

# 使用 Kali Linux 在渗透测试中信息收集

本文会介绍 Kali 中一系列的信息收集工具。在阅读本文之后，我们希望你能够对信息收集有更好的理解。

在这个阶段我们需要尽可能多的收集目标的信息，例如：域名的信息，DNS，IP，使用的技术和配置，文件，联系方式等等。在信息收集中，每一个信息都是重要的。

信息收集的方式可以分为两种：主动和被动。主动的信息收集方式：通过直接访问、扫描网站，这种将流量流经网站的行为。被动的信息收集方式：利用第三方的服务对目标进行访问了解，比例：Google 搜索。

注意：

没有一种方式是最完美的，每个方式都有自己的优势，主动方式，你能获取更多的信息，但是目标主机可能会记录你的操作记录。被动方式，你收集的信息会先对少，但是你的行动并不会被目标主机发现。一般在一个渗透项目下，你需要有多次的信息收集，同时也要运用不同的收集方式，才能保证信息收集的完整性。

## 1、使用公共资源

在互联网中，有几个公开的资源网站可以用来对目标信息进行收集，使用这些网站，流量并不会流经目标主机，所以目标主机也不会记录你的行为。

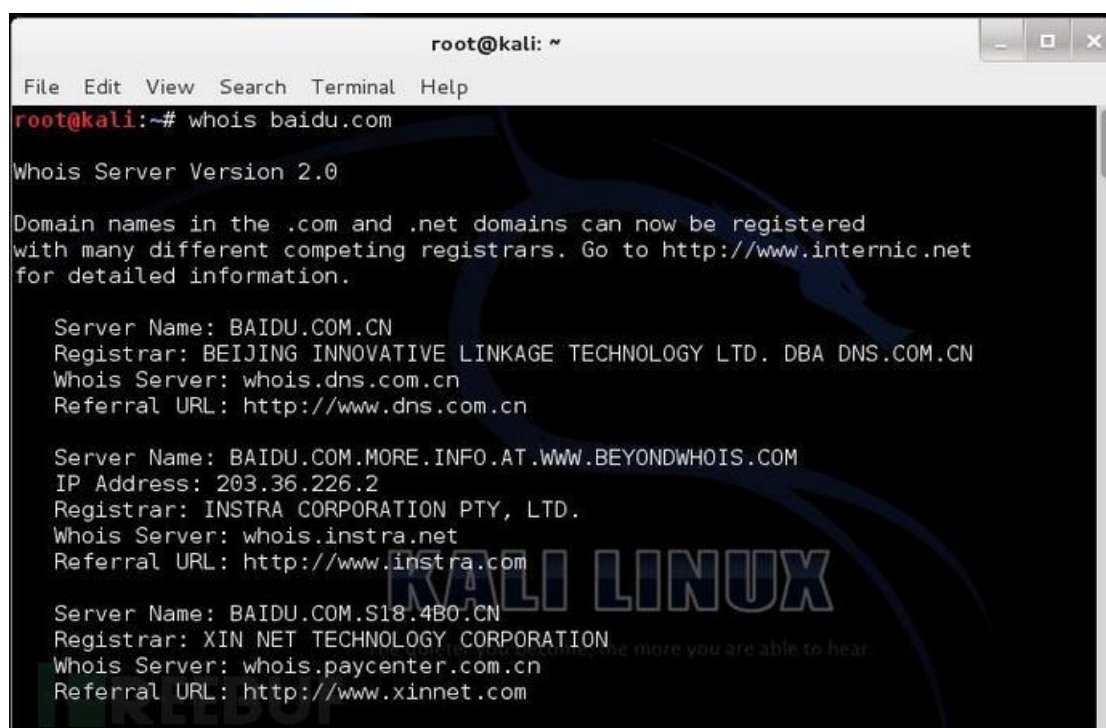
## 2、域名注册信息

当你知道目标的域名，你首先要做的就是通过 Whois 数据库查询域名的注册信息，Whois 数据库是提供域名的注册人信息，包括联系方式，管理员名字，管理员邮箱等等，其中也包括 DNS 服务器的信息。

关于 Whois 的介绍请访问：<https://www.ietf.org/rfc/rfc3912.txt>

默认情况下，Kali 已经安装了 Whois。你只需要输入要查询的域名即可：

```
#whois baidu.com
```

A terminal window titled 'root@kali: ~' showing the output of the 'whois baidu.com' command. The output includes 'Whois Server Version 2.0', a notice about domain registration, and three sets of server information for Baidu's domains: BAIDU.COM.CN, BAIDU.COM.MORE.INFO.AT.WWW.BEYONDWHOIS.COM, and BAIDU.COM.S18.4B0.CN. The background of the terminal has a Kali Linux logo.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# whois baidu.com  
  
Whois Server Version 2.0  
  
Domain names in the .com and .net domains can now be registered  
with many different competing registrars. Go to http://www.internic.net  
for detailed information.  
  
Server Name: BAIDU.COM.CN  
Registrar: BEIJING INNOVATIVE LINKAGE TECHNOLOGY LTD. DBA DNS.COM.CN  
Whois Server: whois.dns.com.cn  
Referral URL: http://www.dns.com.cn  
  
Server Name: BAIDU.COM.MORE.INFO.AT.WWW.BEYONDWHOIS.COM  
IP Address: 203.36.226.2  
Registrar: INSTRA CORPORATION PTY, LTD.  
Whois Server: whois.instra.net  
Referral URL: http://www.instra.com  
  
