子域名暴破软件 dnsmap 介绍

--金山安全应急响应中心/KSSG

渗透工作中，前期的信息收集是必不可少的，而对子域名的收集占据着一定的比重，收集子域名经常会给渗透者带来惊喜，比如发现监控系统或者一些比较敏感的后台等。

对子域名的收集方法一般有利用搜索引擎，暴破子域名，DNS 域传送等等，今天要讲解的软件 dnsmap 主要是采用暴破子域名方法。软件安装很简单，使用以下几条命令即可：

wget http://dnsmap.googlecode.com/files/dnsmap-0.30.tar.gz
tar zvxf dnsmap-0.30.tar.gz
cd dnsmap-0.30
make

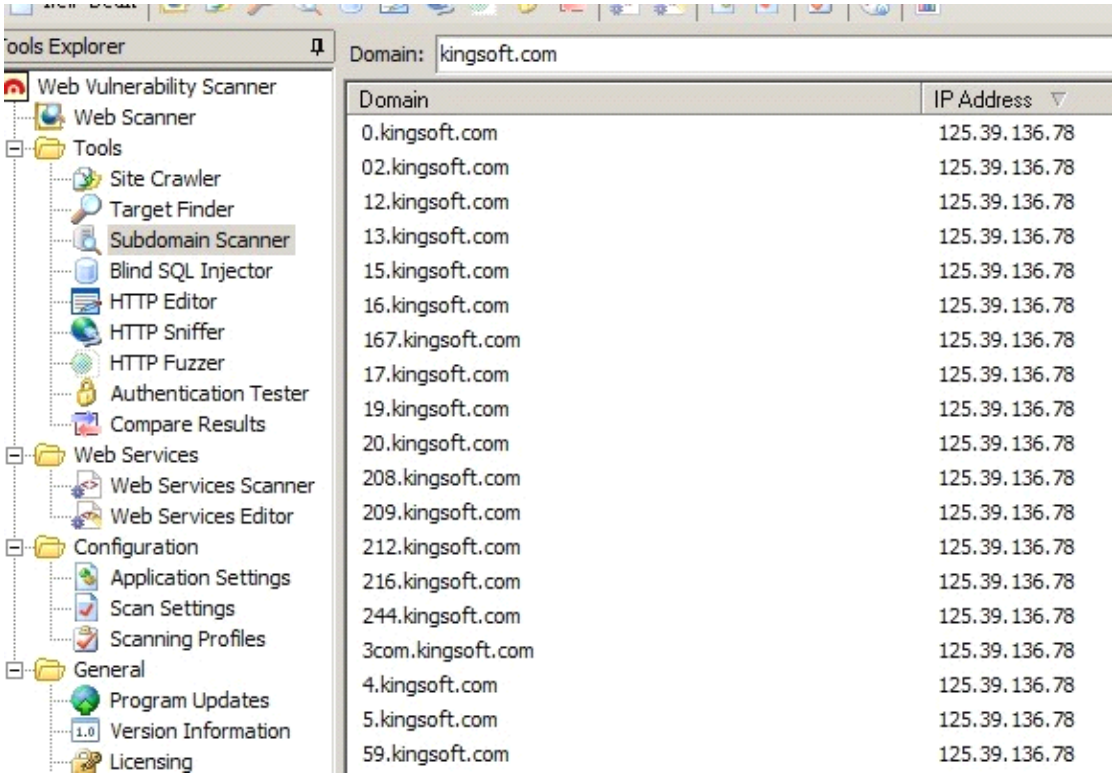
输入./dnsmap 可看到 dnsmap 的使用说明

```
[root@vpstest dnsmap-0.30]# ./dnsmap
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

usage: dnsmap <target-domain> [options]
options:
-w <wordlist-file>
-r <regular-results-file>
-c <csv-results-file>
-d <delay-millisecs>
-i <ips-to-ignore> (useful if you're obtaining false positives)

e.g.:
dnsmap target-domain.foo
dnsmap target-domain.foo -w yourwordlist.txt -r /tmp/domainbf_results.txt
dnsmap target-fomain.foo -r /tmp/ -d 3000
dnsmap target-fomain.foo -r ./domainbf_results.txt
```

-w 参数后面加你自己的域名字典，也可以使用程序自带的
-r 参数后面加你想保存结果的目录/文件名
-c 将结果保存为 csv 格式
-d 检测延时
-i 忽略所解析到的指定 ip（这个参数很有用，后面会讲到）

