

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Scanning the world for DNS in under an hour.](#)

Vaider - May 31, 2014, 1:47 am

Easy DNS list scanning!

Aye, welcome to my thread..

Alright lets get right too it..

Things needed:

1. 1Gbps port server (vps or dedi will work)
2. perl (with Net::DNS, Net::Pcap, Net::Pcap::Easy)
3. A Brain
5. Zmap

Table of Contents:

0x1: Getting Ready

0x2: Building Packet

0x3: Starting Filter

0x4: Starting Scan

0x5: Manually Filtering Output

0x1 - Getting Ready:

Step 1: Download Perl on your server:

Debain / Ubuntu:

Code apt-get install perlRedhat / Centos:

Code yum install perl

Step 2: Install Perl modules:

Debain / Ubuntu:

Code apt-get install cpan

cpan install Net::DNS

cpan install Net::Pcap

cpan install Net::Pcap::Easy

Redhat / Centos:

Code yum install cpan

cpan install Net::DNS

cpan install Net::Pcap

cpan install Net::Pcap::Easy

If this does not work use commands below

Code wget http://search.cpan.org/CPAN/authors/id/S/SA/SAPER/Net-Pcap-0.17.tar.gz

tar -xvf Net-Pcap-0.17.tar.gz

cd Net-Pcap-0.17

perl Makefile.pl

make

make install

cd ../

rm -rf Net-Pcap-0.17*

wget http://search.cpan.org/CPAN/authors/id/J/JE/JETTERO/Net-Pcap-Easy-1.4207.tar.gz

```
tar -xvf Net-Pcap-Easy-1.4207.tar.gz
cd Net-Pcap-Easy-1.4207
perl Makefile.pl
make
make install
cd ../
rm -rf Net-Pcap-Easy*
```

```
wget http://search.cpan.org/CPAN/authors/id/N/NL/NLNETLABS/Net-DNS-0.76.tar.gz
tar -xvf Net-DNS-0.76.tar.gz
cd Net-DNS-0.76
perl Makefile.pl
make
make install
cd ../
rm -rf Net-DNS-0.76*
```

Step 3: Install Zmap:

Debian / Ubuntu:

Code apt-get install build-essential cmake libgmp3-dev libpcap-dev gengetopt byacc flex
Redhat / Centos:

Code yum install cmake gmp gmp-devel libpcap-devel gengetopt byacc flex

Then Download and install zmap:

Code wget https://github.com/zmap/zmap/archive/v1.2.0.tar.gz

```
tar -xvf v1.2.0.tar.gz
```

```
cd zmap-1.2.0
```

```
cmake -DENABLE_HARDENING=ON
```

```
make
```

```
make install
```

Ok, we are done with installing the things we need C:

0x2 - Building Packet:

Here we are going to use one of my scripts to build a packet to use with zmap.

This will include the domain your going to use to scan..

Step 1: Download buildpacket.pl

Quote:wget <https://raw.githubusercontent.com/Vypor/DnsScanTutorial/master/buildpacket.pl>

Script Usage:

Code root@localhost:~# perl buildpacket.pl

Usage: perl buildpacket.pl <domain>

Example: perl buildpacket.pl 1x1.cz

Coded by Vypor, <https://github.com/Vypor>

Step 2: Build the packet with the script (this is easy)

Now we gotta build the packet for zmap to use. this can be done by simply typing:

Code perl buildpacket.pl domain.com

domain.com is the domain your going to use to amp

Anyways, To the next step!

0x3 - Starting Filter:

Step 1: Download dnsfilter.pl

Code wget https://raw.githubusercontent.com/Vypor/DnsScanTutorial/master/DNSfilter.pl

Step 2: run the filter script

Must be ran before scan starts to get full scan

Code perl DNSfilter.pl dnslistoutput.txt 3000 1x1.cz

Note, the domain MUST be the same one you used in your buildpacket.pl

Code root@localhost:~# perl filt.pl

Usage: perl filter.pl <outputfile> <minbytereplay> <domain>

Example: perl filter.pl output.txt 3000 1x1.cz

Coded by Vypor, <https://github.com/Vypor>

0x4 - Starting Scan:

Woo! you made it here, congrats..