Server Name: BAIDU.COM.S18.4B0.CN  
Registrar: XIN NET TECHNOLOGY CORPORATION  
Whois Server: whois.paycenter.com.cn  
Referral URL: http://www.xinnet.com
```

我们可以获取关于百度的 DNS 服务器信息，域名注册基本信息。这些信息在以后的测试阶段中有可能会发挥重大的作用。

除了使用 whois 命令，也有一些网站提供在线 whois 信息查询：

[whois.chinaz.com/](http://whois.chinaz.com/)

[www.internic.net/whois.html](http://www.internic.net/whois.html)

收集完域名信息之后，我们将开始收集关于 DNS 服务器的详细信息。

## 1.1 DNS 分析

使用 DNS 分析工具的目的在于收集有关 DNS 服务器和测试目标的相应记录信息。

以下是几种常见的 DNS 记录类型：

No	TYPE ( 类型 )	说明
1	SOA	权威记录
2	NS	服务器记录
3	A	IPv4地址记录
4	MX	邮件交换记录
5	PTR	IP地址反解析
6	AAAA	IPv6地址记录
7	CNAME	别名记录

例如，在一个测试项目中，客户只给了一个域名，需要你根据域名，来查找所有目标主机的 IP 和可用的域。接下来我们将带你实现这样的功能。

host

在获取 DNS 服务器信息之后，下一步就是借助 DNS 服务器找出目标主机 IP 地址。我们可以使用下面的命令行工具来借助一个 DNS 服务器查找目标主机的 IP 地址：

```
# host www.baidu.com
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# host www.baidu.com  
www.baidu.com is an alias for www.a.shifen.com.  
www.a.shifen.com has address 180.149.131.205  
www.a.shifen.com has address 180.149.131.236  
root@kali:~#
```

我们可以看到有两个 IP 地址

一般情况下，host 查找的是 A，AAAA，和 MX 的记录。

查询详细的记录只需要添加 -a

```
#host -a baidu.com 8.8.8.8
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# host -a baidu.com 8.8.8.8  
Trying "baidu.com"  
Using domain server:  
Name: 8.8.8.8  
Address: 8.8.8.8#53  
Aliases:  
  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 63653  
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;baidu.com.  
IN ANY  
  
;; ANSWER SECTION:  
baidu.com. 20084 IN NS ns2.baidu.com.  
baidu.com. 20084 IN NS ns3.baidu.com.  
baidu.com. 20084 IN NS ns4.baidu.com.  
baidu.com. 20084 IN NS ns7.baidu.com.  
baidu.com. 20084 IN NS dns.baidu.com.  
baidu.com. 317 IN A 220.181.57.217  
baidu.com. 317 IN A 123.125.114.144  
baidu.com. 317 IN A 220.181.57.216  
  
Received 165 bytes from 8.8.8.8#53 in 40 ms  
root@kali:~#
```

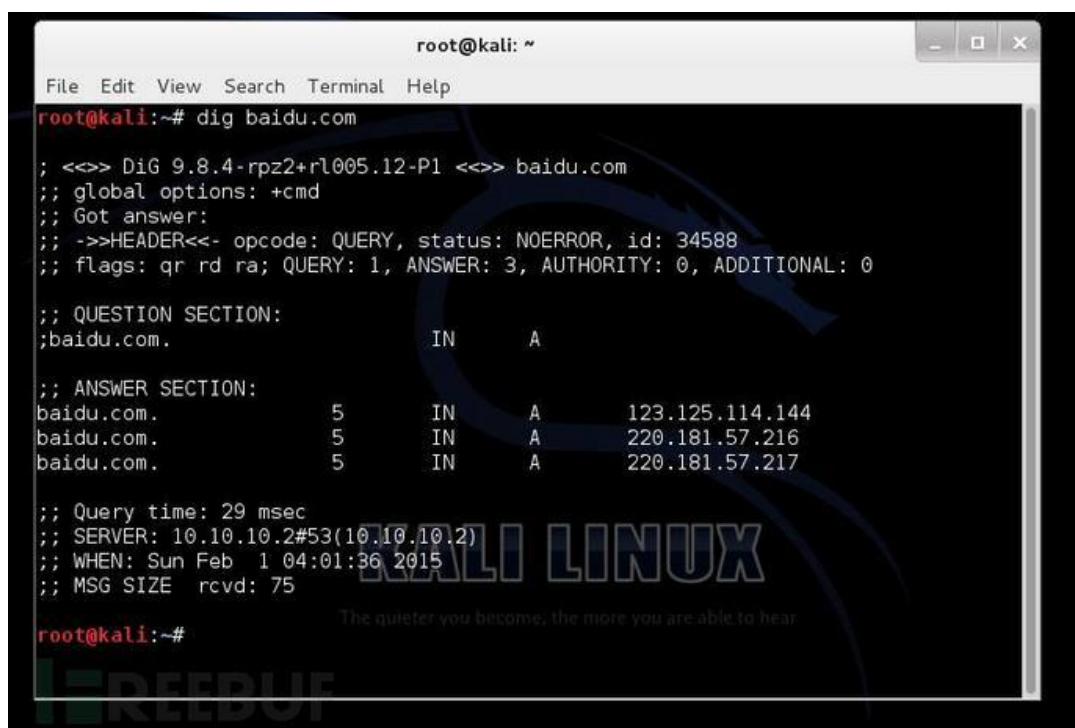
这里 8.8.8.8 是指定一个 DNS 服务器。

因为 host 命令查找记录是通过 Kali 的 DNS 服务器系统文件，该文件位于 /etc/resolv.conf.你可以往里面添加 DNS 任意服务器。当然也可以像我一样直接在命令行中指定 DNS 服务器。

## 1.2 dig

除了 host 命令，你也可以使用 dig 命令对 DNS 服务器进行挖掘。相对于 host 命令，dig 命令更具有灵活和清晰的显示信息。

```
#dig baidu.com
```



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# dig baidu.com  
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> baidu.com  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 34588  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;baidu.com.                IN      A  
  
;; ANSWER SECTION:  
baidu.com.                 5       IN      A       123.125.114.144  
baidu.com.                 5       IN      A       220.181.57.216  
baidu.com.                 5       IN      A       220.181.57.217  
  
;; Query time: 29 msec  
;; SERVER: 10.10.10.2#53(10.10.10.2)  
;; WHEN: Sun Feb  1 04:01:36 2015  
;; MSG SIZE  rcvd: 75  
  
root@kali:~#
```

