Fierce

feature是一款半轻量级扫描仪，有助于定位不连续的区域 指定域的IP空间和主机名。这真的意味着 作为nmap、unicornscan、nessus、nikto等的预游标，因为所有 其中要求您已经知道您正在查看的IP空间 为了。这不会执行攻击，也不会扫描整个 互联网不分青红皂白。它是专门用来定位的 公司网络内外的目标。因为它使用 主要是你会经常发现错误配置的网络泄漏 内部地址空间。这在有针对性的恶意软件中特别有.

作者

一，帮助手册

选项: -连接尝试与任何非RFC1918建立http连接 (公开)地址。这将输出返回头，但是 请注意，对于一家拥有 许多目标，取决于网络/机器滞后。我不会的 除非是一家小公司或者你有一个 你有很多空闲时间 (可能需要几个小时到几天)。 在指定的文件中，文本“主机:\n”将被替换 由指定的主机执行。用法:

example.com-连接头

-delay两次查找之间等待的秒数。 -dns您想要扫描的域。 DNS文件使用文件提供的DNS服务器(每行一个)，用于 反向查找(强力)。 -域名服务器使用特定的域名服务器进行反向查找 (可能应该是目标的DNS服务器)。凶猛的 将您的DNS服务器用于初始SOA查询，然后使用 默认情况下，目标的所有附加查询的DNS服务器。 -文件要输出以记录到的文件。 -fulloutput当与-connect结合时，这将输出所有内容 网络服务器发回的不仅仅是HTTP头。 -帮助这个屏幕。 -nopattern在附近搜索时不要使用搜索模式 主持人。相反抛弃一切。这真的很吵，但是 对于查找垃圾邮件发送者可能所在的其他域很有用 使用。它也会给你很多假阳性， 尤其是在大型领域。 -范围扫描内部知识产权范围(必须结合 -dnsserver)。请注意，这不支持模式 并将简单地输出它找到的任何东西。用法:

ns1.example.co地区111.222.333.0-255

-搜索搜索列表。当凶猛的尝试穿越 在ipspace中，它可能会遇到其他服务器中的其他服务器 可能属于同一公司的域。如果你提供一个 逗号分隔的列表将报告任何发现。 如果公司服务器被命名，这尤其有用 不同于面向公众的网站。用法:

examplecompany.com搜索公司

请注意，使用搜索还可以大大增加 找到了主机，因为一旦找到它，它将继续遍历 您在搜索列表中指定的服务器。越多 更好。 -抑制抑制所有TTY输出(与-file结合时)。 -t超时指定不同的超时时间(默认为10秒)。你们 如果您正在查询的DNS服务器 速度慢或网络滞后。 -线程指定扫描时要使用多少个线程(默认是单线程的)。 -遍历指定任意IP之上和之下的IP数量 找到了附近的入侵者。默认值为5以上 下面。遍历不会移动到其他的C块。 -版本输出版本号。 -在找到匹配项后，扫描整个C类 这将产生更多的流量 但是可以发现更多的信息。 -单词列表使用单独的单词列表(每行一个单词)。用法:

examplecompany.com

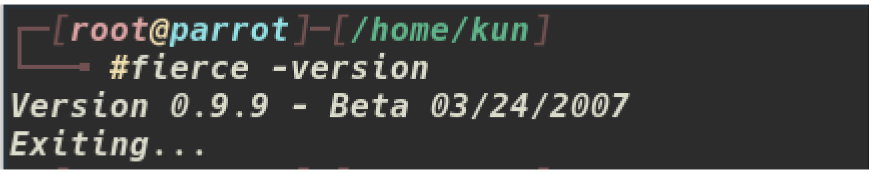
```
Options:
        -connect        Attempt to make http connections to any non RFC1918
                (public) addresses.  This will output the return headers but
                be warned, this could take a long time against a company with
        many targets, depending on network/machine lag.  I wouldn't
        recommend doing this unless it's a small company or you have a
        lot of free time on your hands (could take hours-days).
        Inside the file specified the text "Host:\n" will be replaced
        by the host specified. Usage:

perl fierce.pl -dns example.com -connect headers.txt

-delay          The number of seconds to wait between lookups.
-dns            The domain you would like scanned.
-dnsfile        Use DNS servers provided by a file (one per line) for
        reverse lookups (brute force).
-dnsserver      Use a particular DNS server for reverse lookups
        (probably should be the DNS server of the target).  Fierce
        uses your DNS server for the initial SOA query and then uses
        the target's DNS server for all additional queries by default.
-file           A file you would like to output to be logged to.
-fulloutput     When combined with -connect this will output everything
        the webserver sends back, not just the HTTP headers.
-help           This screen.
-nopattern      Don't use a search pattern when looking for nearby
        hosts.  Instead dump everything.  This is really noisy but
        is useful for finding other domains that spammers might be
        using.  It will also give you lots of false positives,
        especially on large domains.
-range          Scan an internal IP range (must be combined with
        -dnsserver).  Note, that this does not support a pattern
        and will simply output anything it finds.  Usage:

perl fierce.pl -range 111.222.333.0-255 -dnsserver ns1.example.co

-search         Search list.  When fierce attempts to traverse up and
        down ipspace it may encounter other servers within other
        domains that may belong to the same company.  If you supply a
        comma delimited list to fierce it will report anything found.
        This is especially useful if the corporate servers are named
        different from the public facing website.  Usage:

perl fierce.pl -dns examplecompany.com -search corpcompany,blahcompany

        Note that using search could also greatly expand the number of
        hosts found, as it will continue to traverse once it locates
        servers that you specified in your search list.  The more the
        better.
-suppress       Suppress all TTY output (when combined with -file).
-tcptimeout     Specify a different timeout (default 10 seconds).  You
        may want to increase this if the DNS server you are querying
        is slow or has a lot of network lag.
-threads  Specify how many threads to use while scanning (default
  is single threaded).
-traverse       Specify a number of IPs above and below whatever IP you
        have found to look for nearby IPs.  Default is 5 above and
        below.  Traverse will not move into other C blocks.
-version        Output the version number.
-wide           Scan the entire class C after finding any matching
        hostnames in that class C.  This generates a lot more traffic
        but can uncover a lot more information.
-wordlist       Use a seperate wordlist (one word per line).  Usage:
```

```
perl fierce.pl -dns examplecompany.com -wordlist dictionary.txt
```