Now we gotta start the dns scan itself, Before this make sure your dnsfilter.pl script is running, and open a new window in your server with your SSH program.

Step 1: Run zmap and listen for data on other screen

Alright, we need to run zmap.. this is easy command is below.

Code zmap -M udp -p 53 --probe-args=file:1x1.cz.pkt

Now, 1x1.cz.pkt is where your buildpacket.pl output is (in the same folder as buildpacket.pl)

After your run the command you will begin to see this on your screen:

root@localhost:~# zmap -M udp -p 53 --probe-args=file:1x1.cz.pkt

Code May 31 10:07:04.554 [INFO] zmap: output module: csv

May 31 10:07:04.554 [WARN] csv: no output file selected. no results will be provided.

0:01 0%; send: 875419 875 Kp/s (772 Kp/s avg); recv: 1182 1.18 Kp/s (1.04 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.14%

0:02 0%; send: 1750345 875 Kp/s (820 Kp/s avg); recv: 2761 1.58 Kp/s (1.29 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.16%

0:03 0%; send: 2626753 876 Kp/s (838 Kp/s avg); recv: 4411 1.65 Kp/s (1.41 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.17%

0:04 0%; send: 3501963 875 Kp/s (847 Kp/s avg); recv: 6071 1.66 Kp/s (1.47 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.17%

0:05 0% (1h12m left); send: 4377578 876 Kp/s (852 Kp/s avg); recv: 7817 1.75 Kp/s (1.52 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.18%

0:06 0% (1h12m left); send: 5251892 874 Kp/s (856 Kp/s avg); recv: 9418 1.60 Kp/s (1.53 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.18%

0:07 0% (1h11m left); send: 6120570 869 Kp/s (858 Kp/s avg); recv: 11068 1.65 Kp/s (1.55 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.18%

0:08 0% (1h11m left); send: 6986364 866 Kp/s (859 Kp/s avg); recv: 12727 1.66 Kp/s (1.56 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.18%

0:09 0% (1h11m left); send: 7851315 865 Kp/s (859 Kp/s avg); recv: 14365 1.64 Kp/s (1.57 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.18%

0:10 0% (1h11m left); send: 8717009 866 Kp/s (860 Kp/s avg); recv: 15985 1.62 Kp/s (1.58 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.18%

0:11 0% (1h11m left); send: 9585269 868 Kp/s (861 Kp/s avg); recv: 17805 1.82 Kp/s (1.60 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.19%

0:12 0% (1h11m left); send: 10455611 870 Kp/s (861 Kp/s avg); recv: 19565 1.76 Kp/s (1.61 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.19%

0:13 0% (1h11m left); send: 11325755 870 Kp/s (862 Kp/s avg); recv: 21230 1.66 Kp/s (1.62 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.19%

0:14 0% (1h11m left); send: 12196419 871 Kp/s (863 Kp/s avg); recv: 22900 1.67 Kp/s (1.62 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.19%

0:15 0% (1h11m left); send: 13068931 872 Kp/s (863 Kp/s avg); recv: 24676 1.77 Kp/s (1.63 Kp/s

avg); drops: 0 p/s (0 p/s avg); hits: 0.19%

0:16 0% (1h11m left); send: 13938015 869 Kp/s (864 Kp/s avg); recv: 26355 1.68 Kp/s (1.63 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.19%

0:17 0% (1h11m left); send: 14812427 874 Kp/s (864 Kp/s avg); recv: 28074 1.72 Kp/s (1.64 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.19%

0:18 0% (1h11m left); send: 15683980 871 Kp/s (865 Kp/s avg); recv: 29779 1.70 Kp/s (1.64 Kp/s avg); drops: 0 p/s (0 p/s avg); hits: 0.19%

May 31 10:07:23.717 [WARN] monitor: Dropped 1841 packets in the last second, (1842 total dropped (pcap: 1842 + iface: 0))

0:19 0% (1h11m left); send: 16479319 795 Kp/s (861 Kp/s avg); recv: 31350 1.57 Kp/s (1.64 Kp/s avg); drops: 1.84 Kp/s (96 p/s avg); hits: 0.19%

Its fine if packets drop. it WILL happen..

