

Dnsenum

dnsenum是一款非常强大的 域名信息收集工具，它是由参与backtrack 开发项目的程序员所设计，设计者名叫Fillp (barbsie) Waeythens，该名开发者是一个精通web渗透测试的安全人员，并对DNS信息收集有着非常丰富的经验。

二，基本参数及命令 (中英对照)

dnsenum VERSION:1.2.6

dnsenum版本： 1.2.6

Usage: dnsenum [Options]

用法：dnsenum[选项]

[Options]:

[选项]:

Note: If no -f tag supplied will default to /usr/share/dnsenum/dns.txt or

注意：如果没有提供-f标记，则默认为/usr/share/dnsenum/dns.txt或

the dns.txt file in the same directory as dnsenum.pl

dnsenum.pl所在目录中的dns.txt文件

GENERAL OPTIONS:

一般选项：

--dnsserver

--dnsserver

Use this DNS server for A, NS and MX queries.

使用此DNS服务器进行A、NS和MX查询。

--enum Shortcut option equivalent to --threads 5 -s 15 -w.

--枚举快捷方式选项等效于--threads 5-s 15-w。

-h, --help Print this help message.

-h、 --帮助打印此帮助消息。

--noreverse Skip the reverse lookup operations.

--noreverse跳过反向查找操作。

--nocolor Disable ANSIColor output.

--nocolor禁用ANSIColor输出。

--private Show and save private ips at the end of the file domain_ips.txt.

--在文件domain_ips.txt的末尾显示和保存私有IP。

--subfile Write all valid subdomains to this file.

--子文件将所有有效子域写入此文件。

-t, --timeout The tcp and udp timeout values in seconds (default: 10s).

-t、 --timeouttcp和udp超时值（秒）（默认值：10s）。

--threads The number of threads that will perform different queries.

--threads将执行不同查询的线程数。

-v, --verbose Be verbose: show all the progress and all the error messages.

-v、 --verbose Be verbose：显示所有进度和所有错误消息。

GOOGLE SCRAPING OPTIONS:

谷歌抓取选项：

-p, --pages The number of google search pages to process when scraping names,

-p、 --pages抓取名称时要处理的谷歌搜索页面数，

the default is 5 pages, the -s switch must be specified.

默认值为5页，必须指定-s开关。

-s, --scrap The maximum number of subdomains that will be scraped from Google (default 15).

-s、 --scrap将从Google中删除的最大子域数（默认值为15）。

BRUTE FORCE OPTIONS:

暴力选项：

-f, --file Read subdomains from this file to perform brute force. (Takes priority over default dns.txt)

-f、 --file从该文件读取子域以执行暴力。（优先于默认dns.txt）

-u, --update <a|g|r|z>

-u、 --更新<a | g | r | z>

Update the file specified with the -f switch with valid subdomains.

用有效的子域更新用-f开关指定的文件。

a (all) Update using all results.

使用所有结果进行（全部）更新。

g Update using only google scraping results.

g只使用谷歌抓取结果更新。

r Update using only reverse lookup results.

r只使用反向查找结果进行更新。

z Update using only zonetransfer results.

z仅使用区域传输结果进行更新。

-r, --recursion Recursion on subdomains, brute force all discovered subdomains that have an NS record.

-r、 --子域递归递归，强制所有发现的有NS记录的子域。

WHOIS NETRANGE OPTIONS:

WHOIS NETRANGE选项：

-d, --delay The maximum value of seconds to wait between whois queries, the value is defined randomly, default: 3s.

-d、 --delaywhois查询之间等待的最大秒数，该值是随机定义的，默认为3s。

-w, --whois Perform the whois queries on c class network ranges.

-w、 --whois在c类网络范围上执行whois查询。

Warning: this can generate very large netranges and it will take lot of time to perform reverse lookups.

警告：这可能会生成非常大的网络范围，执行反向查找需要很多时间。

REVERSE LOOKUP OPTIONS:

反向查找选项：

-e, --exclude

-e、--排除

Exclude PTR records that match the regexp expression from reverse lookup results, useful on invalid hostnames.