二，命令实例

fierce -version

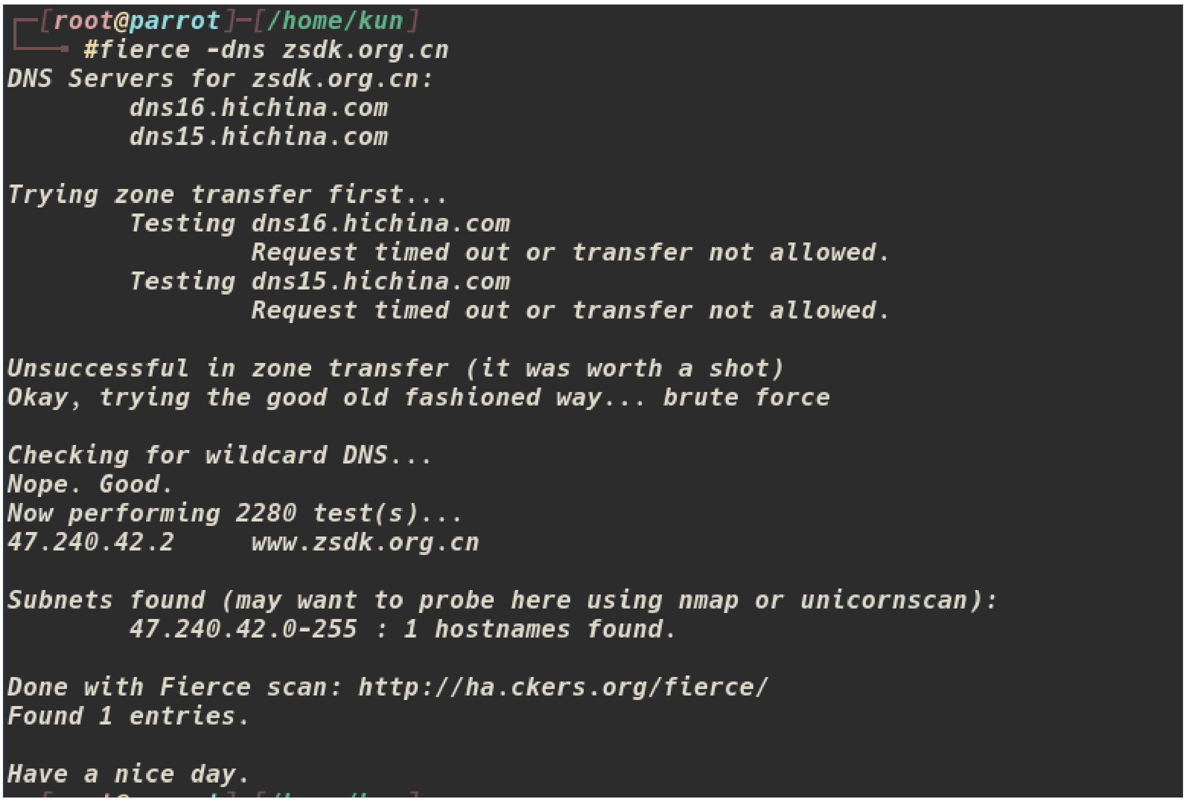
输出fierce版本号



```
┌─[root@parrot]─[/home/kun]
└──╼ #fierce -version
Version 0.9.9 - Beta 03/24/2007
Exiting...
```

fierce -dns zsdk.org.cn

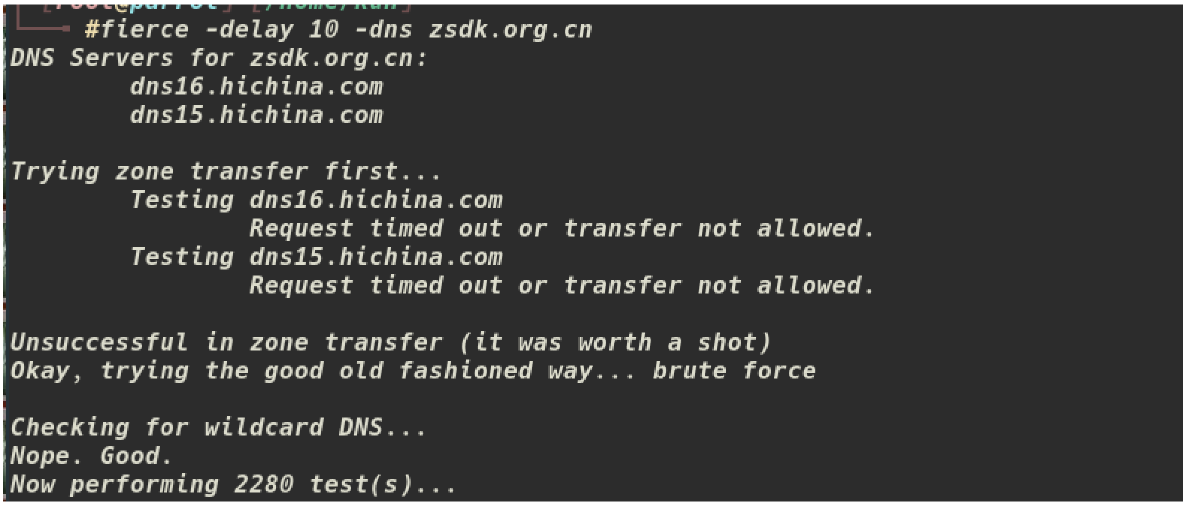
枚举zsdk.org.cn域名解析记录



```
┌─[root@parrot]─[/home/kun]
└──╼ #fierce -dns zsdk.org.cn
DNS Servers for zsdk.org.cn:
        dns16.hichina.com
        dns15.hichina.com

Trying zone transfer first...
        Testing dns16.hichina.com
                Request timed out or transfer not allowed.
        Testing dns15.hichina.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
47.240.42.2     www.zsdk.org.cn

Subnets found (may want to probe here using nmap or unicornscan):
        47.240.42.0-255 : 1 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 1 entries.

Have a nice day.
```

fierce -delay 10 -dns zsdk.org.cn

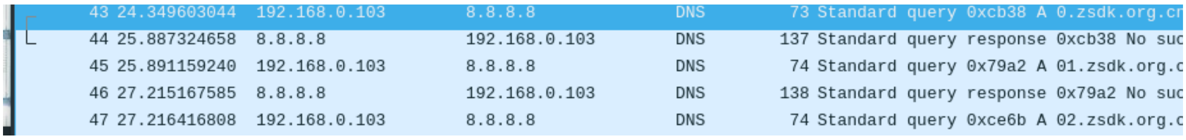
10秒后对zsdk.org.cn进行枚举[^时间根据所需而定]



```
    #fierce -delay 10 -dns zsdk.org.cn
DNS Servers for zsdk.org.cn:
        dns16.hichina.com
        dns15.hichina.com

Trying zone transfer first...
        Testing dns16.hichina.com
                Request timed out or transfer not allowed.
        Testing dns15.hichina.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
```