不使用选项的 dig 命令，只返回一个记录。如果要返回全部的记录，只需要在命令添加给出的类型：

```
#dig baidu.com any
```

```
root@kali: ~  
File Edit View Search Terminal Help  
  
root@kali:~# dig baidu.com any  
  
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> baidu.com any  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47536  
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;baidu.com.  
  
;; ANSWER SECTION:  
baidu.com. 15308 IN NS ns7.baidu.com.  
baidu.com. 15308 IN NS dns.baidu.com.  
baidu.com. 15308 IN NS ns2.baidu.com.  
baidu.com. 15308 IN NS ns3.baidu.com.  
baidu.com. 15308 IN NS ns4.baidu.com.  
baidu.com. 342 IN A 220.181.57.216  
baidu.com. 342 IN A 220.181.57.217  
baidu.com. 342 IN A 123.125.114.144  
  
;; Query time: 26 msec  
;; SERVER: 8.8.8.8#53(8.8.8.8)
```

### 1.3 dnsenum

我们可以利用 dnsenum 从 DNS 服务器上获取以下信息：

1. 主机 IP 地址
2. 该域名的 DNS 服务器
3. 该域名的 MX 记录

除了被用来获取 DNS 信息，dnsenum 还具有以下特点：

1. 使用谷歌浏览器获取子域名
2. 暴力破解
3. C 级网络扫描
4. 反向查找网络

启动 dnsenum，使用如下命令

```
#dnsenum
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dnsenum
dnsenum.pl VERSION:1.2.3
Usage: dnsenum.pl [Options] <domain>
[Options]:
Note: the brute force -f switch is obligatory.
GENERAL OPTIONS:
  --dnsserver <server>      Use this DNS server for A, NS and MX queries.
  --enum                    Shortcut option equivalent to --threads 5 -s 15 -w.
  -h, --help                Print this help message.
  --noreverse               Skip the reverse lookup operations.
  --nocolor                 Disable ANSIColor output.
  --private                 Show and save private ips at the end of the file domain_
ips.txt.
  --subfile <file>          Write all valid subdomains to this file.
  -t, --timeout <value>    The tcp and udp timeout values in seconds (default: 10s)
  --threads <value>        The number of threads that will perform different queries.
  -v, --verbose             Be verbose: show all the progress and all the error messages.
                           The quieter you become, the more you are able to hear.
GOOGLE SCRAPING OPTIONS:
  -p, --pages <value>      The number of google search pages to process when scraping names,
```

通过一个例子来演示：

```
# dnsnum baidu.com
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dnsenum baidu.com
dnsenum.pl VERSION:1.2.3
----- baidu.com -----

Host's addresses:
-----
baidu.com.          5      IN      A       220.181.57.216
baidu.com.          5      IN      A       220.181.57.217
baidu.com.          5      IN      A       123.125.114.144

Wildcard detection using: ziirmabmscfm
-----
ziirmabmscfm.baidu.com. 5      IN      A       211.98.70.227

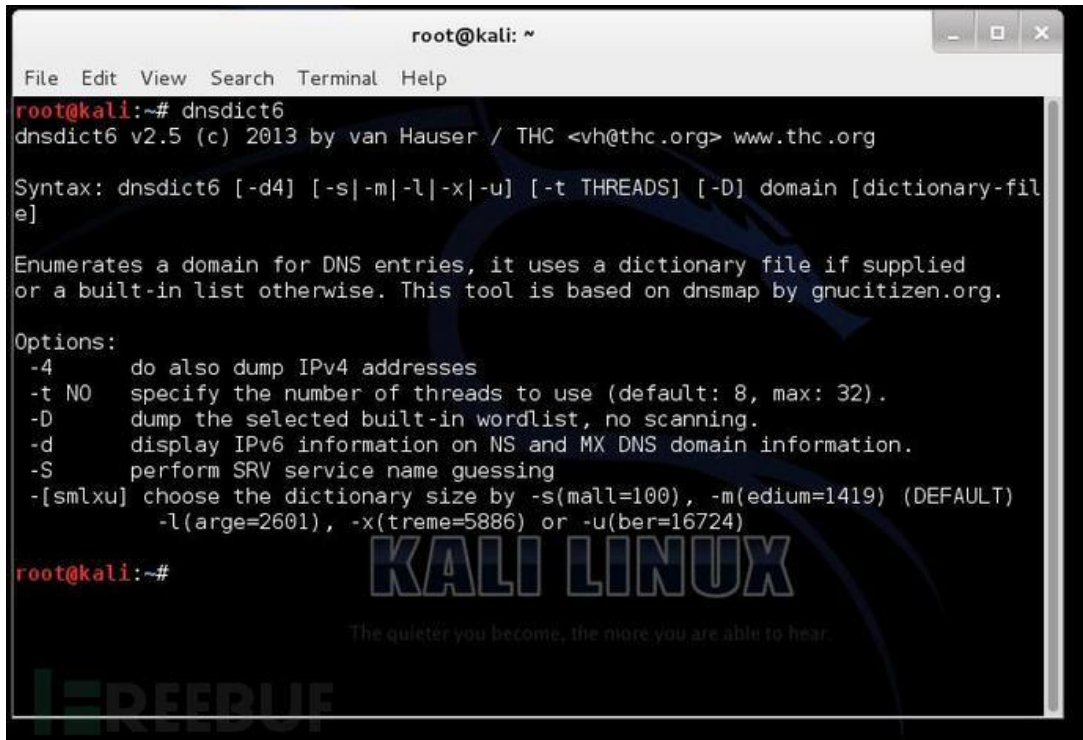
!!!!!!!!!!!!!!!!!!!!
Wildcards detected, all subdomains will point to the same IP address
Omitting results containing 211.98.70.227.
Maybe you are using OpenDNS servers.
!!!!!!!!!!!!!!!!!!!!
```



