
0x00. dnsenum简介

dnsenum

是一款非常强大的域名信息收集工具。它的目的是尽可能多的收集一个域的信息，能够通过谷歌或者字典文件猜测可能存在的域名，以及对一个网段进行反向查 record（邮件交换记录），在域名服务器上执行axfr请求，通过谷歌脚本得到扩展域名信息（google hacking），提取自域名并查询，计算C类地址并执行whois查询，执行反向查询，把地址段写入文件等。

语法基础：

dnsenum sina.com.cn

dnsenum sina.com.cn -f /usr/share/dnsenum/dns.txt

指定字典爆破子域

dnsenum sina.com.cn --enum

参数：

--dnsserver 8.8.8.8 指定DNS server

--enum 指定线程5，使用谷歌查询，进行whois查询

--noreverse 跳过反向域名查询

--threads 指定线程

-f dns.txt 指定域名爆破字典

-w 进行whois查询

-o report.xml 输出XML格式的文件

```

root@kali:~# dnsenum sina.com.cn -f /usr/share/dnsenum/dns.txt
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

-----  sina.com.cn  -----

Host's addresses:
-----
sina.com.cn.          134      IN      A       202.108.33.107
sina.com.cn.          134      IN      A       202.108.33.60

Name Servers:
-----
ns1.sina.com.cn.      54575    IN      A       202.106.184.166
ns4.sina.com.cn.      54584    IN      A       121.14.1.22
ns2.sina.com.cn.      54576    IN      A       61.172.201.254
ns3.sina.com.cn.      54578    IN      A       123.125.29.99

Mail (MX) Servers:
-----
freemx1.sinamail.sina.com.cn. 85      IN      A       60.28.113.250
freemx2.sinamail.sina.com.cn. 1487    IN      A       180.149.134.158
freemx3.sinamail.sina.com.cn. 101     IN      A       60.28.113.250

```

0x01. dnsrecon简介

dns是最主要的服务暴露信息来源，我们可以根据dns域名收集以下信息：

- 发现开放端口的主机
- 发现子域及开放端口
- DNS域名注册信息
- DNS服务器区域传输

语法基础：

dnsrecon -d sina.com.cn

基本的SOA、NS、A、AAAA、MX、SRV查询

dnsrecon -r 60.28.2.0/24

反向PTR查询域名

dnsrecon -a -d sina.com.cn

标准加axfr区域传输

dnsrecon -w -d sina.com.cn

标准加whois查询

dnsrecon -g -d sina.com.cn

标准加google

```
dnsrecon -D dictionary.txt sina.com.cn
```

字典爆破主机和子域名

```
dnsrecon -z -d weberdns.de
```

当域启动DNSSEC，对于缺乏防护的DNS服务器，可以利用NSEC记录获取区域内全部记录，无需爆破

参数：

-t brt 使用内建字典

-t std 默认的标准查询

-t srv 只查srv记录（AD、voip电话）

-t axfr 标准加axfr记录（-a）

-t tld 删除并尝试所有顶级域名(IANA)

--threads 指定线程数

```
Applications ▾ Places ▾ Terminal ▾ Sat 00:07
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dnsrecon -d sina.com.cn
[*] Performing General Enumeration of Domain: sina.com.cn
[*] Checking for Zone Transfer for sina.com.cn name servers
[*] Resolving SOA Record
[+] SOA ns1.sina.com.cn 202.106.184.166
[*] Resolving NS Records
[*] NS Servers found:
[*] NS ns4.sina.com.cn 121.14.1.22
[*] NS ns2.sina.com.cn 61.172.201.254
[*] NS ns3.sina.com.cn 123.125.29.99
[*] NS ns1.sina.com.cn 202.106.184.166
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 121.14.1.22
[+] 121.14.1.22 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
[*]
[*] Trying NS server 202.106.184.166
[-] Zone Transfer Failed for 202.106.184.166!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 123.125.29.99
[+] 123.125.29.99 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
[*]
[*] Trying NS server 61.172.201.254
[+] 61.172.201.254 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
[*] Checking for Zone Transfer for sina.com.cn name servers
[*] Resolving SOA Record
[+] SOA ns1.sina.com.cn 202.106.184.166
[*] Resolving NS Records
[*] NS Servers found:
[*] NS ns1.sina.com.cn 202.106.184.166
[*] NS ns4.sina.com.cn 121.14.1.22
[*] NS ns2.sina.com.cn 61.172.201.254
[*] NS ns3.sina.com.cn 123.125.29.99
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 121.14.1.22
[+] 121.14.1.22 Has port 53 TCP Open
```

