DNS ENUMERATION

When we start looking at defense or pentesting we often overlook the importance of information gathering, and even with that we often overlook the amount of data available through simple DNS queries. DNS can offer up a lot of information for those who are just willing to look for it. I would like to show you what I mean.

Lets start with the first of the possible tools, *dnsmap* (link in the output below). It basically takes a domain and a wordlist and checks to see what is there. There is a builtin wordlist and I want to use that to show what just some simple checking will show you. For my tests I choose the *eff.org* domain. So lets see what we can see..

```
# ./dnsmap eff.org
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for eff.org using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

bt.eff.org
IP address #1: 64.147.188.11
IP address #2: 64.147.188.3

email.eff.org
IP address #1: 64.147.188.4

irc.eff.org
IP address #1: 75.101.97.68

jabber.eff.org
IP address #1: 75.101.97.68

ns1.eff.org
IP address #1: 64.147.188.9

ns2.eff.org
IP address #1: 64.147.188.6

ns3.eff.org
IP address #1: 64.147.188.13

secure.eff.org
IP address #1: 66.45.103.43

staff.eff.org
IP address #1: 64.147.188.3
IP address #2: 64.147.188.11

staging.eff.org
IP address #1: 64.147.188.3

stats.eff.org
IP address #1: 64.147.188.22

web.eff.org
IP address #1: 64.147.188.7
```

```
web1.eff.org
IP address #1: 64.147.188.10

web2.eff.org
IP address #1: 64.147.188.11

web3.eff.org
IP address #1: 64.147.188.3

webmail.eff.org
IP address #1: 64.147.188.4

www.eff.org
IP address #1: 64.147.188.11
IP address #2: 64.147.188.3

[+] 17 (sub)domains and 20 IP address(es) found
[+] completion time: 1942 second(s)
```