前面我们获取的是 IPv4 的信息，接下来我们使用 dnsdict6。该工具可以获取 IPv6 地址信息

#### 1.4 dnsdict6

```
#dnsdict6
```

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the command 'dnsdict6' being executed, which displays its version (v2.5), copyright (c) 2013 by van Hauser / THC, and website (www.thc.org). It then shows the syntax: 'dnsdict6 [-d4] [-s|-m|-l|-x|-u] [-t THREADS] [-D] domain [dictionary-file]'. Below this is a description: 'Enumerates a domain for DNS entries, it uses a dictionary file if supplied or a built-in list otherwise. This tool is based on dnsmap by gnucitizen.org.' A list of options follows: '-4 do also dump IPv4 addresses', '-t NO specify the number of threads to use (default: 8, max: 32).', '-D dump the selected built-in wordlist, no scanning.', '-d display IPv6 information on NS and MX DNS domain information.', '-S perform SRV service name guessing', and '-[smlxu] choose the dictionary size by -s(mall=100), -m(edium=1419) (DEFAULT), -l(arge=2601), -x(treme=5886) or -u(ber=16724)'. The prompt 'root@kali:~#' is visible at the bottom. The terminal background has a 'KALI LINUX' logo and the text 'The quieter you become, the more you are able to hear.' and 'FREEBUF'.

默认情况下，dnsdict6 将使用自带的字典和八个线程

```
#dnsdict6 baidu.com
```



```
root@kali: ~  
File Edit View Search Terminal Help  
-D dump the selected built-in wordlist, no scanning.  
-d display IPv6 information on NS and MX DNS domain information.  
-S perform SRV service name guessing  
-[smlxu] choose the dictionary size by -s(mall=100), -m(edium=1419) (DEFAULT)  
-l(arge=2601), -x(treme=5886) or -u(ber=16724)  
  
root@kali:~# dnsdict6 baidu.com  
Starting DNS enumeration work on baidu.com. ...  
Starting enumerating baidu.com. - creating 8 threads for 1419 words...  
Estimated time to completion: 1 to 2 minutes  
  
img.baidu.com. => ::ffff:222.47.21.37  
img.baidu.com. => ::ffff:222.47.21.36  
img.baidu.com. => ::ffff:222.47.21.46  
ipv6.baidu.com. => 2400:da00::dbf:0:100  
mp3.baidu.com. => ::ffff:222.47.21.37  
mp3.baidu.com. => ::ffff:222.47.21.46  
mp3.baidu.com. => ::ffff:222.47.21.36  
^Z  
[1]+ Stopped dnsdict6 baidu.com  
root@kali:~#
```

由此可见，是有默认的状态对百度进行 IPv6 扫描。

同时，我们也可以使用 dnsdict6 查找域名上的 IPv4，使用选项 -4.并且使用-d 还可以收集 DNS 和 NS 的信息：

```
#dnsdict6 -4 -d baidu.com
```

```
root@kali: ~  
File Edit View Search Terminal Help  
^Z  
[1]+  Stopped                  dnsdict6 baidu.com  
root@kali:~# dnsdict6 -4 -d baidu.com  
Starting DNS enumeration work on baidu.com. ...  
Gathering NS and MX information...  
NS of baidu.com. is ns4.baidu.com. => 220.181.38.10  
NS of baidu.com. is dns.baidu.com. => 202.108.22.220  
NS of baidu.com. is ns2.baidu.com. => 61.135.165.235  
NS of baidu.com. is ns3.baidu.com. => 220.181.37.10  
NS of baidu.com. is ns7.baidu.com. => 119.75.219.82  
No IPv6 address for NS entries found in DNS for domain baidu.com.  
MX of baidu.com. is mx1.baidu.com. => 61.135.163.61  
MX of baidu.com. is mx.n.shifen.com. => 61.135.163.61  
MX of baidu.com. is jpmx.baidu.com. => 61.208.132.13  
MX of baidu.com. is mx50.baidu.com. => 220.181.50.208  
No IPv6 address for MX entries found in DNS for domain baidu.com.  
  
Starting enumerating baidu.com. - creating 8 threads for 1419 words...  
Estimated time to completion: 1 to 2 minutes  
Warning: wildcard domain configured  
*.baidu.com. -> 211.98.70.227  
Warning: wildcard domain configured (2nd test)  
l.baidu.com. => 119.75.219.60
```

### 1.5 fierce

fierce 是使用多种技术来扫描目标主机 IP 地址和主机名的一个 DNS 服务器枚举工具。运用递归的方式来工作。它的工作原理是先通过查询本地 DNS 服务器来查找目标 DNS 服务器，然后使用目标 DNS 服务器来查找子域名。fierce 的主要特点就是可以用来地位独立 IP 空间对应域名和主机名。

启动 fierce 使用的命令：

```
#fierce -h
```

```
root@kali: ~  
File Edit View Search Terminal Help  
but can uncover a lot more information.  
-wordlist Use a separate wordlist (one word per line). Usage:  
  
perl fierce.pl -dns examplecompany.com -wordlist dictionary.txt  
root@kali:~# fierce -h  
fierce.pl (C) Copywrite 2006,2007 - By RSnake at http://ha.ckers.org/fierce/  
  
Usage: perl fierce.pl [-dns example.com] [OPTIONS]  
  
Overview:  
Fierce is a semi-lightweight scanner that helps locate non-contiguous  
IP space and hostnames against specified domains. It's really meant  
as a pre-cursor to nmap, unicornscan, nessus, nikto, etc, since all  
of those require that you already know what IP space you are looking  
for. This does not perform exploitation and does not scan the whole  
internet indiscriminately. It is meant specifically to locate likely  
targets both inside and outside a corporate network. Because it uses  
DNS primarily you will often find mis-configured networks that leak  
internal address space. That's especially useful in targeted malware.  
  
Options:  
-connect The quieter you become, the more you are able to hear  
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
```