fierce -dnsserver 8.8.8.8 -dns zsdk.org.cn

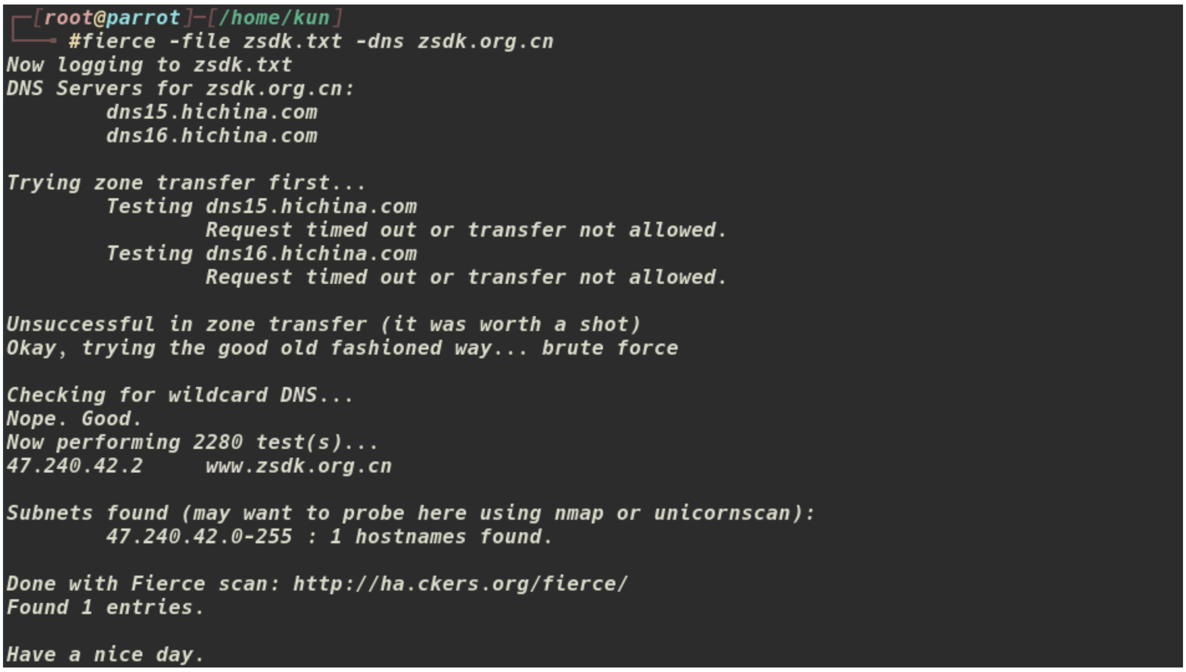
使用指定的DNS服务器对zsdk.org.cn进行反向查找



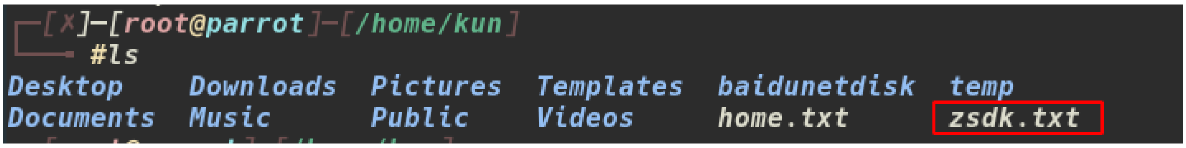
```
43 24.349603044  192.168.0.103   8.8.8.8          DNS    73 Standard query 0xcb38 A 0.zsdk.org.cn
44 25.887324658  8.8.8.8         192.168.0.103    DNS   137 Standard query response 0xcb38 No suc
45 25.891159240  192.168.0.103   8.8.8.8          DNS    74 Standard query 0x79a2 A 01.zsdk.org.c
46 27.215167585  8.8.8.8         192.168.0.103    DNS   138 Standard query response 0x79a2 No suc
47 27.216416808  192.168.0.103   8.8.8.8          DNS    74 Standard query 0xce6b A 02.zsdk.org.c
```

fierce -file -dns zsdk.org.cn

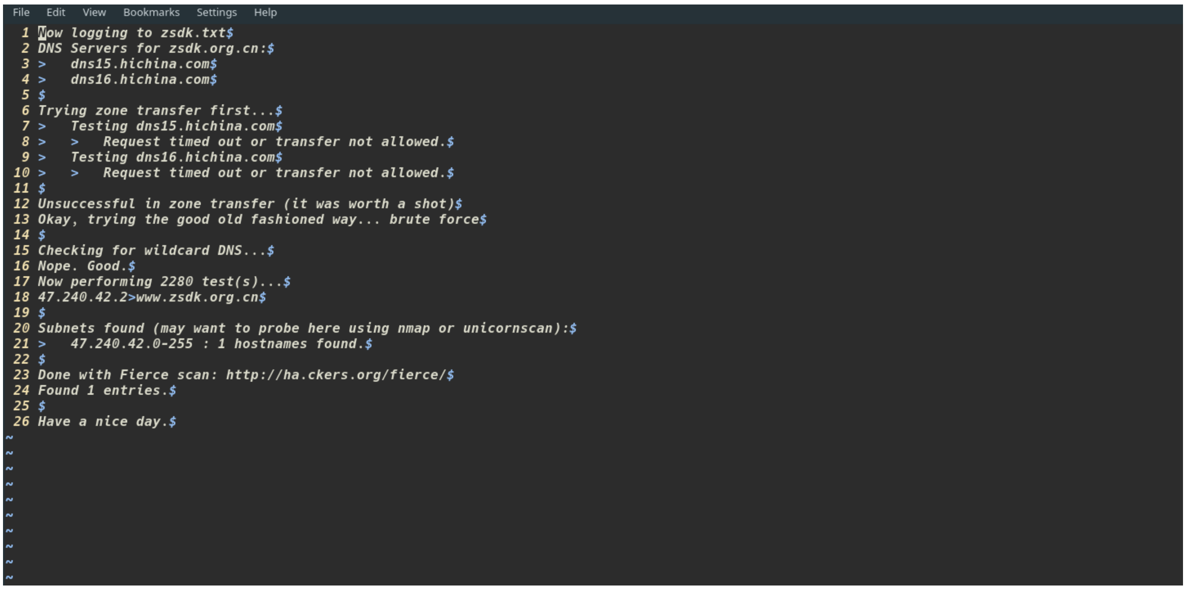
将枚举完后的结果导出至zsdk.txt



```
┌─[root@parrot]─[/home/kun]
└──╼ #fierce -file zsdk.txt -dns zsdk.org.cn
Now logging to zsdk.txt
DNS Servers for zsdk.org.cn:
        dns15.hichina.com
        dns16.hichina.com

Trying zone transfer first...
        Testing dns15.hichina.com
                Request timed out or transfer not allowed.
        Testing dns16.hichina.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
47.240.42.2     www.zsdk.org.cn

Subnets found (may want to probe here using nmap or unicornscan):
        47.240.42.0-255 : 1 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 1 entries.

Have a nice day.
```