We can see straight away the various web sites, the fact that there is *jabber* and *webmail* and *irc*. Not bad to start with. But I like running different tools to validate results so lets move onto *fierce.pl* (from here). So lets have another look at the *eff.org*...

```
# ./fierce.pl -dns eff.org -threads 3
DNS Servers for eff.org:
        ns2.eff.org
        ns1.eff.org

Trying zone transfer first...
        Testing ns2.eff.org
                Request timed out or transfer not allowed.
        Testing ns1.eff.org
                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 1908 test(s)...
bt.eff.org              alias           eff.org
eff.org address 64.147.188.11
eff.org address 64.147.188.3
64.147.188.0    net-gni.eff.org
64.147.188.1    gw-gni.eff.org
64.147.188.2    db3.eff.org
64.147.188.3    web3.eff.org
64.147.188.4    mail1.eff.org
64.147.188.5    pde.eff.org
64.147.188.6    ns2.eff.org
64.147.188.9    ns1.eff.org
64.147.188.10   web1.eff.org
64.147.188.11   web2.eff.org
64.147.188.3    bt.eff.org
```

```
64.147.188.11   bt.eff.org
email.eff.org           alias           mail1.eff.org
falcon.eff.org          alias           mail1.eff.org
mail1.eff.org   address 64.147.188.4
64.147.188.4    email.eff.org
mail1.eff.org   address 64.147.188.4
64.147.188.4    falcon.eff.org
irc.eff.org             alias           conure.eff.org
conure.eff.org  address 75.101.97.68
75.101.97.66    gw-shotwell.eff.org
lincoln.eff.org         alias           eff.org
75.101.97.68    conure.eff.org
75.101.97.70    wifi.eff.org
75.101.97.68    irc.eff.org
127.0.0.1       localhost.eff.org
eff.org address 64.147.188.11
eff.org address 64.147.188.3
64.147.188.3    lincoln.eff.org
64.147.188.11   lincoln.eff.org
64.147.188.13   ns3.eff.org
office.eff.org          alias           conure.eff.org
conure.eff.org  address 75.101.97.68
75.101.97.68    office.eff.org
projects.eff.org                alias           eff.org
eff.org address 64.147.188.11
eff.org address 64.147.188.3
64.147.188.11   projects.eff.org
64.147.188.3    projects.eff.org
secure.eff.org          alias           eff-live.convio.net
eff-live.convio.net     address 66.45.103.43
staff.eff.org           alias           eff.org
staging.eff.org         alias           web3.eff.org
66.45.103.43    secure.eff.org
stats.eff.org           alias           tbird2.eff.org
eff.org address 64.147.188.11
eff.org address 64.147.188.3
64.147.188.11   staff.eff.org
64.147.188.3    staff.eff.org
switzerland.eff.org             alias           tbird1.eff.org
web3.eff.org    address 64.147.188.3
64.147.188.3    staging.eff.org
tbird1.eff.org  address 64.147.188.21
64.147.188.21   tbird1.eff.org
64.147.188.22   tbird2.eff.org
64.147.188.23   tbird3.eff.org
64.147.188.26   ssl-survey1.eff.org
64.147.188.27   ssl-survey2.eff.org
64.147.188.28   ssl-survey3.eff.org
64.147.188.29   dc-laptop.eff.org
64.147.188.30   nesticle.eff.org
64.147.188.31   bcast-gni.eff.org
tbird2.eff.org  address 64.147.188.22
64.147.188.22   stats.eff.org
64.147.188.21   switzerland.eff.org
```

```
w2.eff.org              alias           eff.org
64.147.188.7    web.eff.org
webmail.eff.org         alias           mail1.eff.org
eff.org address 64.147.188.11
eff.org address 64.147.188.3
64.147.188.11   w2.eff.org
64.147.188.3    w2.eff.org
www.eff.org             alias           eff.org
mail1.eff.org   address 64.147.188.4
64.147.188.4    webmail.eff.org
eff.org address 64.147.188.11
eff.org address 64.147.188.3
64.147.188.3    www.eff.org
64.147.188.11   www.eff.org

Subnets found (may want to probe here using nmap or unicornscan):
        127.0.0.0-255 : 1 hostnames found.
        64.147.188.0-255 : 39 hostnames found.
        66.45.103.0-255 : 1 hostnames found.
        75.101.97.0-255 : 5 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 67 entries.

Have a nice day.
```