通过一个例子来演示：

```
#fierce -dns baidu.com -threads 3
```

```
root@kali: ~  
File Edit View Search Terminal Help  
perl fierce.pl -dns examplecompany.com -wordlist dictionary.txt  
root@kali:~# fierce -dns baidu.com -threads 3  
DNS Servers for baidu.com:  
ns7.baidu.com  
ns3.baidu.com  
ns2.baidu.com  
ns4.baidu.com  
dns.baidu.com  
  
Trying zone transfer first...  
Testing ns7.baidu.com  
Request timed out or transfer not allowed.  
Testing ns3.baidu.com  
Request timed out or transfer not allowed.  
Testing ns2.baidu.com  
Request timed out or transfer not allowed.  
Testing ns4.baidu.com  
Request timed out or transfer not allowed.  
Testing dns.baidu.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
```

## 1.6 DMitry

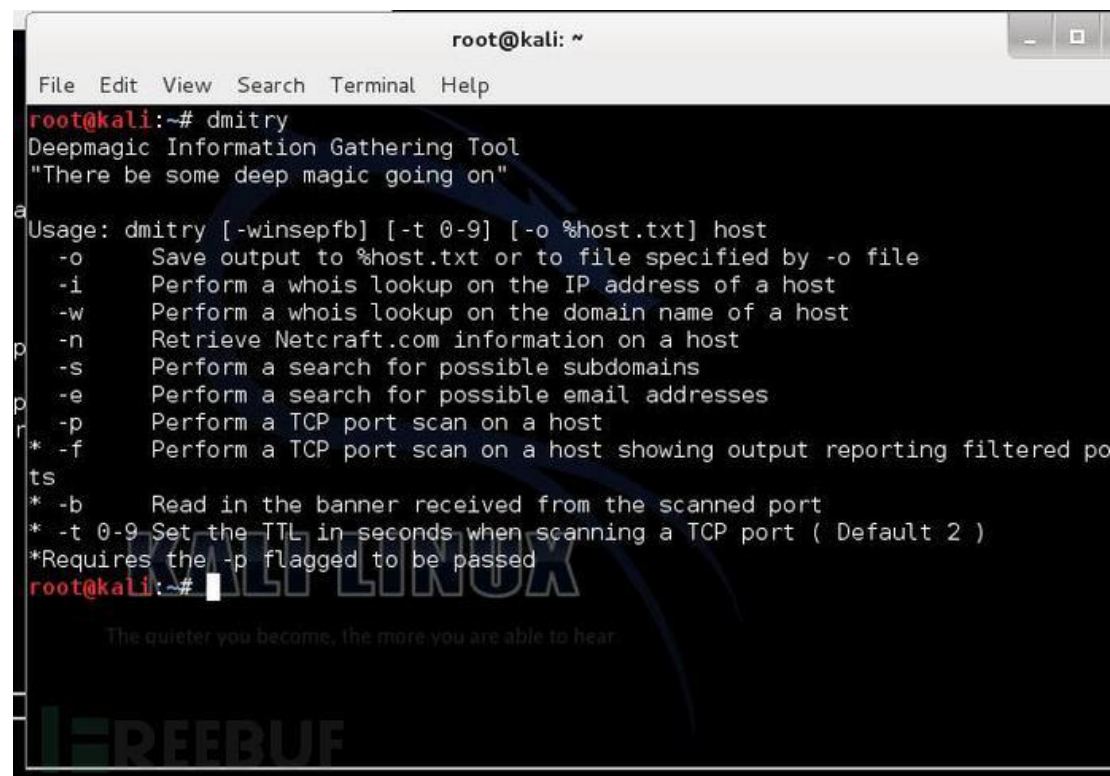
DMitry ( Deepmagic Information Gathering Tool ) 是一个一体化的信息收集工具。它可以用来收集以下信息：

1. 端口扫描
2. whois 主机 IP 和域名信息
3. 从 Netcraft.com 获取主机信息
4. 子域名
5. 域名中包含的邮件地址

尽管这些信息可以在 Kali 中通过多种工具获取，但是使用 DMitry 可以将收集的信息保存在一个文件中，方便查看。

使用 DMitry 可以使用如下命令：

```
#dmitry
```



The screenshot shows a terminal window titled 'root@kali: ~'. The user has entered the command 'dmitry'. The terminal output displays the tool's name 'Deepmagic Information Gathering Tool' and a quote: 'There be some deep magic going on'. Below this, the usage instructions are shown: 'Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host'. A list of options follows: '-o' for saving output to a file, '-i' for whois on IP, '-w' for whois on domain, '-n' for Netcraft.com info, '-s' for subdomains, '-e' for email addresses, '-p' for TCP port scan, and '-f' for TCP port scan with filtered ports. There are also options for reading banners (-b) and setting TTL (-t). A note states '\*Requires the -p flagged to be passed'. The prompt 'root@kali:~#' is visible at the bottom of the terminal output.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
-o      Save output to %host.txt or to file specified by -o file
-i      Perform a whois lookup on the IP address of a host
-w      Perform a whois lookup on the domain name of a host
-n      Retrieve Netcraft.com information on a host
-s      Perform a search for possible subdomains
-e      Perform a search for possible email addresses
-p      Perform a TCP port scan on a host
-f      Perform a TCP port scan on a host showing output reporting filtered ports
-b      Read in the banner received from the scanned port
-t 0-9  Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
root@kali:~#
```

通过一个例子来演示：

这个演示是要获取 whois ， ip ， 主机信息 ， 子域名 ， 电子邮件。

```
#dmitry -winse baidu.com
```



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# dmitry -winse baidu.com  
Deepmagic Information Gathering Tool  
"There be some deep magic going on"  
HostIP:220.181.57.216  
HostName:baidu.com  
Gathered Inet-whois information for 220.181.57.216  
-----  
inetnum:          220.181.0.0 - 220.181.255.255  
netname:          CHINANET-IDC-BJ  
country:         CN  
descr:           CHINANET Beijing province network  
descr:           China Telecom  
descr:           No.31,jingrong street  
descr:           Beijing 100032  
admin-c:         CH93-AP  
tech-c:          HC55-AP  
remarks:         hostmaster is not for spam complaint,  
remarks:         please send spam complaint to anti-spam@ns.chinanet.cn.net  
mnt-by:          MAINT-CHINANET  
mnt-lower:       MAINT-CHINATELECOM-BJ
```