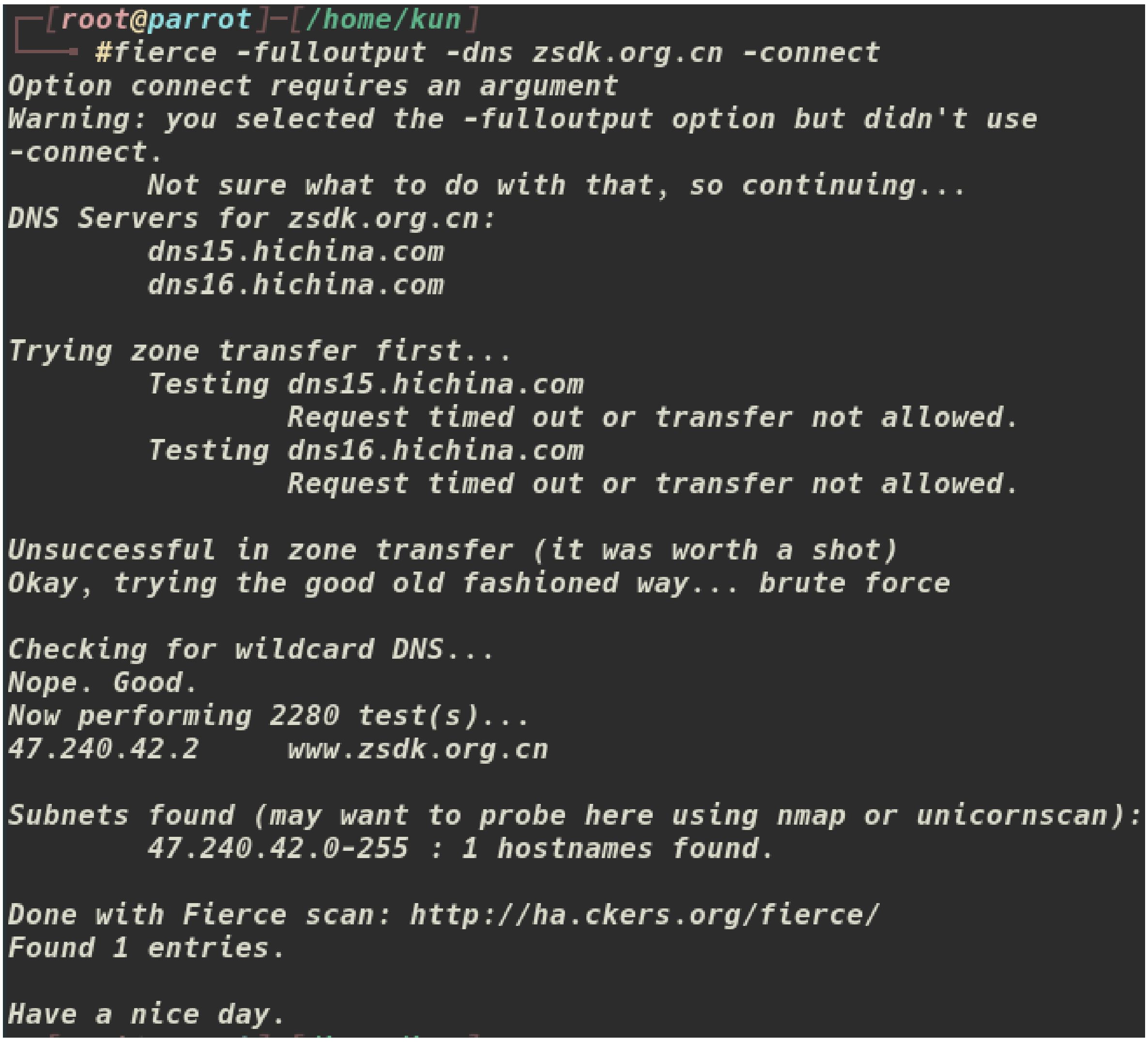
```
┌─[✗]─[root@parrot]─[/home/kun]
└──╼ #ls
Desktop    Downloads  Pictures  Templates  baidunetdisk  temp
Documents  Music      Public    Videos     home.txt      zsdk.txt
```



```
Now logging to zsdk.txt$
DNS Servers for zsdk.org.cn:$
>   dns15.hichina.com$
>   dns16.hichina.com$
$
Trying zone transfer first...$
>   Testing dns15.hichina.com$
>   >   Request timed out or transfer not allowed.$
>   Testing dns16.hichina.com$
>   >   Request timed out or transfer not allowed.$
$
Unsuccessful in zone transfer (it was worth a shot)$
Okay, trying the good old fashioned way... brute force$
$
Checking for wildcard DNS...$
Nope. Good.$
Now performing 2280 test(s)...$
47.240.42.2>www.zsdk.org.cn$
$
Subnets found (may want to probe here using nmap or unicornscan):$
>   47.240.42.0-255 : 1 hostnames found.$
$
Done with Fierce scan: http://ha.ckers.org/fierce/$
Found 1 entries.$
$
Have a nice day.$
~
~
~
~
~
~
~
~
~
~
```

fierce -fulloutput -dns zsdk.org.cn -connec

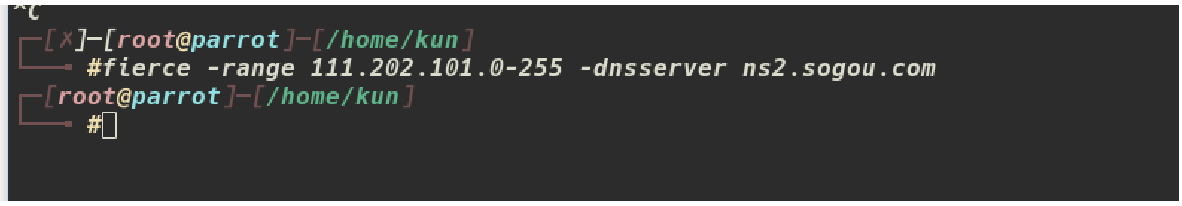
使用-fulloutput 和 -connect组合可以检索所有信息。



```
┌─[root@parrot]─[/home/kun]
└──╼ #fierce -fulloutput -dns zsdk.org.cn -connect
Option connect requires an argument
Warning: you selected the -fulloutput option but didn't use
-connect.
        Not sure what to do with that, so continuing...
DNS Servers for zsdk.org.cn:
        dns15.hichina.com
        dns16.hichina.com

Trying zone transfer first...
        Testing dns15.hichina.com
                Request timed out or transfer not allowed.
        Testing dns16.hichina.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
47.240.42.2     www.zsdk.org.cn

Subnets found (may want to probe here using nmap or unicornscan):
        47.240.42.0-255 : 1 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 1 entries.

Have a nice day.
```

fierce -range 110.202.101.0-255 -dnsserver ns2.sogou.com

-range 扫描的范围是110.202.101.0-255，-dnsserver列出枚举的所有结果[^当然我这个例子没有找到相应的信息]

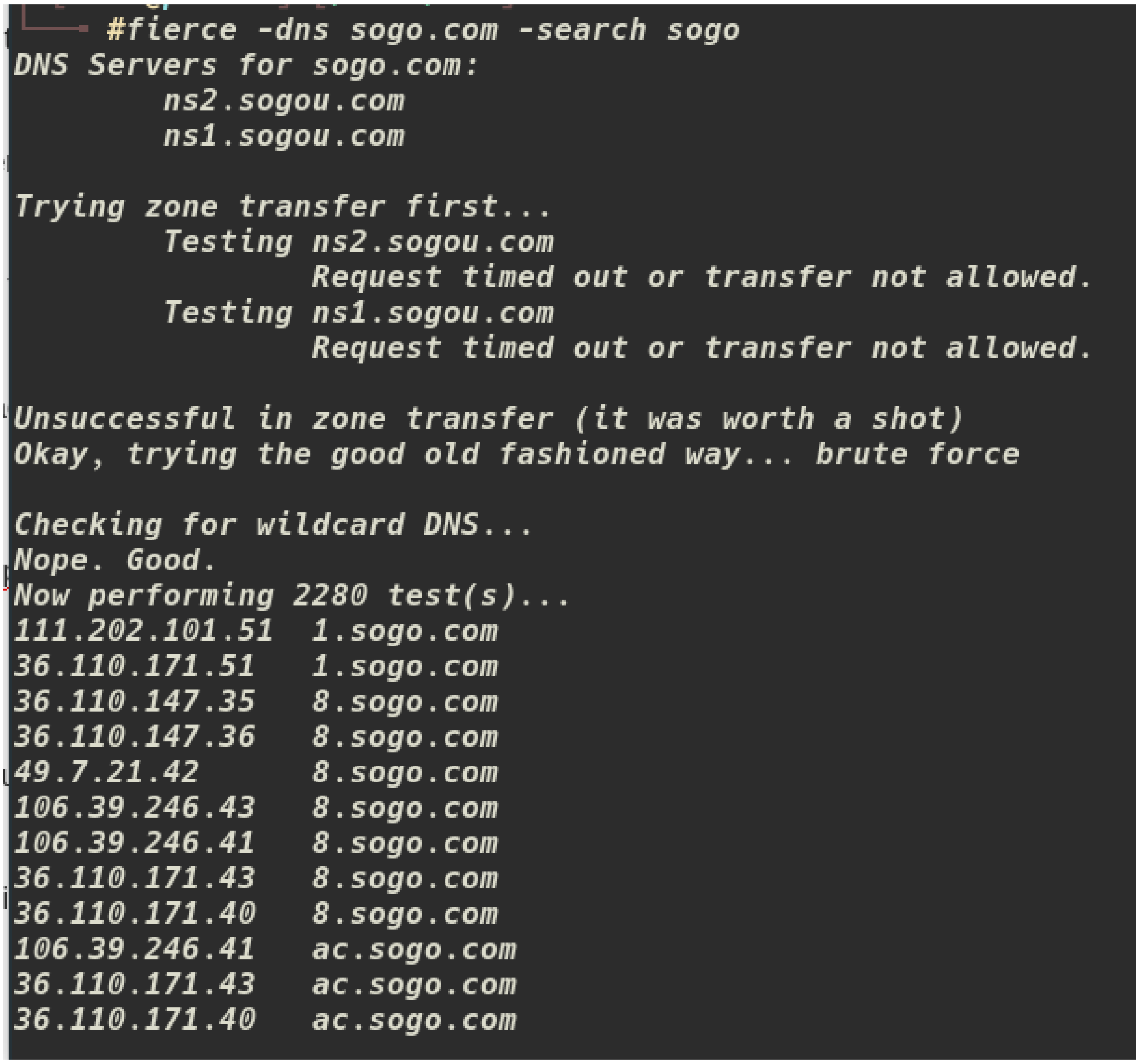


```
^C
┌─[✗]─[root@parrot]─[/home/kun]
└──╼ #fierce -range 111.202.101.0-255 -dnsserver ns2.sogou.com
┌─[root@parrot]─[/home/kun]
└──╼ #
```