Well now, thats nice. A lot more results (my personal favourite is the *wifi* subdomain), a nice output of the ip ranges covered and some manners ("Have a nice day"). So we know a lot more of the *eff* already. But I want to mention at least one more simply becaue it is part of a very popular exploit framework - *metasploit*. *Metasploit* has a bunch of tools within the auxilary branch of modules and one of them is the *dns_enum* tool. So lets try that...

```
# msfcli auxiliary/gather/dns_enum DOMAIN=eff.org NS=8.8.8.8 ENUM_BRT=true E
[*] Please wait while we load the module tree...
[*] Using DNS Server: 8.8.8.8
[*] Retrieving General DNS Records
[*] Domain: eff.org IP Address: 64.147.188.3 Record: A
[*] Domain: eff.org IP Address: 64.147.188.11 Record: A
[*] Start of Authority: ns1.eff.org. IP Address: 64.147.188.9 Record: SOA
[*] Name Server: ns2.eff.org. IP Address: 64.147.188.6 Record: NS
[*] Name Server: ns1.eff.org. IP Address: 64.147.188.9 Record: NS
[*] Name: mail1.eff.org. Preference: 5 Record: MX
[*] Text: v=spf1 mx ptr +include:outboundmail.convio.net ?all , TXT
[*] Running Brute Force against Domain eff.org
[*] Host Name: bt.eff.org IP Address: 64.147.188.3
[*] Host Name: bt.eff.org IP Address: 64.147.188.11
[*] Host Name: email.eff.org IP Address: 64.147.188.4
[*] Host Name: falcon.eff.org IP Address: 64.147.188.4
[*] Host Name: irc.eff.org IP Address: 75.101.97.68
[*] Host Name: lincoln.eff.org IP Address: 64.147.188.11
[*] Host Name: lincoln.eff.org IP Address: 64.147.188.3
[*] Host Name: localhost.eff.org IP Address: 127.0.0.1
[*] Host Name: ns3.eff.org IP Address: 64.147.188.13
[*] Host Name: ns2.eff.org IP Address: 64.147.188.6
[*] Host Name: ns1.eff.org IP Address: 64.147.188.9
```

```
[*] Host Name: office.eff.org IP Address: 75.101.97.68
[*] Host Name: projects.eff.org IP Address: 64.147.188.3
[*] Host Name: projects.eff.org IP Address: 64.147.188.11
[*] Host Name: secure.eff.org IP Address: 66.45.103.43
[*] Host Name: staging.eff.org IP Address: 64.147.188.3
[*] Host Name: stats.eff.org IP Address: 64.147.188.22
[*] Host Name: switzerland.eff.org IP Address: 64.147.188.21
[*] Host Name: w2.eff.org IP Address: 64.147.188.11
[*] Host Name: w2.eff.org IP Address: 64.147.188.3
[*] Host Name: web.eff.org IP Address: 64.147.188.7
[*] Host Name: webmail.eff.org IP Address: 64.147.188.4
[*] Host Name: www.eff.org IP Address: 64.147.188.11
[*] Host Name: www.eff.org IP Address: 64.147.188.3
[*] Performing Zone Transfer against all nameservers in eff.org
[*] Testing Nameserver: ns2.eff.org.
AXFR query, switching to TCP
[*] Zone Transfer Failed
[*] Testing Nameserver: ns1.eff.org.
AXFR query, switching to TCP
[*] Zone Transfer Failed
[*] Enumerating SRV Records for eff.org
```

Not a bad tool, but I have personally had threading problems using it. But it does give a good list of results. Now moving on, lets not forget some simple custom tools. Lets carry our example a bit further. We have seen answers on a couple of subnets, one of which is 64.147.188. So lets slap together a quick bash script..

```
RNG="64.147.188"
START=1
END=40
KEEP=/tmp/kp.1

for x in $(seq $START 1 $END)
 do
  dig -x $RNG.$x +answer +short > $KEEP
  CNT=`cat $KEEP | wc -l`
  if [ "$CNT" = "0" ]
   then
    echo . > /dev/null
   else
    echo "============"
    echo $RNG.$x
    cat $KEEP
  fi
 done

rm -rf $KEEP
```

This will do *dig* queries for every ip in the range you specify. This particular setup gives us..

```
# sh ./bf-ip2dns
============
64.147.188.1
gw-gni.eff.org.
============
64.147.188.2
```

```
db3.eff.org.
============
64.147.188.3
web3.eff.org.
============
64.147.188.4
mail1.eff.org.
============
64.147.188.5
pde.eff.org.
============
64.147.188.6
ns2.eff.org.
============
64.147.188.9
ns1.eff.org.
============
64.147.188.10
web1.eff.org.
============
64.147.188.11
web2.eff.org.
============
64.147.188.21
tbird1.eff.org.
============
64.147.188.22
tbird2.eff.org.
============
64.147.188.23
tbird3.eff.org.
============
64.147.188.26
ssl-survey1.eff.org.
============
64.147.188.27
ssl-survey2.eff.org.
============
64.147.188.28
ssl-survey3.eff.org.
============
64.147.188.29
dc-laptop.eff.org.
============
64.147.188.30
nesticle.eff.org.
============
64.147.188.31
bcast-gni.eff.org.
```

