# Fierce

在一个安全的环境中，暴力破解 DNS 的方式是一种获取不连续 IP 地址空间主机的有效手段。 fierce 工具可以满足这样的需求，而且已经预装在 Kali Linux中。 fierce 是 RSnake 创立的快速有效地 DNS 暴力破解工具。 fierce 工具首先域名的 IP 地址，查询相关的域名服务器，然后利用字典进行攻击。

1.DNS字典爆破
fierce -dnsserver 8.8.8.8 -dns sogo.com -wordlist y.txt
指定8.8.8.8DNS服务器指定y.txt文件为字典爆破sogo.com域

可以使用dpkg -L fierce 显示fierce生成的所有文件

```
C:\root> dpkg -L fierce
/.
/usr
/usr/bin
/usr/bin/fierce
/usr/share
/usr/share/doc
/usr/share/doc/fierce
/usr/share/doc/fierce/changelog.Debian.gz
/usr/share/doc/fierce/copyright
/usr/share/fierce
/usr/share/fierce/hosts.txt
```

之后使用more /usr/share/fierce/hosts.txt 查看字典，
随后使用cat /usr/share/fierce/hosts.txt | grep www
查找www相关的关键字字典

fierce - dnsserver 8.8.8.8 -dns sogo.com -wordlist /usr/share/fierce/hosts.txt
使用8.8.8.8DNS服务器对sogo.com进行DNS字典爆破，字典为 /usr/share/fierce/hosts.txt

```
/hosts.txt
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...
```

```
                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
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
```

也可以使用

fierce -dns sogo.com

查询sogo.com的dns服务器信息

```
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...
^C
```