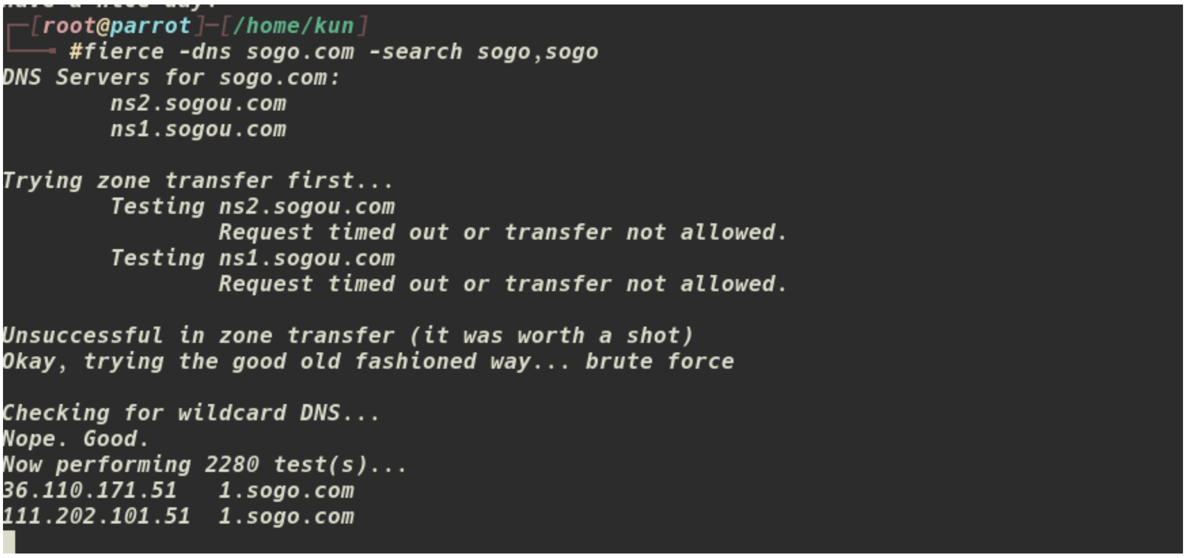
fierce -dns sogo.com -search sogo

搜索一个公司的所属域，可以使用“,”分割比如 sogo,sogo

> 使用此方法搜索和多的信息，因为他可以根据找到的主机，从而根据主机进行继续遍历。



```
└──╼ #fierce -dns sogo.com -search sogo
DNS Servers for sogo.com:
        ns2.sogou.com
        ns1.sogou.com

Trying zone transfer first...
        Testing ns2.sogou.com
                Request timed out or transfer not allowed.
        Testing ns1.sogou.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
111.202.101.51  1.sogo.com
36.110.171.51   1.sogo.com
36.110.147.35   8.sogo.com
36.110.147.36   8.sogo.com
49.7.21.42      8.sogo.com
106.39.246.43   8.sogo.com
106.39.246.41   8.sogo.com
36.110.171.43   8.sogo.com
36.110.171.40   8.sogo.com
106.39.246.41   ac.sogo.com
36.110.171.43   ac.sogo.com
36.110.171.40   ac.sogo.com
```

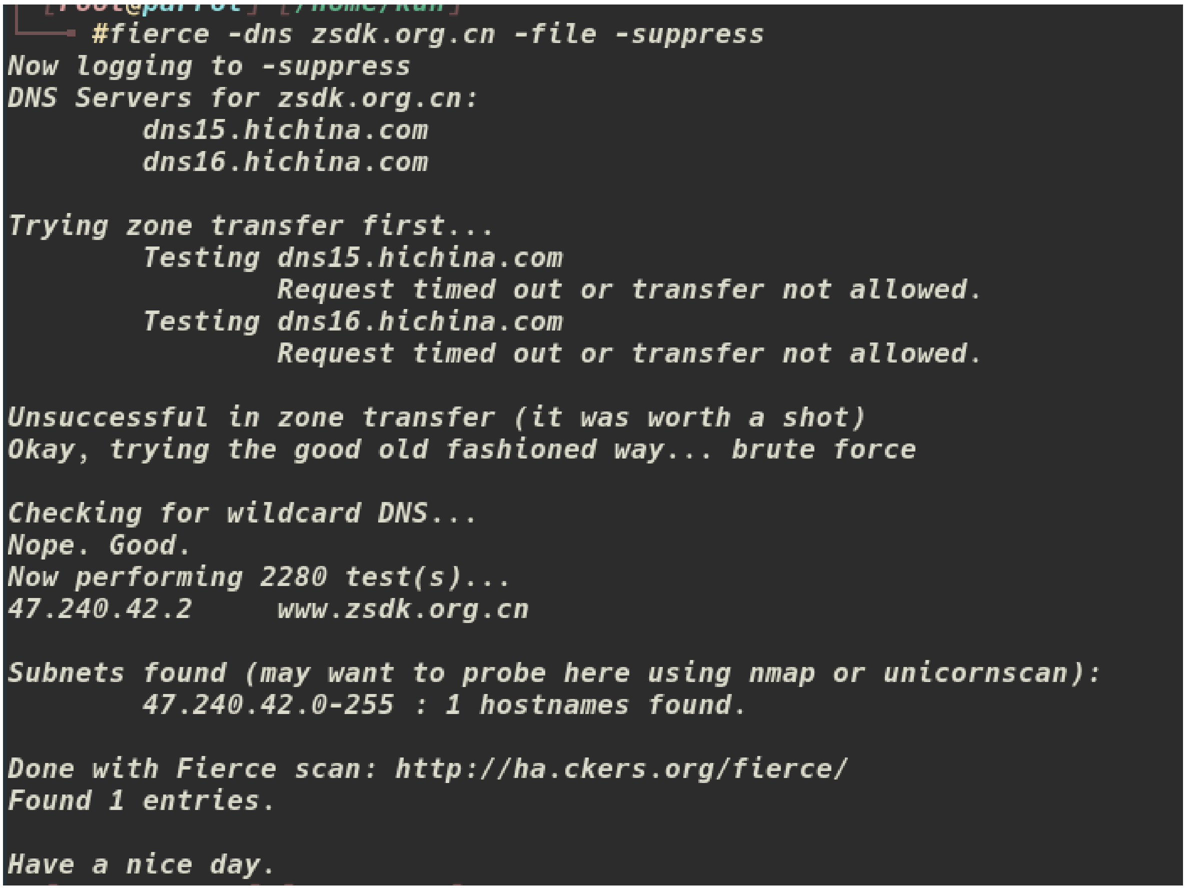


```
┌─[root@parrot]─[/home/kun]
└──╼ #fierce -dns sogo.com -search sogo,sogo
DNS Servers for sogo.com:
        ns2.sogou.com
        ns1.sogou.com

Trying zone transfer first...
        Testing ns2.sogou.com
                Request timed out or transfer not allowed.
        Testing ns1.sogou.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
36.110.171.51   1.sogo.com
111.202.101.51  1.sogo.com
```