Now, look on the screen running DNSfilter.pl it will look something like this:

```
Code root@localhost:~# perl DNSfilter.pl output.txt 1000 1x1.cz
```

```
10:07:31 193.239.186.91 ->X.X.X.X 1764
```

```
10:07:31 89.174.18.233 ->X.X.X.X 1472
```

```
10:07:31 79.133.62.62 ->X.X.X.X 1764
```

```
10:07:31 163.20.133.1 ->X.X.X.X 4094
```

```
10:07:31 113.160.24.26 ->X.X.X.X 1248
```

```
10:07:31 5.70.201.32 ->X.X.X.X 1113
```

```
10:07:31 197.164.20.131 ->X.X.X.X 1508
```

```
10:07:31 203.146.152.189 ->X.X.X.X 1082
```

```
10:07:31 179.192.243.146 ->X.X.X.X 3994
```

```
10:07:31 208.58.53.99 ->X.X.X.X 4038
```

```
10:07:31 83.69.88.178 ->X.X.X.X 4027
```

```
10:07:31 125.177.151.92 ->X.X.X.X 1127
```

```
X.X.X.X Is my server IP, its removed
```

The filter script is formatted:

Code Time : Incoming_IP -> Outgoing_IP bytesizeBut the output will be just like a regular DNS list:

```
Code 193.239.186.91 1x1.cz 1764
```

```
89.174.18.233 1x1.cz 1472
```

```
79.133.62.62 1x1.cz 1764
```

```
163.20.133.1 1x1.cz 4094
```

```
113.160.24.26 1x1.cz 1248
```

```
5.70.201.32 1x1.cz 1113
```

```
197.164.20.131 1x1.cz 1508
```

```
203.146.152.189 1x1.cz 1082
```

```
179.192.243.146 1x1.cz 3994
```

```
208.58.53.99 1x1.cz 4038
```

```
83.69.88.178 1x1.cz 4027
```

```
125.177.151.92 1x1.cz 1127
```

C: Now that we have our list, we have an extra option.. We can Manually filter it.

0x5 - Manually Filtering Output:

Step 1: Find your DNS list file

Step 2: Use your linux command line and sort your list.

Now the command below will do things, first thing being reading the list, then filtering the third column, then sorting for duplicates, then randomizing the list, and finally the output file.

Now lets say your list name is dnslist.txt and you want to sort it to everything above 4000 bytesize, and then output it to newdnslist.txt heres the command:

```
Code cat dnslist.txt | awk '$3 >= 4000' | sort -u | sort -R > newdnslist.txt
```

Command Explanation: "cat" reads the file into a pipe "|", awk then sorts \$3 "the third column" for any number 4000 and over, then it pipes again, sorts for unique lines, then pipes, and randomizes the lines of the list, then ">" outputs the lines to a file.

Tutorial Made by Vypor, Also made so it can be easily modified for other amp methods.

<https://github.com/Vypor>

Addressed Issues:

(May 31, 2014 10:56 PM)ItsFluffy Wrote: [\[CITE\]](#) Ok following the tut I thought this was nothing but it prevents me from using the filter properly:

```
[root@2 ~]# cd zmap-1.2.0
[root@2 zmap-1.2.0]# cmake -DENABLE_HARDENING=ON
-- Configuring done
-- Generating done
-- Build files have been written to: /root/zmap-1.2.0
```

```
[root@2 zmap-1.2.0]# make
[ 2%] Generating zopt.h
/bin/sh: gengetopt: command not found
make[2]: * [src/zopt.h] Error 127
make[1]: * [src/CMakeFiles/zmap.dir/all] Error 2
make: * [all] Error 2
```

```
[root@2 zmap-1.2.0]# make
[ 2%] Generating zopt.h
/bin/sh: gengetopt: command not found
make[2]: * [src/zopt.h] Error 127
make[1]: * [src/CMakeFiles/zmap.dir/all] Error 2
make: * [all] Error 2
```

```
[root@2 zmap-1.2.0]# make install
[ 2%] Generating zopt.h
/bin/sh: gengetopt: command not found
make[2]: * [src/zopt.h] Error 127
make[1]: * [src/CMakeFiles/zmap.dir/all] Error 2
make: * [all] Error 2This is a zmap build error, "/bin/sh: gengetopt: command not found"
To fix this error read below.
```