从反向查找结果中排除与regexp表达式匹配的PTR记录，这对无效主机名很有用。

OUTPUT OPTIONS:

输出选项：

-o --output Output in XML format. Can be imported in MagicTree (www.gremwell.com)

-o——输出XML格式的输出。可在MagicTree (www.gremwell.com) 中导入

三，命令范例

dnsenum --dnsserver 8.8.8.8 zsdk.org.cn

指定DNS 8.8.8.8 服务器对zsdk.org.cn进行查询

4	5.022017179	192.168.0.103	8.8.8.8	DNS	71	Standard que
5	5.201337100	8.8.8.8	192.168.0.103	DNS	87	Standard que
6	5.203137534	192.168.0.103	8.8.8.8	DNS	84	Standard que
7	5.434622212	8.8.8.8	192.168.0.103	DNS	148	Standard que
8	5.439198759	192.168.0.103	8.8.8.8	DNS	71	Standard que
9	5.661654958	8.8.8.8	192.168.0.103	DNS	122	Standard que
10	5.663866823	192.168.0.103	8.8.8.8	DNS	77	Standard que

```
[root@parrot] ~/home/kun
#dnsenum --dnsserver 8.8.8.8 zsdk.org.cn
dnsenum VERSION:1.2.6

----- zsdk.org.cn -----

Host's addresses:
-----
zsdk.org.cn.                599      IN      A       47.240.42.2

Name Servers:
-----
dns16.hichina.com.         3599     IN      A       106.11.211.66
dns16.hichina.com.         3599     IN      A       106.11.211.56
dns16.hichina.com.         3599     IN      A       106.11.141.126
dns16.hichina.com.         3599     IN      A       106.11.141.116
dns16.hichina.com.         3599     IN      A       140.205.41.26
dns16.hichina.com.         3599     IN      A       140.205.41.16
dns16.hichina.com.         3599     IN      A       140.205.81.26
dns16.hichina.com.         3599     IN      A       140.205.81.16
dns15.hichina.com.         3599     IN      A       106.11.211.65
dns15.hichina.com.         3599     IN      A       106.11.211.55
dns15.hichina.com.         3599     IN      A       106.11.141.125
dns15.hichina.com.         3599     IN      A       106.11.141.115
dns15.hichina.com.         3599     IN      A       140.205.41.25
dns15.hichina.com.         3599     IN      A       140.205.41.15
dns15.hichina.com.         3599     IN      A       140.205.81.25
dns15.hichina.com.         3599     IN      A       140.205.81.15
```

dnsenum -w zsdk.org.cn
在c类网络范围上执行whois查询

```
dns16.hichina.com.      2785      IN      A      106.11.141.116
dns16.hichina.com.      2785      IN      A      106.11.141.126
dns16.hichina.com.      2785      IN      A      106.11.211.56
dns16.hichina.com.      2785      IN      A      106.11.211.66
dns16.hichina.com.      2785      IN      A      140.205.41.16
dns16.hichina.com.      2785      IN      A      140.205.41.26
dns15.hichina.com.      172442    IN      A      140.205.81.15
dns15.hichina.com.      172442    IN      A      140.205.81.25
dns15.hichina.com.      172442    IN      A      106.11.141.115
dns15.hichina.com.      172442    IN      A      106.11.141.125
dns15.hichina.com.      172442    IN      A      106.11.211.55
dns15.hichina.com.      172442    IN      A      106.11.211.65
dns15.hichina.com.      172442    IN      A      140.205.41.15
dns15.hichina.com.      172442    IN      A      140.205.41.25

Mail (MX) Servers:
-----

mxbiz2.qq.com.          383       IN      A      183.57.48.34
mxbiz1.qq.com.          600       IN      A      183.57.48.34
```

dnsenum -g zsdk.org.cn
仅是用谷歌炸抓取搜索结果

```
dnsenum VERSION:1.2.6
Unknown option: g

-----  zsdk.org.cn  -----

Host's addresses:
-----

zsdk.org.cn.            600       IN      A      47.240.42.2

Name Servers:
-----

dns16.hichina.com.      2168      IN      A      140.205.41.16
dns16.hichina.com.      2168      IN      A      140.205.41.26
dns16.hichina.com.      2168      IN      A      140.205.81.16
dns16.hichina.com.      2168      IN      A      140.205.81.26
dns16.hichina.com.      2168      IN      A      106.11.141.116

35 65.759077311 192.168.0.103 8.8.8.8 DNS 71 Standard que
36 66.013590449 8.8.8.8 192.168.0.103 DNS 87 Standard que
37 66.015443505 192.168.0.103 8.8.8.8 DNS 84 Standard que
38 66.107018964 8.8.8.8 192.168.0.103 DNS 148 Standard que
```

dnsenum -r zsdk.org.cn

仅发现所有子域所有NS信息。

```
[root@parrot]~[/home/kun]
#dnsenum -r zsdk.org.cn
dnsenum VERSION:1.2.6
```