fierce -dns zsdk.org.cn -file -suppress

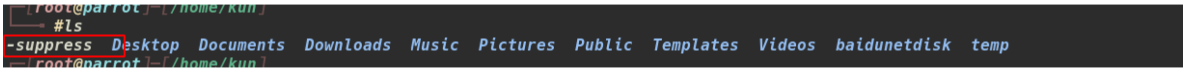
"-suppress"与""-file" 相结合时将会禁止TTY输出。

> TTY（TeleTYpe）设备包括虚拟控制台，串口以及伪终端设备。
>
> 可以理解为你扫描出来的信息不会出现在你的终端上。

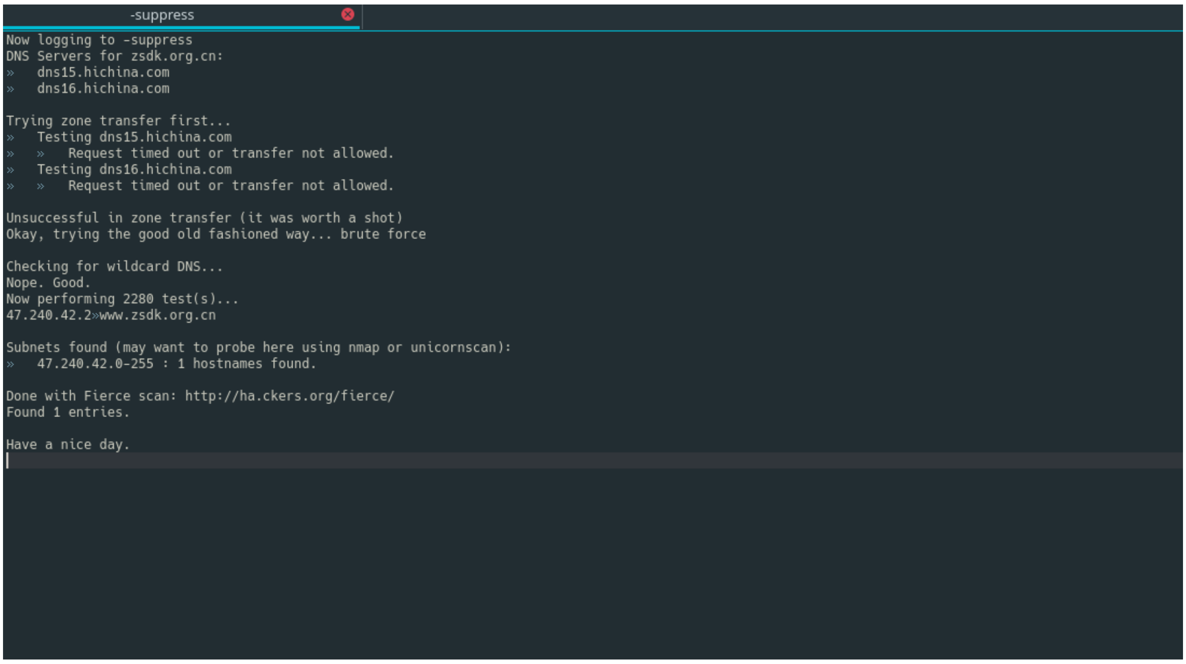


```
┌─[root@parrot]─[/home/kun]
└──╼ #fierce -dns zsdk.org.cn -file -suppress
Now logging to -suppress
DNS Servers for zsdk.org.cn:
        dns15.hichina.com
        dns16.hichina.com

Trying zone transfer first...
        Testing dns15.hichina.com
                Request timed out or transfer not allowed.
        Testing dns16.hichina.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
47.240.42.2     www.zsdk.org.cn

Subnets found (may want to probe here using nmap or unicornscan):
        47.240.42.0-255 : 1 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 1 entries.

Have a nice day.
```

> 此时你会发现fierce祝福了你“Have a nice day” " 祝您有个美好的一天。"，其实你在终端输出的信息并不是很多，而是存储到了你本地，其名称为"-suppress"



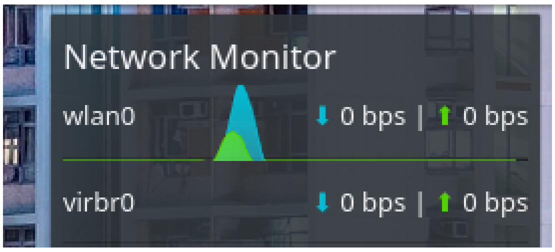
```
┌─[root@parrot]─[/home/kun]
└──╼ #ls
-suppress  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  baidunetdisk  temp
┌─[root@parrot]─[/home/kun]
```



```
Now logging to -suppress
DNS Servers for zsdk.org.cn:
»   dns15.hichina.com
»   dns16.hichina.com

Trying zone transfer first...
»   Testing dns15.hichina.com
»   »   Request timed out or transfer not allowed.
»   Testing dns16.hichina.com
»   »   Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
47.240.42.2»www.zsdk.org.cn

Subnets found (may want to probe here using nmap or unicornscan):
»   47.240.42.0-255 : 1 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 1 entries.

Have a nice day.
```