Centos 5:

```
Code wget http://dl.fedoraproject.org/pub/epel/5/x86_64/epel-release-5-4.noarch.rpm
wget http://rpms.famillecollet.com/enterprise/remi-release-5.rpm
sudo rpm -Uvh remi-release-5*.rpm epel-release-5*.rpm
yum install gengetopt
```

Centos 6:

```
Code wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
wget http://rpms.famillecollet.com/enterprise/remi-release-6.rpm
sudo rpm -Uvh remi-release-6*.rpm epel-release-6*.rpm
```

yum install gengetopt
Debian / Ubuntu:
Code apt-get install gengetopt

7H3 3XP3R7 - May 31, 2014, 2:01 am

ah that is nice Vypor :) let me know if you have priv8 shits for sale..

Phenomite - May 31, 2014, 2:25 am

Cool stuff vypor. But seriously stop making so many accounts lol.

I'm also running into an issue prior to seeing this where my /etc/zmap folder exists but when I go to read in it or delete it, it doesnt exist >_<.

Vaider - May 31, 2014, 2:30 am

(May 31, 2014 02:25 AM)Phenomite Wrote: [\[CITE\]](#) Cool stuff vypor. But seriously stop making so many accounts lol.

I'm also running into an issue prior to seeing this where my /etc/zmap folder exists but when I go to read in it or delete it, it doesnt exist >_<.

I like accounts..

Reinstall your server man.
or install zmap from source and define a diffrent install location.

Pepe goes REEEEEEEEEEEEEEEEE - May 31, 2014, 3:12 am

Nice Vypor, this is working and is better than most paid for scanners, but you still smell like egg salad.

Mority - May 31, 2014, 3:16 am

Great tutorial man, I appreciate the hard work you have put in!

Proxseas - May 31, 2014, 4:29 am

Vouch after 5 minutes of scanning lmfaoo

ItsFluffy - May 31, 2014, 8:45 am

Nice tut I'm going to be bookmarking this to try tonight

Vaider - May 31, 2014, 9:49 am

Yeah, after testing a few times on a few different servers.. it takes about 3 hours to scan the world for dns servers with your specific domain.

OwnerORAdminPlease - May 31, 2014, 12:28 pm

Vouch for this! I scanned the whole world soooo fast!

SMTP Server - May 31, 2014, 3:19 pm

Thanks for the tutorial, i scanned dns and got a nice list, mya1

Phenomite - May 31, 2014, 8:57 pm

Why pay for DNS scanners when this is 500x faster, better, stronger, longer, sexier, and more annoying to setup on centos than anything else!

Aka do not buy ddosDev scanner, wasteful.

ItsFluffy - May 31, 2014, 10:56 pm

Ok following the tut I thought this was nothing but it prevents me from using the filter properly:

```
[root@2 ~]# cd zmap-1.2.0
[root@2 zmap-1.2.0]# cmake -DENABLE_HARDENING=ON
-- Configuring done
-- Generating done
-- Build files have been written to: /root/zmap-1.2.0
```

```
[root@2 zmap-1.2.0]# make
[ 2%] Generating zopt.h
/bin/sh: gengetopt: command not found
make[2]: * [src/zopt.h] Error 127
make[1]: * [src/CMakeFiles/zmap.dir/all] Error 2
make: * [all] Error 2
```

```
[root@2 zmap-1.2.0]# make
[ 2%] Generating zopt.h
/bin/sh: gengetopt: command not found
make[2]: * [src/zopt.h] Error 127
make[1]: * [src/CMakeFiles/zmap.dir/all] Error 2
make: * [all] Error 2
```

```
[root@2 zmap-1.2.0]# make install
[ 2%] Generating zopt.h
/bin/sh: gengetopt: command not found
make[2]: * [src/zopt.h] Error 127
make[1]: * [src/CMakeFiles/zmap.dir/all] Error 2
make: * [all] Error 2
```