----- zsdk.org.cn -----

Host's addresses:

zsdk.org.cn.	600	IN	A	47.240.42.2
--------------	-----	----	---	-------------

Name Servers:

dns16.hichina.com.	145	IN	A	106.11.211.56
dns16.hichina.com.	145	IN	A	106.11.211.66
dns16.hichina.com.	145	IN	A	140.205.41.16
dns16.hichina.com.	145	IN	A	140.205.41.26

dnsenum --delay 6 zsdk.org.cn

whois查询时间等待最大秒数不得超过3s，Dnsenum默认的等待值也是3s。

494 108.789274800 202.96.128.166	192.168.0.103	DNS	139 Standard query response 0x3832 No such name A 607.zsdk.org.cn SOA dns15.hichina.com
495 108.790756258 192.168.0.103	202.96.128.166	DNS	75 Standard query 0x56fb A 616.zsdk.org.cn
496 108.799522489 202.96.128.166	192.168.0.103	DNS	139 Standard query response 0x56fb No such name A 616.zsdk.org.cn SOA dns15.hichina.com
497 108.800413400 192.168.0.103	202.96.128.166	DNS	75 Standard query 0xa488 A 624.zsdk.org.cn
498 108.836238940 202.96.128.166	192.168.0.103	DNS	139 Standard query response 0xa488 No such name A 624.zsdk.org.cn SOA dns15.hichina.com
499 108.837473133 192.168.0.103	202.96.128.166	DNS	75 Standard query 0xdd65 A 625.zsdk.org.cn
500 108.846690080 202.96.128.166	192.168.0.103	DNS	139 Standard query response 0xdd65 No such name A 625.zsdk.org.cn SOA dns15.hichina.com
501 108.847787958 192.168.0.103	202.96.128.166	DNS	75 Standard query 0x7b72 A 629.zsdk.org.cn
502 108.883322632 202.96.128.166	192.168.0.103	DNS	139 Standard query response 0x7b72 No such name A 629.zsdk.org.cn SOA dns15.hichina.com
503 108.884615116 192.168.0.103	202.96.128.166	DNS	75 Standard query 0x73f2 A 630.zsdk.org.cn
504 108.922517139 202.96.128.166	192.168.0.103	DNS	139 Standard query response 0x73f2 No such name A 630.zsdk.org.cn SOA dns15.hichina.com
505 108.923913518 192.168.0.103	202.96.128.166	DNS	75 Standard query 0xd4cd A 648.zsdk.org.cn
506 108.932528956 202.96.128.166	192.168.0.103	DNS	139 Standard query response 0xd4cd No such name A 648.zsdk.org.cn SOA dns15.hichina.com
507 108.933701084 192.168.0.103	202.96.128.166	DNS	75 Standard query 0x9cdc A 664.zsdk.org.cn
508 108.942432760 202.96.128.166	192.168.0.103	DNS	139 Standard query response 0x9cdc No such name A 664.zsdk.org.cn SOA dns15.hichina.com
509 108.943522103 192.168.0.103	202.96.128.166	DNS	75 Standard query 0xefff A 669.zsdk.org.cn
510 108.978561438 202.96.128.166	192.168.0.103	DNS	139 Standard query response 0xefff No such name A 669.zsdk.org.cn SOA dns15.hichina.com
511 108.980054258 192.168.0.103	202.96.128.166	DNS	74 Standard query 0x093e A 67.zsdk.org.cn
642 109.014610636 202.96.128.166	192.168.0.103	DNS	139 Standard query response 0x093e No such name A 67.zsdk.org.cn SOA dns15.hichina.com

```
2
[3]+ Stopped dnsenum -delay 6 zsdk.org.cn
[~][x]-[root@parrot]~[/home/kun]
```