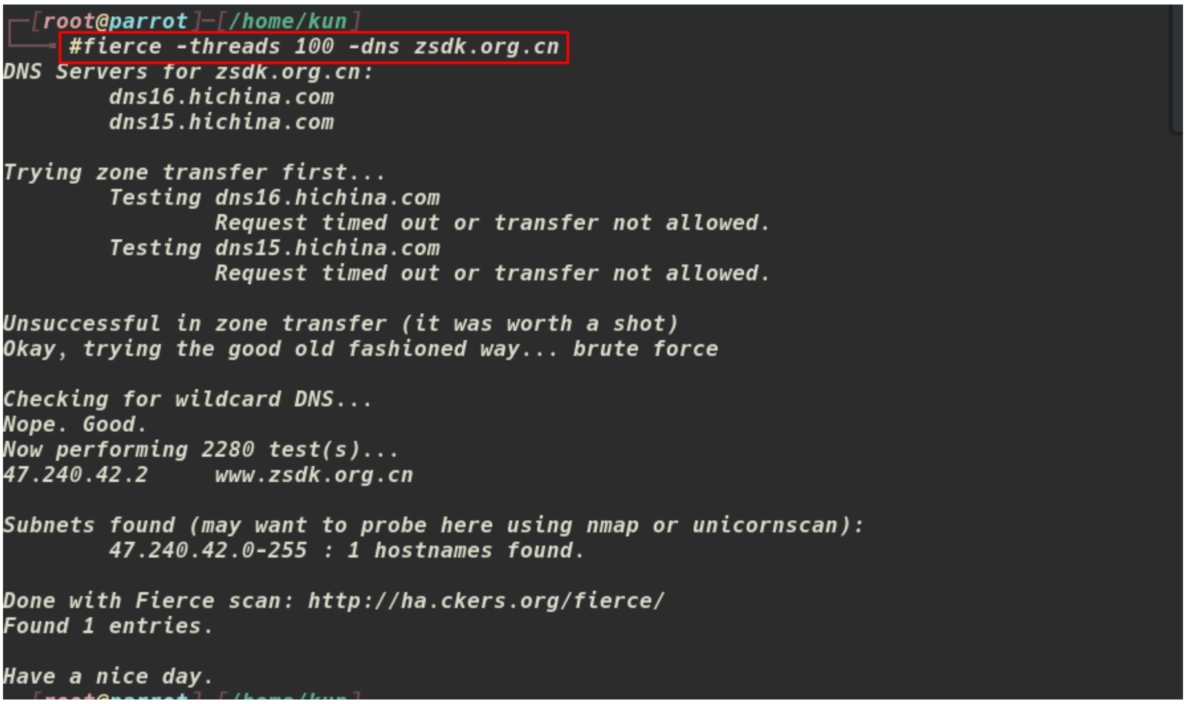
fierce -tcptimeout 200 -dns zsdk.org.cn

根据你想要的速度而定，如果你觉得检索的很慢，你可以选择增加“-tcptimeout”的值了。[^默认值为10,案例演示的值为200]



fierce -threads 100 -dns zsdk.org.cn

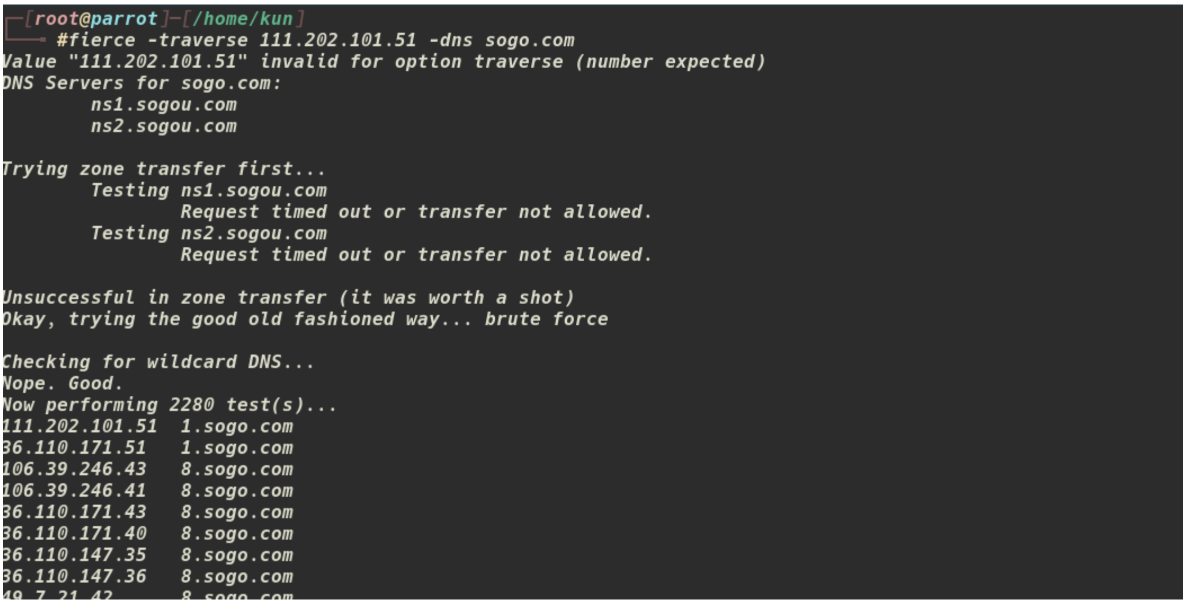
使用多线程[^默认为单线程，也就是1,此处实例为100线程]对zsdk.org.cn进行枚举



```
┌─[root@parrot]─[/home/kun]
└──╼ #fierce -threads 100 -dns zsdk.org.cn
DNS Servers for zsdk.org.cn:
        dns16.hichina.com
        dns15.hichina.com

Trying zone transfer first...
        Testing dns16.hichina.com
                Request timed out or transfer not allowed.
        Testing dns15.hichina.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
47.240.42.2     www.zsdk.org.cn

Subnets found (may want to probe here using nmap or unicornscan):
        47.240.42.0-255 : 1 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 1 entries.

Have a nice day.
┌─[root@parrot]─[/home/kun]
```

fierce -traverse 111.202.101.51[^地址你可以通过fierce -dns sogo.com进行获取] -dns sogo.com

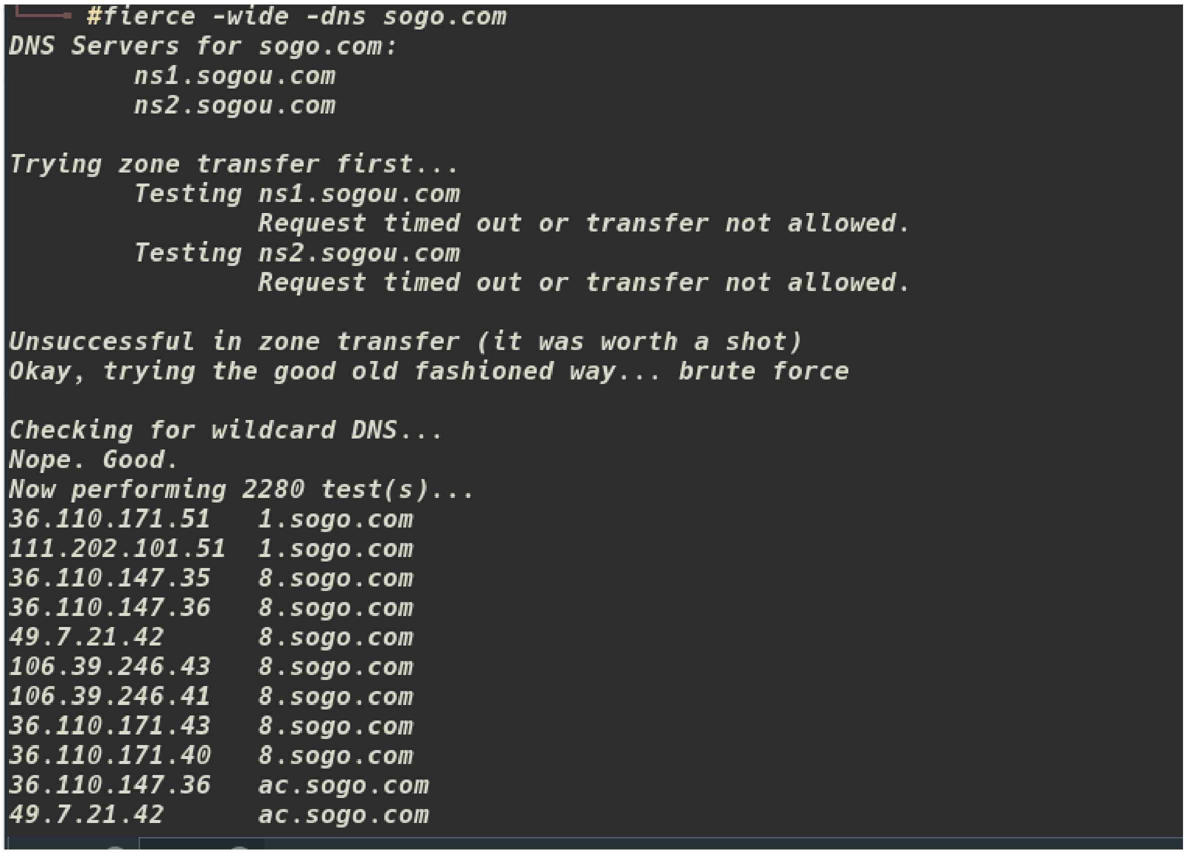
遍历111.202.101.51 IP之上和之下的IP数量，查找附近的IP，默认上下值为5



```
┌─[root@parrot]─[/home/kun]
└──╼ #fierce -traverse 111.202.101.51 -dns sogo.com
Value "111.202.101.51" invalid for option traverse (number expected)
DNS Servers for sogo.com:
        ns1.sogou.com
        ns2.sogou.com

Trying zone transfer first...
        Testing ns1.sogou.com
                Request timed out or transfer not allowed.
        Testing ns2.sogou.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
111.202.101.51  1.sogo.com
36.110.171.51   1.sogo.com
106.39.246.43   8.sogo.com
106.39.246.41   8.sogo.com
36.110.171.43   8.sogo.com
36.110.171.40   8.sogo.com
36.110.147.35   8.sogo.com
36.110.147.36   8.sogo.com
49.7.21.42      8.sogo.com
```