再一个例子，通过 dmitry 来扫描网站端口

```
#dmitry -p baidu.com -f -b
```



```
root@kali: ~  
File Edit View Search Terminal Help  
g All scans completed, exiting  
g root@kali:~# dmitry -p baidu.com -f -b  
Deepmagic Information Gathering Tool  
9 "There be some deep magic going on"  
tx  
b HostIP:220.181.57.217  
b HostName:baidu.com  
j  
pGathered TCP Port information for 220.181.57.217  
p-----  
ar  
ar Port          State  
c1/tcp          filtered  
s 2/tcp          filtered  
p3/tcp          filtered  
4/tcp          filtered  
5/tcp          filtered  
6/tcp          filtered  
7/tcp          filtered  
8/tcp          filtered  
9/tcp          filtered  
10/tcp         filtered  
11/tcp         filtered
```

扫描之后我们会发现百度只开放了 80 端口。（截图只有部分。）

### 1.7 Maltego

Maltego 是一个开源的取证工具。它可以挖掘和收集信息。

Maltego 是一个图形界面。

Maltego 的基础网络特点：

1. 域名
2. DNS
3. Whois
4. IP 地址
5. 网络块

也可以被用于收集相关人员的信息：

1. 公司、组织
2. 电子邮件

3. 社交网络关系

4. 电话号码

使用 Maltego 的命令行如下：

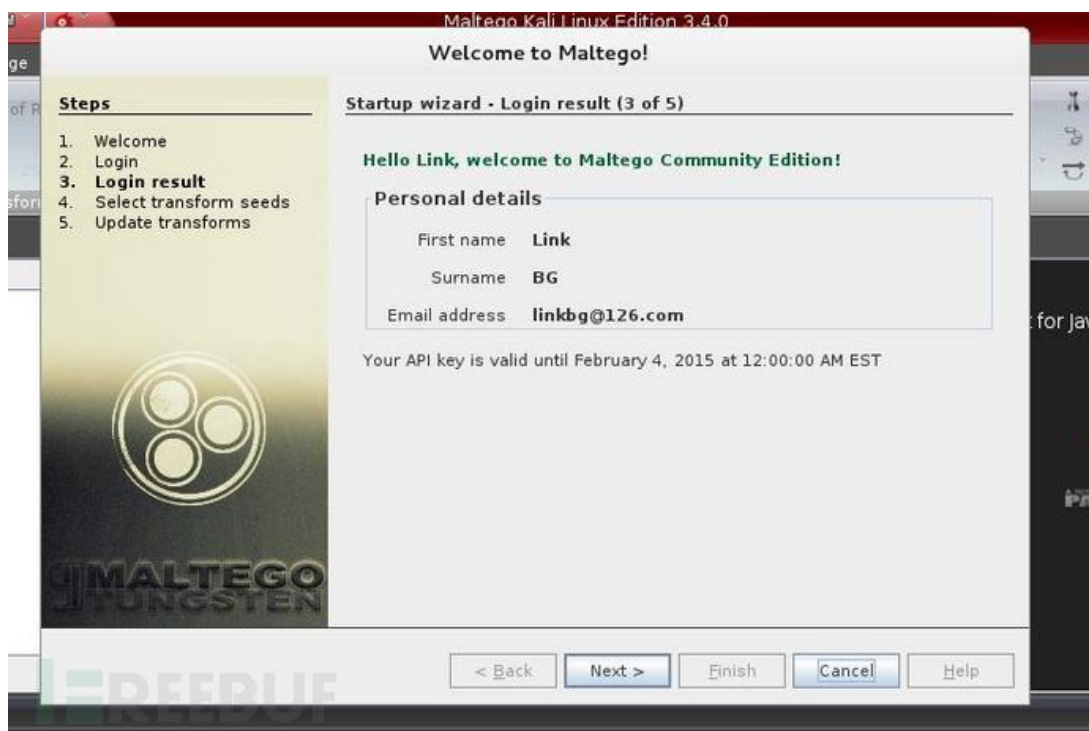
```
#maltego
```

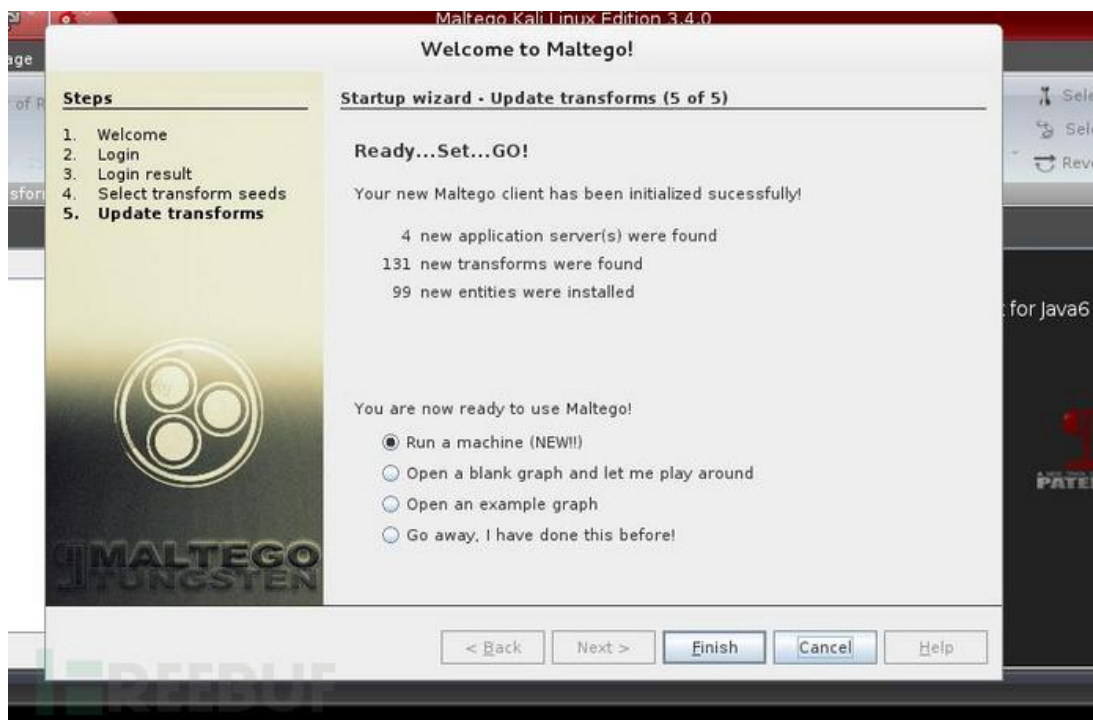
```
root@kali:~#  
root@kali:~# maltego
```