Hmmm. A few more interesting names there. But also remember that companies can own more then one domain, so lets try another custom script..

```
TMP=/tmp/rbtq.txt
IP=$1
```

```
links "http://www.robtex.com/ip/$IP.html#shared" -dump > $TMP

RSLT=`cat $TMP |grep -e "Sorry, we have no information about" 1> /dev/null ; echo $?`
if [ $RSLT = 0 ]
 then
  echo "-no info for $IP"
 else
  ONE=`cat $TMP | grep -n whois | tail -1 | cut -f 1 -d ":"`
  TWO=`cat $TMP | grep -n "IP numbers of host"  | cut -f 1 -d ":"`
  THREE=`expr $ONE - $TWO`
  cat $TMP | grep -A $THREE "IP numbers of host" | grep -v "whois"
 fi
echo "----------------------------------------"
```

Now this rough script queries the nice *robtex.com* site for a given range of ip numbers and shows any shared names - a quick note though, it is not polite to do lots of such queries to a website so unless you put a pause inbetween each check, or route through tor, you may find yourself temporarily blocked. But now lets see what crops up..

```
# for x in $(seq 1 1 40); do  sh ./robtex-qry 64.147.188.$x; done
     IP numbers of host

   64.147.188.1

     PTRs of IP numbers

   gw-gni.eff.org

     Host names sharing IP with A records

   gw-gni.eff.org

                          Host names sharing IP with A records
                                  PTRs of IP numbers
   gw-gni.eff.org         X       X

----------------------------------------
     IP numbers of host

   64.147.188.2

     PTRs of IP numbers

   db3.eff.org

     Host names sharing IP with A records

   db3.eff.org

                        Host names sharing IP with A records
                                PTRs of IP numbers
   db3.eff.org          X       X

----------------------------------------
```

  IP numbers of host

64.147.188.3

  PTRs of IP numbers

web3.eff.org

  Host names sharing IP with A records

eff.com
eff.net
eff.org
panopticlick.eff.org
robin.eff.org
teachingcopyright.net
tor.eff.org
tosback.org
w2.eff.org
web3.eff.org
www.eff.org

                          Host names sharing IP with A records
                                  PTRs of IP numbers
web3.eff.org   X   X