Vaider - May 31, 2014, 11:14 pm

(May 31, 2014 10:56 PM)ItsFluffy Wrote: [CITE](#) Ok following the tut I thought this was nothing but it prevents me from using the filter properly:

```
[root@2 ~]# cd zmap-1.2.0
[root@2 zmap-1.2.0]# cmake -DENABLE_HARDENING=ON
-- Configuring done
-- Generating done
-- Build files have been written to: /root/zmap-1.2.0
```

```
[root@2 zmap-1.2.0]# make
[ 2%] Generating zopt.h
/bin/sh: gengetopt: command not found
make[2]: * [src/zopt.h] Error 127
make[1]: * [src/CMakeFiles/zmap.dir/all] Error 2
make: * [all] Error 2
```

```
[root@2 zmap-1.2.0]# make
[ 2%] Generating zopt.h
/bin/sh: gengetopt: command not found
make[2]: * [src/zopt.h] Error 127
make[1]: * [src/CMakeFiles/zmap.dir/all] Error 2
make: * [all] Error 2
```

```
[root@2 zmap-1.2.0]# make install
[ 2%] Generating zopt.h
/bin/sh: gengetopt: command not found
make[2]: * [src/zopt.h] Error 127
make[1]: * [src/CMakeFiles/zmap.dir/all] Error 2
make: * [all] Error 2
I have addressed your issue with a fix at the bottom of my thread.
```

ItsFluffy - June 1, 2014, 4:07 am

ok thanks for solving that matter, that worked nicely, when trying to packetbuild -->

```
perl buildpacket.pl mydomainnamehere
Net::DNS::Header::size: no such method at buildpacket.pl line 18
```

Vaider - June 1, 2014, 3:05 pm

(Jun 1, 2014 04:07 AM)ItsFluffy Wrote: [\[CITE\]](#) ok thanks for solving that matter, that worked nicely, when trying to packetbuild -->

```
perl buildpacket.pl mydomainnamehere
Net::DNS::Header::size: no such method at buildpacket.pl line 18
```

Thats an issue with how you installed Net::DNS, these scripts are made for debain / ubuntu but you can use them for centos, and redhat.. its just annoying

Phenomite - June 1, 2014, 3:26 pm

(Jun 1, 2014 03:05 PM)iVivIVs Wrote: [\[CITE\]](#) Thats an issue with how you installed Net::DNS, these scripts are made for debain / ubuntu but you can use them for centos, and redhat.. its just annoying
Annoying yes, I watched you do it to my server and it was a bloody nuisance lol. Especially when cpan was bugging out.

ItsFluffy - June 1, 2014, 6:41 pm

(Jun 1, 2014 03:05 PM)iVivIVs Wrote: [\[CITE\]](#) Thats an issue with how you installed Net::DNS, these scripts are made for debain / ubuntu but you can use them for centos, and redhat.. its just annoying
so is there any particular correction i should be trying to make?

Gary The Goat - February 22, 2016, 11:28 am

Hey,

I am having a problem here:

```
Code [root@localhost dns]# perl DNSfilter.pl dnslistoutput.txt 3000 1x1.cz
Can't locate Net/Netmask.pm in @INC (@INC contains: /usr/local/lib64/perl5 /usr/local/share/perl5
/usr/lib64/perl5/vendor_perl /usr/share/perl5/vendor_perl /usr/lib64/perl5 /usr/share/perl5 .) at
/usr/local/share/perl5/Net/Pcap/Easy.pm line 10.
BEGIN failed--compilation aborted at /usr/local/share/perl5/Net/Pcap/Easy.pm line 10.
Compilation failed in require at DNSfilter.pl line 4.
BEGIN failed--compilation aborted at DNSfilter.pl line 4.
Any ideas how I can fix this?[/code]
```