0x02. dnswalk 简介

基础语法：

```
dnswalk -radmilF sina.com.cn
```

参数：

-r #对指定域名的子域进行递归查询

-a #发现重复的A记录发出告警

-d #将调试状态信息输出到stderr

-m #仅检查上次运行后发生变化的记录

- F #检查PTR记录IP是否与对应A记录相符
- i #不检查域名中的无效字符
- l #检查区域文件中NS记录主机是否能返回正确的应答

0x03. dnstracer 简介

dnstracer 是用于追踪DNF查询请求的，可以从根域->目标域一步一步迭代查看查询请求。

基础语法：

dnstracer -co4 -s . www.baidu.com

参数：

- c #不使用本地缓存
- o #只显示查询简介
- 4 #不进行IPv6查询
- s . #指定初始查询的服务器是根域

```
root@kali:~# dnstracer -co4 -s . times0ng.github.io
Tracing to times0ng.github.io[a] via A.ROOT-SERVERS.NET, maximum of 3 retries
A.ROOT-SERVERS.NET [.] (198.41.0.4)
| \___ c0.nic.io [io] (2a01:8840:00a0:0000:0000:0000:0000:0017) Not queried
| \___ c0.nic.io [io] (65.22.162.17)
| \___ ns-1339.awsdns-39.org [github.io] (205.251.197.59) Got authoritative answer [received type is cname]
| \___ ns-1339.awsdns-39.org [github.io] (2600:9000:5305:3b00:0000:0000:0000:0001) Not queried
| \___ ns-692.awsdns-22.net [github.io] (205.251.194.180) Got authoritative answer [received type is cname]
| \___ ns-692.awsdns-22.net [github.io] (2600:9000:5302:b400:0000:0000:0000:0001) Not queried
| \___ ns1.p16.dynect.net [github.io] (208.78.70.16) Got authoritative answer [received type is cname]
| \___ ns1.p16.dynect.net [github.io] (2001:0500:0090:0001:0000:0000:0000:0016) Not queried
| \___ ns-1622.awsdns-10.co.uk [github.io] (205.251.198.86) Got authoritative answer [received type is cname]
| \___ ns-1622.awsdns-10.co.uk [github.io] (2600:9000:5306:5600:0000:0000:0000:0001) Not queried
| \___ ns2.p16.dynect.net [github.io] (204.13.250.16) Got authoritative answer [received type is cname]
| \___ ns-a3.io [io] (74.116.178.1)
| \___ ns-1622.awsdns-10.co.uk [github.io] (205.251.198.86) Got authoritative answer [received type is cname]
| \___ ns-1622.awsdns-10.co.uk [github.io] (2600:9000:5306:5600:0000:0000:0000:0001) Not queried
| \___ ns-1339.awsdns-39.org [github.io] (205.251.197.59) Got authoritative answer [received type is cname]
| \___ ns-1339.awsdns-39.org [github.io] (2600:9000:5305:3b00:0000:0000:0000:0001) Not queried
| \___ ns-692.awsdns-22.net [github.io] (205.251.194.180) Got authoritative answer [received type is cname]
| \___ ns-692.awsdns-22.net [github.io] (2600:9000:5302:b400:0000:0000:0000:0001) Not queried
| \___ ns2.p16.dynect.net [github.io] (204.13.250.16) Got authoritative answer [received type is cname]
| \___ ns1.p16.dynect.net [github.io] (208.78.70.16) Got authoritative answer [received type is cname]
| \___ ns1.p16.dynect.net [github.io] (2001:0500:0090:0001:0000:0000:0000:0016) Not queried
| \___ ns-a1.io [io] (2001:0678:0004:0000:0000:0000:0000:0001) Not queried
| \___ ns-a1.io [io] (194.0.1.1)
| \___ ns-1622.awsdns-10.co.uk [github.io] (205.251.198.86) Got authoritative answer [received type is cname]
| \___ ns-1622.awsdns-10.co.uk [github.io] (2600:9000:5306:5600:0000:0000:0000:0001) Not queried
| \___ ns-1339.awsdns-39.org [github.io] (205.251.197.59) Got authoritative answer [received type is cname]
| \___ ns-1339.awsdns-39.org [github.io] (2600:9000:5305:3b00:0000:0000:0000:0001) Not queried
| \___ ns-692.awsdns-22.net [github.io] (205.251.194.180) Got authoritative answer [received type is cname]
| \___ ns-692.awsdns-22.net [github.io] (2600:9000:5302:b400:0000:0000:0000:0001) Not queried
| \___ ns2.p16.dynect.net [github.io] (204.13.250.16) Got authoritative answer [received type is cname]
| \___ ns1.p16.dynect.net [github.io] (208.78.70.16) Got authoritative answer [received type is cname]
| \___ ns1.p16.dynect.net [github.io] (2001:0500:0090:0001:0000:0000:0000:0016) Not queried
| \___ a2.nic.io [io] (2a01:8840:00a1:0000:0000:0000:0000:0017) Not queried
| \___ a2.nic.io [io] (65.22.163.17)
| \___ ns2.p16.dynect.net [github.io] (204.13.250.16) Got authoritative answer [received type is cname]
| \___ ns-1622.awsdns-10.co.uk [github.io] (205.251.198.86) Got authoritative answer [received type is cname]
| \___ ns-1622.awsdns-10.co.uk [github.io] (2600:9000:5306:5600:0000:0000:0000:0001) Not queried
| \___ ns-1339.awsdns-39.org [github.io] (205.251.197.59) Got authoritative answer [received type is cname]
| \___ ns-1339.awsdns-39.org [github.io] (2600:9000:5305:3b00:0000:0000:0000:0001) Not queried
```

点击收藏 | 0 关注 | 0

[上一篇：SNMP协议攻击](#) [下一篇：hping3数据包定制](#)

1. 2 条回复



[33715****@qq.com](#) 2017-11-17 14:17:40

但是谷歌访问不了

0 回复Ta



[haorenx](#) 2018-07-25 09:00:39

可以利用网站服务进行查询：https://github.com/haorenx/SDL-Tools/blob/master/sub_domain.py
皮一下 <http://35.231.125.239/t1.htm>

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)