[illegible]

```

Name Servers:
-----
dns16.hichina.com.      172139  IN      A        140.205.41.16
dns16.hichina.com.      172139  IN      A        140.205.41.26
dns16.hichina.com.      172139  IN      A        140.205.81.16
dns16.hichina.com.      172139  IN      A        140.205.81.26
dns16.hichina.com.      172139  IN      A        106.11.141.116
dns16.hichina.com.      172139  IN      A        106.11.141.126
dns16.hichina.com.      172139  IN      A        106.11.211.56
dns16.hichina.com.      172139  IN      A        106.11.211.66
dns15.hichina.com.      172356  IN      A        140.205.41.15
dns15.hichina.com.      172356  IN      A        140.205.41.25
dns15.hichina.com.      172356  IN      A        140.205.81.15
dns15.hichina.com.      172356  IN      A        140.205.81.25
dns15.hichina.com.      172356  IN      A        106.11.141.115
dns15.hichina.com.      172356  IN      A        106.11.141.125
dns15.hichina.com.      172356  IN      A        106.11.211.55
dns15.hichina.com.      172356  IN      A        106.11.211.65

Mail (MX) Servers:
-----
mxbiz1.qq.com.          362     IN      A        183.57.48.34
mxbiz2.qq.com.          600     IN      A        183.57.48.34

Trying Zone Transfers and getting Bind Versions:
-----

Trying Zone Transfer for zsdk.org.cn on dns15.hichina.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for zsdk.org.cn on dns16.hichina.com ...
AXFR record query failed: corrupt packet

Brute forcing with /usr/share/dnsenum/dns.txt:
-----

www.zsdk.org.cn.         600     IN      A        47.240.42.2

zsdk.org.cn class C netranges:
-----

47.240.42.0/24

Performing reverse lookup on 256 ip addresses:
-----

0 results out of 256 IP addresses.

zsdk.org.cn ip blocks:
-----

done.
└─[root@parrot]-[/home/kun]

```

dnsenum --pages 5 zsdk.org.cn

抓取页面名称并处理，默认页面为5.

```
File Edit View Bookmarks Settings Help

Host's addresses:
-----

zsdk.org.cn.                600      IN      A       47.240.42.2

Name Servers:
-----

dns16.hichina.com.         172139   IN      A       140.205.41.16
dns16.hichina.com.         172139   IN      A       140.205.41.26
dns16.hichina.com.         172139   IN      A       140.205.81.16
dns16.hichina.com.         172139   IN      A       140.205.81.26
dns16.hichina.com.         172139   IN      A       106.11.141.116
dns16.hichina.com.         172139   IN      A       106.11.141.126
dns16.hichina.com.         172139   IN      A       106.11.211.56
dns16.hichina.com.         172139   IN      A       106.11.211.66
dns15.hichina.com.         172356   IN      A       140.205.41.15
dns15.hichina.com.         172356   IN      A       140.205.41.25
dns15.hichina.com.         172356   IN      A       140.205.81.15
dns15.hichina.com.         172356   IN      A       140.205.81.25
dns15.hichina.com.         172356   IN      A       106.11.141.115
dns15.hichina.com.         172356   IN      A       106.11.141.125
dns15.hichina.com.         172356   IN      A       106.11.211.55
dns15.hichina.com.         172356   IN      A       106.11.211.65

Mail (MX) Servers:
-----

mxbiz2.qq.com.             485      IN      A       183.57.48.34
mxbiz1.qq.com.             198      IN      A       183.57.48.34

Trying Zone Transfers and getting Bind Versions:
-----

Trying Zone Transfer for zsdk.org.cn on dns15.hichina.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for zsdk.org.cn on dns16.hichina.com ...
AXFR record query failed: corrupt packet

Brute forcing with /usr/share/dnsenum/dns.txt:
-----

www.zsdk.org.cn.           600      IN      A       47.240.42.2

zsdk.org.cn class C netranges:
-----

47.240.42.0/24

Performing reverse lookup on 256 ip addresses:
-----

0 results out of 256 IP addresses.

zsdk.org.cn ip blocks:
-----

done.
```

dnsenum --noreverse zsdk.org.cn

跳过反向查找操作扫描zsdk.org.cn [^反向操作法，
<https://baike.baidu.com/item/%E5%8F%8D%E5%90%91%E6%93%8D%E4%BD%9C%E6%B3%95/9207534>]

- 反向操作法

“反向操作法”一词常常出现在股市之中，其核心意思为“不受外界干扰”。