  IP numbers of host

64.147.188.4

  PTRs of IP numbers

mail1.eff.org

  Host names sharing IP with A records

falcon.eff.org
mail1.eff.org

  Domains using this as mail server

copyright-watch.org(primary)
dearaol.com(primary)
eff.com(primary)
eff.net(primary)
eff.org(primary)
freeyourphone.org(primary)
ourvotelive.com(primary)
ourvotelive.info(primary)
ourvotelive.net(primary)
ourvotelive.org(primary)
soundcopyright.eu(primary)
stopthespying.org(primary)

```
                          Host names sharing IP with A records
                                  PTRs of IP numbers
mail1.eff.org             X       X

-----------------------------------------
     IP numbers of host

   64.147.188.5

     PTRs of IP numbers

   pde.eff.org

     Host names sharing IP with A records

   pde.eff.org

                         Host names sharing IP with A records
                                 PTRs of IP numbers
   pde.eff.org           X       X

-----------------------------------------
     IP numbers of host

   64.147.188.6

     PTRs of IP numbers

   ns2.eff.org

     Host names sharing IP with A records

   ns2.eff.org

     Domains using this as name server

   4brad.com
   callerapp.com
   copycrime.org
   copyright-watch.org
   directvdefense.org
   eff.com
   eff.net
   eff.org
   freeyourphone.org
   ksml.com
   netfunny.com
   orphanworks.com
   orphanworks.org
   ourvotelive.com
   ourvotelive.info
   ourvotelive.net
   ourvotelive.org
```

```
   robocars.net
   slowfeed.net
   soundcopyright.eu
   stopthespying.org
   teachingcopyright.net
   teachingcopyright.org
   templetons.com
   tosback.com
   tosback.net
   tosback.org
   tytempleton.com
   zer0.org

                        Host names sharing IP with A records
                                PTRs of IP numbers
   ns2.eff.org          X       X

-----------------------------------------
-no info for 64.147.188.7
-----------------------------------------
-no info for 64.147.188.8
-----------------------------------------
     IP numbers of host

   64.147.188.9

     PTRs of IP numbers

   ns1.eff.org

     Host names sharing IP with A records

   ns1.eff.org

     Domains using this as name server

   copycrime.org
   copyright-watch.org
   directvdefense.org
   eff.com
   eff.net
   eff.org
   freeyourphone.org
   orphanworks.com
   orphanworks.org
   ourvotelive.com
   ourvotelive.info
   ourvotelive.net
   ourvotelive.org
   soundcopyright.eu
   stopthespying.org
   teachingcopyright.net
   teachingcopyright.org
   tosback.com
```

```
   tosback.net
   tosback.org
   zer0.org

                        Host names sharing IP with A records
                                PTRs of IP numbers
   ns1.eff.org          X       X

-----------------------------------------
  IP numbers of host

64.147.188.10

  PTRs of IP numbers

web1.eff.org

  Host names sharing IP with A records

copycrime.org
copyright-watch.org
directvdefense.org
freeyourphone.org
orphanworks.com
orphanworks.org
ourvotelive.com
ourvotelive.info
ourvotelive.net
ourvotelive.org
soundcopyright.eu
stopthespying.org
teachingcopyright.org
tosback.com
tosback.net
web1.eff.org
www.copyright-watch.org
www.tosback.org

                          Host names sharing IP with A records
                                  PTRs of IP numbers
web1.eff.org              X       X

-----------------------------------------
  IP numbers of host

64.147.188.11

  PTRs of IP numbers

web2.eff.org

  Host names sharing IP with A records

copycrime.org
```

copyright-watch.org
eff.com
eff.net
eff.org
orphanworks.com
orphanworks.org
ourvotelive.com
ourvotelive.info
ourvotelive.net
ourvotelive.org
panopticlick.eff.org
stopthespying.org
teachingcopyright.net
teachingcopyright.org
tor.eff.org
tosback.com
tosback.net
tosback.org
w2.eff.org
web2.eff.org
www.copyright-watch.org
www.eff.org
www.tosback.org

	Host names sharing IP with A records	PTRs of IP numbers
web2.eff.org	X	X

-no info for 64.147.188.12

-no info for 64.147.188.13

-no info for 64.147.188.14

-no info for 64.147.188.15

-no info for 64.147.188.16

-no info for 64.147.188.17

-no info for 64.147.188.18

-no info for 64.147.188.19

-no info for 64.147.188.20

-no info for 64.147.188.21

-no info for 64.147.188.22

-no info for 64.147.188.23

IP numbers of host

64.147.188.24

  Host names sharing IP with A records

tbird4.eff.org
tbird4.ourvotelive.org

-no info for 64.147.188.25

-no info for 64.147.188.26

-no info for 64.147.188.27

-no info for 64.147.188.28

-no info for 64.147.188.29

-no info for 64.147.188.30

  IP numbers of host

64.147.188.31

  PTRs of IP numbers

bcast-gni.eff.org

  Host names sharing IP with A records

bcast-gni.eff.org

	Host names sharing IP with A records	PTRs of IP numbers
bcast-gni.eff.org	X	X

-no info for 64.147.188.32

-no info for 64.147.188.33

-no info for 64.147.188.34

-no info for 64.147.188.35

-no info for 64.147.188.36

-no info for 64.147.188.37

-no info for 64.147.188.38

-no info for 64.147.188.39

```
-no info for 64.147.188.40
----------------------------------------
```

And now you can see that there are a few more domains that are also used. If this was a proper attack, these domain names would be fed back into the start of the cycle by checking for other records for those newly discovered domains.

So what we have done with some simple tests and non-intrusive tests is get a lot better idea of what is there, and what other linkages there may be.