第一次运行会出现启动向导：





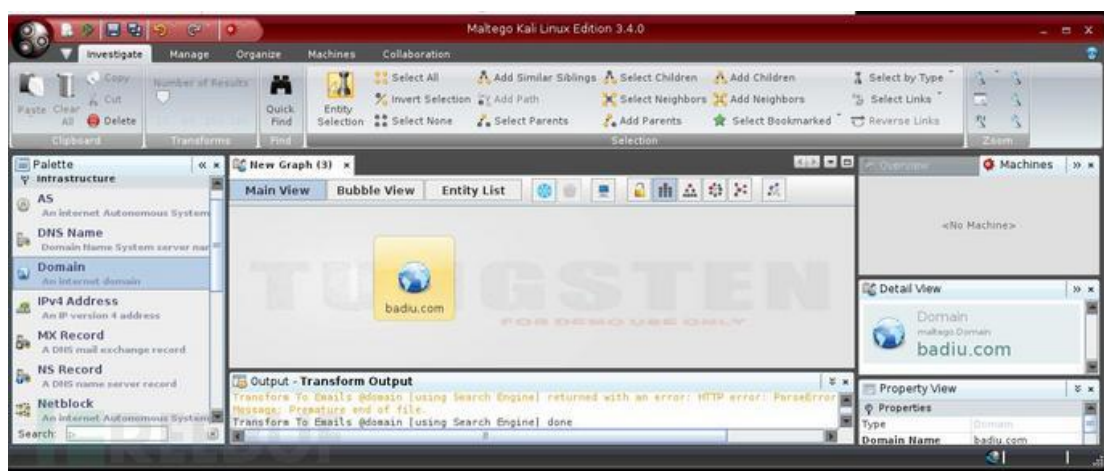






通过一个例子演示：

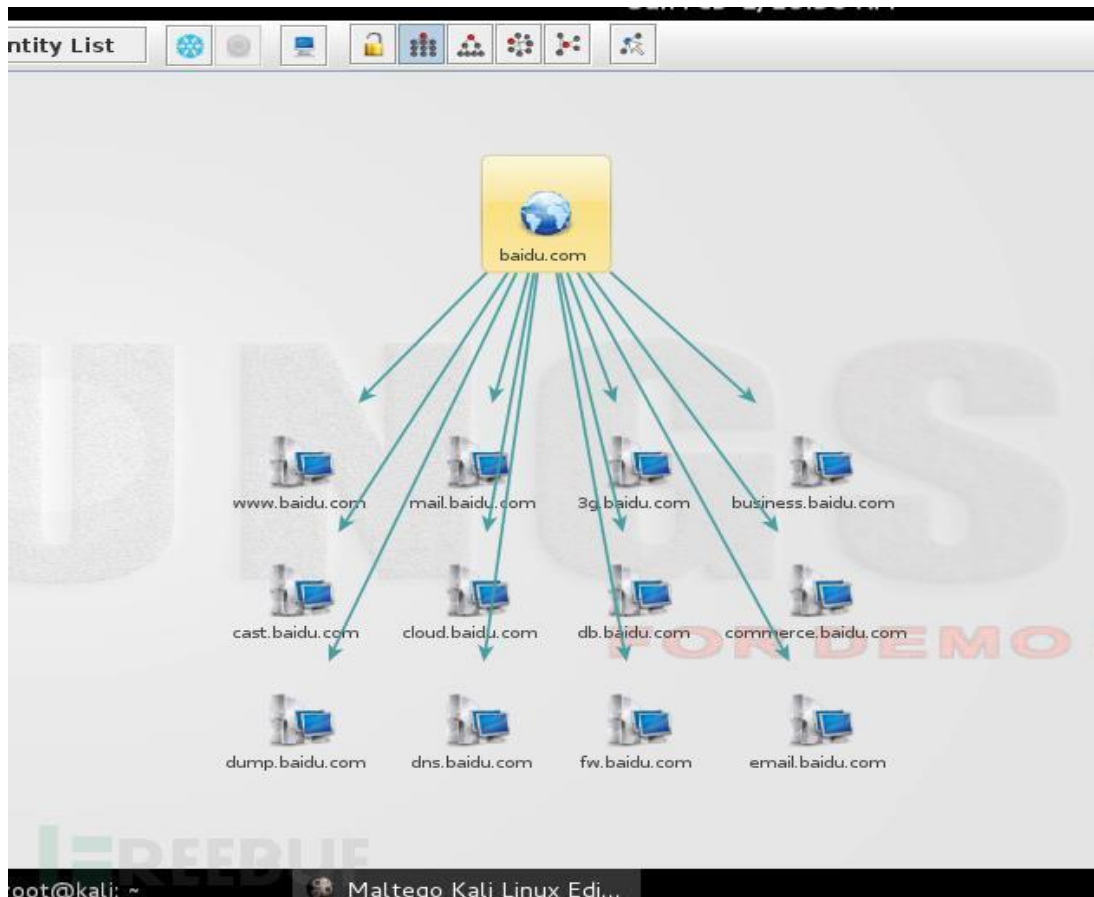
使用快捷键 **ctrl+T** 来创建新的项目。然后到 **Palette** 选项卡，选择基础设施（Infrastructure），选择域（Domain），如果成功建立会出现 **paterva.com**。可以通过双击 **paterva.com** 这个图标进行更改



