgi>
<https://www.ultratools.com/tools/asnInfo>
<https://nmap.org/nsedoc/scripts/targets-asn.html>