很多软件都有暴破子域名的功能，比如 wvs msf 等，但是当域名做了泛解析的时候就会造成很多误报，这里我们以 kingsoft.com 举例

WVS 检测效果如图：



Msf 检测效果如图：

```
msf auxiliary(dns_srv_enum) > use auxiliary/gather/dns_bruteforce
msf auxiliary(dns_bruteforce) > show options

Module options (auxiliary/gather/dns_bruteforce):

   Name       Current Setting                                                Required  Description
   ----       ---------------                                                --------  -----------
   DOMAIN                                                                    yes       The target domain na
   NS                                                                        no        Specify the name ser
   WORDLIST   /opt/metasploit/apps/pro/msf3/data/wordlists/namelist.txt      yes       Wordlist file for do

msf auxiliary(dns_bruteforce) > set domain kingsoft.com
domain => kingsoft.com
msf auxiliary(dns_bruteforce) > exploit

[*] Enumerating kingsoft.com
[*] This Domain has wild-cards enabled!!
[!] Wild-card IP for 8572.kingsoft.com is: 219.239.93.145
[!] Wild-card IP for 8572.kingsoft.com is: 125.39.136.78
[*] Performing bruteforce against kingsoft.com
[+] Host rdr.kingsoft.com. with address 219.239.93.145 found
[+] Host rdr.kingsoft.com. with address 125.39.136.78 found
[+] Host 0.kingsoft.com with address 125.39.136.78 found
[+] Host 0.kingsoft.com with address 219.239.93.145 found
[+] Host rdr.kingsoft.com. with address 125.39.136.78 found
[+] Host rdr.kingsoft.com. with address 219.239.93.145 found
[+] Host rdr.kingsoft.com. with address 125.39.136.78 found
[+] Host rdr.kingsoft.com. with address 219.239.93.145 found
[+] Host 01.kingsoft.com with address 219.239.93.145 found
[+] Host 01.kingsoft.com with address 125.39.136.78 found
[+] Host rdr.kingsoft.com. with address 219.239.93.145 found
[+] Host rdr.kingsoft.com. with address 125.39.136.78 found
[+] Host rdr.kingsoft.com. with address 219.239.93.145 found
[+] Host rdr.kingsoft.com. with address 125.39.136.78 found
[+] Host 02.kingsoft.com with address 125.39.136.78 found
[+] Host 02.kingsoft.com with address 219.239.93.145 found
[+] Host rdr.kingsoft.com. with address 125.39.136.78 found
[+] Host rdr.kingsoft.com. with address 219.239.93.145 found
```

Msf 已经给出了泛解析所指向的 ip 地址，但是并没有选项支持忽略这两个 ip 地址，导致误报，此时我们可以使用 dnsmap 的-i 参数，执行
./dnsmap kingsoft.com -i 219.239.93.145,125.39.136.78

```
[root@vpstest dnsmap-0.30]# ./dnsmap kingsoft.com -i 219.239.93.145,125.39.136.78
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] 2 provided IP address(es) will be ignored from results: 219.239.93.145,125.39.136.78
[+] warning: domain might use wildcards. 125.39.136.78 will be ignored from results
[+] searching (sub)domains for kingsoft.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

ad.kingsoft.com
IP address #1: 61.188.37.41

admin.kingsoft.com
IP address #1: 58.83.211.146

bi.kingsoft.com
IP address #1: 114.112.93.131

bj.kingsoft.com
IP address #1: 222.73.9.14

blog.kingsoft.com
IP address #1: 58.83.211.146
```

成功输出准确结果

部分版本可能会出现如下提示

```
[root@vps123 dnsmap-0.30]# ./dnsmap kingsoft.com
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] error: entered domain is not valid!
```

形成此原因的关键代码如图

```
// some domains like proboards.com return more than 1 IP address
// when resolving random subdomains (wildcards are enabled)
h=gethostbyname(s);
if(h) {
        for(j=0;h->h_addr_list[j];++j)
                inet_ntoa(*((struct in_addr *)h->h_addr_list[j]));
        if(j>1) {
                #if DEBUG

                        printf("wildcard domain\'s number of IP address(es): %d"
                                " (this causes dnsmap to produce false positives)\n",j);
                #endif
                return FALSE;
        }
}
```

程序会测试一个随机数加域名，如果解析此域名对应的 ip 数量超过 1 个即返回错误，可以通过 dig 得到认证

```
[root@vpstest dnsmap-0.30]# dig aaaaaaaa.kingsoft.com

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> aaaaaaaa.kingsoft.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34385
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;aaaaaaaa.kingsoft.com.         IN      A

;; ANSWER SECTION:
aaaaaaaa.kingsoft.com.  600     IN      CNAME   rdr.kingsoft.com.
rdr.kingsoft.com.       600     IN      A       219.239.93.145
rdr.kingsoft.com.       600     IN      A       125.39.136.78

;; AUTHORITY SECTION:
kingsoft.com.           10555   IN      NS      ns.kingsoft.com.
kingsoft.com.           10555   IN      NS      dns.kingsoft.net.

;; ADDITIONAL SECTION:
dns.kingsoft.net.       3156    IN      A       125.89.75.203
dns.kingsoft.net.       3156    IN      A       121.14.11.120
dns.kingsoft.net.       3156    IN      A       125.39.136.74

;; Query time: 559 msec
;; SERVER: 204.74.208.2#53(204.74.208.2)
;; WHEN: Mon Jul 29 12:07:37 2013
;; MSG SIZE  rcvd: 184
```

解决此问题很简单，编辑 dnsmap.c 文件，注释掉以下内容

```
/*
if(!isValidDomain(argv[1])) {
        printf("%s", DOMAINERR);
        exit(1);
}
*/
```

保存编辑后重新 make 一下即可