如果你右键单击域名，你会看到所有的功能（变换？？）：



我们使用 Other transforms->DomainToDNSNameSchema 结果如图：



在对域名的 DNS 变换后，我们得到了百度的相关信息。你还可以试试其他（变换）功能。

## 2、利用搜索引擎

Kali 工具集中有可以用来收集域，电子邮件等信息的工具，这些工具使用第三方搜索引擎进行信息收集，这样的好处在于我们不用直接访问目标，目标并不知道你的行动。

### 2.1 theharvester

thearvester 是一个电子邮件，用户名和主机名/子域名信息收集工具。它收集来自各种公开的信息来源。最新版本支持的信息来源包括：

1. Google
2. Google profiles
3. Bing
4. PGP
5. LinkedIn
6. Yandex
7. People123
8. Jigsaw

使用 theharvester 命令行：

```
# theharvester
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# theharvester
*****
*
* TheHarvester Ver. 2.2a
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

Usage: theharvester options

-d: Domain to search or company name
-b: Data source (google,bing,bingapi,pgp,linkedin,google-profile
s,people123,jigsaw,all)
-s: Start in result number X (default 0)
-v: Verify host name via dns resolution and search for virtual h
osts
-f: Save the results into an HTML and XML file
-n: Perform a DNS reverse query on all ranges discovered
-c: Perform a DNS brute force for the domain name

root@kali: ~
```

通过一个例子来演示：

通过 bing 来收集

```
#theharvester -d baidu.com -l 100 -b bing
```









```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# metagoofil
*****
* Metagoofil Ver 2.2 *
* Christian Martorella *
* Edge-Security.com *
* cmartorella_at_edge-security.com *
*****

Usage: metagoofil options

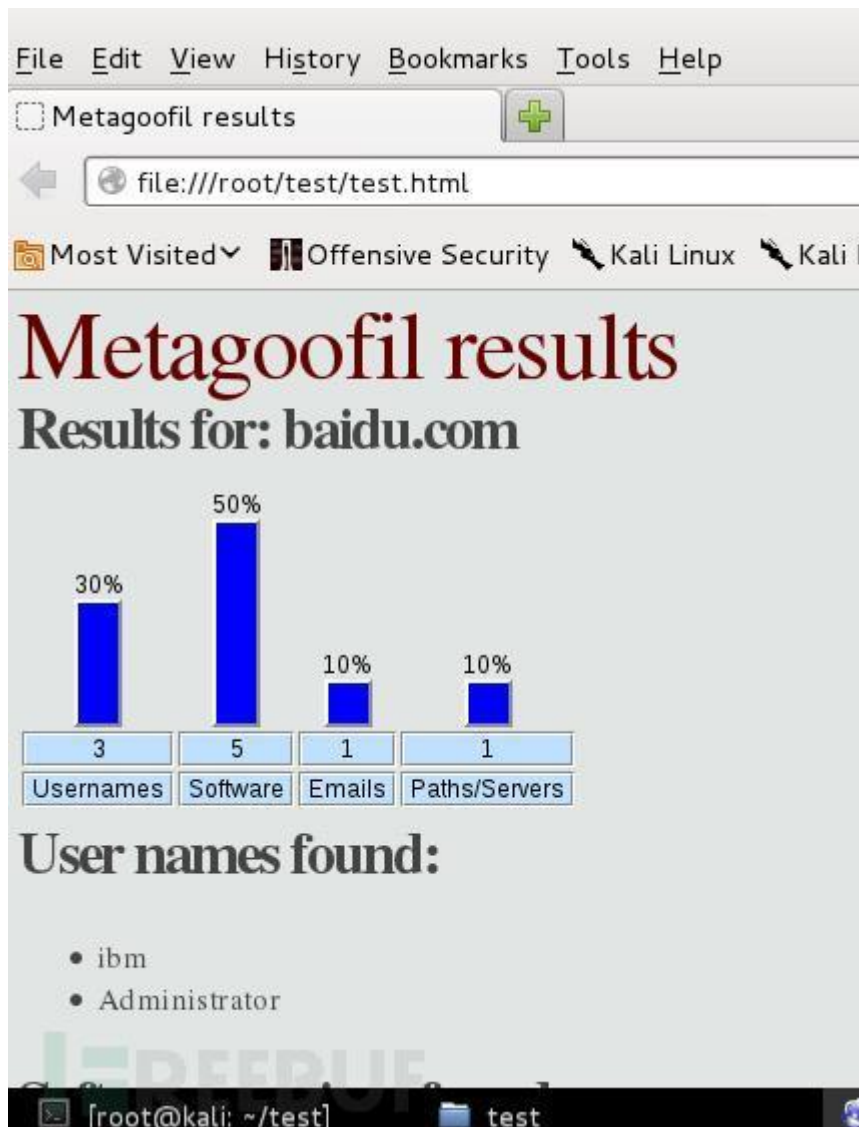
-d: domain to search
-t: filetype to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pp
tx)
-l: limit of results to search (default 200)
-h: work with documents in directory (use "yes" for local anal
ysis)
-n: limit of files to download
-o: working directory (location to save downloaded files)
-f: output file

Examples:
root@kali:~#
```

通过一个例子来演示：

```
#metagoofil -d baidu.com -l 20 -t doc,pdf -n 5 -f tes
t.html -o test
```





至此，我们的信息收集工具介绍已经完成。每个渗透目标，想要通过不同的途径获取目标大量信息。要知道：“知彼知己，百战百胜”。