fierce -wide -dns sogo.com

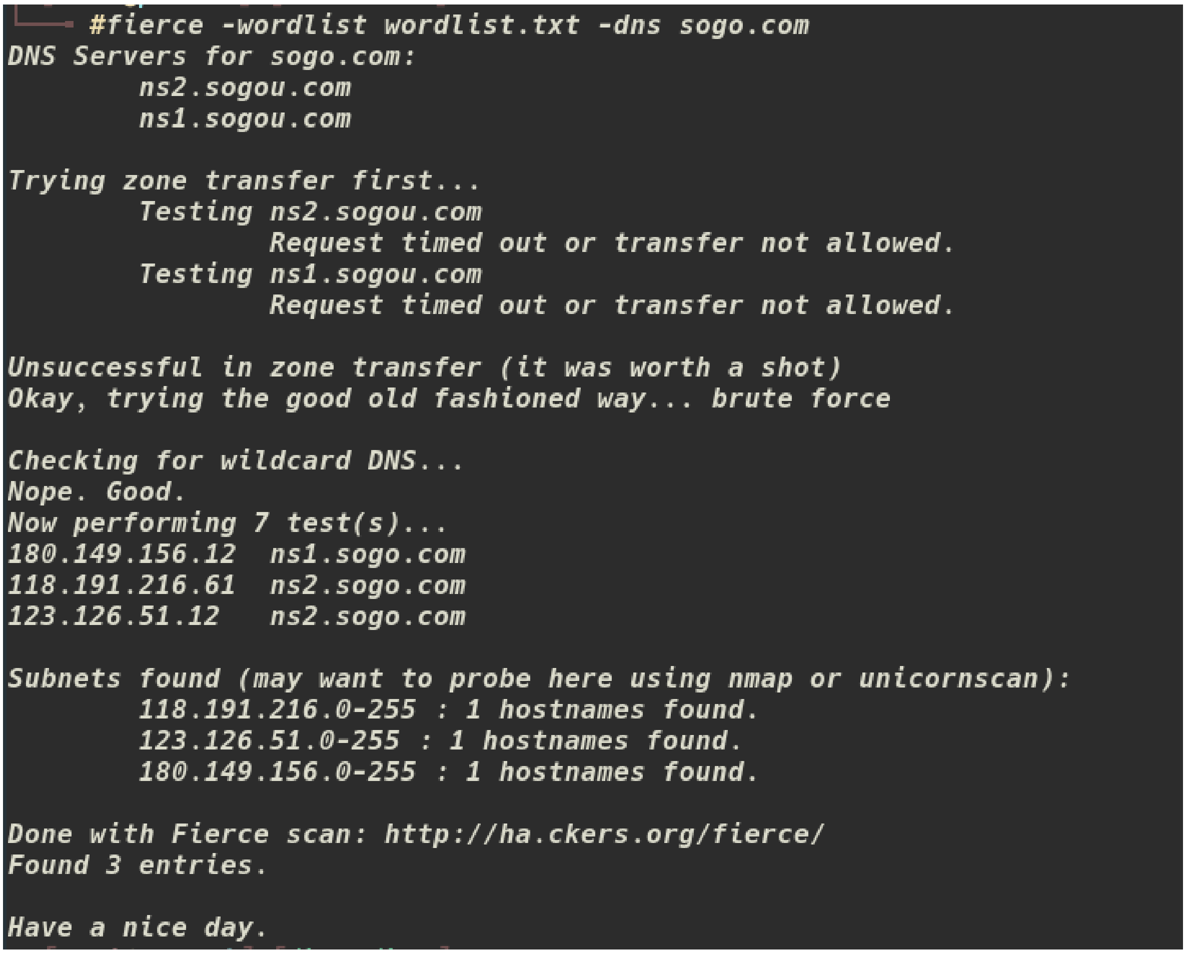
在C类中找到任何匹配的主机名，扫描整个类别C段，可以发现更多的信息[^但是会产生很多的流量请求]



```
└──╼ #fierce -wide -dns sogo.com
DNS Servers for sogo.com:
        ns1.sogou.com
        ns2.sogou.com

Trying zone transfer first...
        Testing ns1.sogou.com
                Request timed out or transfer not allowed.
        Testing ns2.sogou.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
36.110.171.51   1.sogo.com
111.202.101.51  1.sogo.com
36.110.147.35   8.sogo.com
36.110.147.36   8.sogo.com
49.7.21.42      8.sogo.com
106.39.246.43   8.sogo.com
106.39.246.41   8.sogo.com
36.110.171.43   8.sogo.com
36.110.171.40   8.sogo.com
36.110.147.36   ac.sogo.com
49.7.21.42      ac.sogo.com
```

fierce -wordlist wordlist.txt -dns sogo.com

使用一个单独的单词表



```
└──╼ #fierce -wordlist wordlist.txt -dns sogo.com
DNS Servers for sogo.com:
        ns2.sogou.com
        ns1.sogou.com

Trying zone transfer first...
        Testing ns2.sogou.com
                Request timed out or transfer not allowed.
        Testing ns1.sogou.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 7 test(s)...
180.149.156.12  ns1.sogo.com
118.191.216.61  ns2.sogo.com
123.126.51.12   ns2.sogo.com

Subnets found (may want to probe here using nmap or unicornscan):
        118.191.216.0-255 : 1 hostnames found.
        123.126.51.0-255 : 1 hostnames found.
        180.149.156.0-255 : 1 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 3 entries.

Have a nice day.
```