

Forum:[Hack Forums](#)

Thread: [\[The Empire\] \[Tutorial\] How To Steal Amp Lists From Popular Stressers](#)

regexks_ - February 18, 2013, 10:45 pm

Requirements

Hardware:

a dedi or VPS with some form of Linux installed (I'll be using my dedi with Debian Squeeze)

Software:

a network monitor (I'll be using iptraf)

a text editor (nano is fine)

screen

grep

sort

uniq

cat (maybe)

Idea

DNS reflection attacks utilize small, spoofed DNS queries for large amounts of information from open recursive name servers that return this large response to a target. These attacks rely on a fairly large list of these open recursive name servers to query, which, in reality, are fairly easy to scan for and compile into a list. Some users decide to sell these lists and profit off of them though. Naughty naughty. Now there are plenty of guides and utilities online to gather this data yourself but why not just steal tried and tested lists from existing stressers that are using them?

Like I mentioned above, the attack utilizes open recursive name servers to do its dirty work. These servers are sending large amounts of UDP traffic right at a target. Who's to say I can't just log the traffic hitting my server and parse that data to find every single open recursive name server utilized by the attack? Why can't I just SE stressers or use accounts to hit my server for a few minutes to gather this information quickly?

Process

1. SSH into the dedi/VPS and start up iptraf in screen (you don't want your SSH socket to close and have your iptraf process killed! You can just reattach to the detached session in the case of a disconnect)

2. Go into Configure... and make sure Logging is set to On

3. Start up an IP traffic monitor session on all interfaces (or eth0 if you want to keep the list a little less bulky) and specify a location for the log to be saved

4. Hit your server. I suggest hitting the server for 5-10 minutes (most 100Mb dedis will get completely assfucked by most attacks so you'll see your SSH session freeze or even disconnect for the duration). Stop logging after the attack completes (you'll know when your server starts responding again). It's time to parse the logs.

5. I have some logs from previous attacks which I can go ahead and show you some data from. I'll be using Formality Stresser as an example

So you have your log... but none of this data is usable... yet. "There are words and duplicates and OH MY GOD REGEXKS WHAT DO I DO WITH THIS LOG?" We'll have to pass it through some stuff to get the data we need. This is easy with some piping!

```
Code grep -Eo "[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}:53" formalitystresser1.log | sort -n | uniq |  
grep -Eo "[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}" > finaldnslist.txt
```

Using some simple regular expressions, sort and uniq you've managed to pull only the IP address ending in port 53 (the port name servers use), list them all in numerical order (mostly to get all the duplicates right next to each other) and merge all the duplicates! You're a god!

ENJOY YOUR FREE AMP LISTS

Oh and you can use cat to merge lists if you ever need to.

Zanelot - February 18, 2013, 10:47 pm

Vouch for this method, it works, and I've personally used it.

Starfall - February 18, 2013, 11:00 pm

Very impressive. Can be done with SNMP reflectors as well, just change the port you're looking for

Whiteh4t - February 18, 2013, 11:17 pm

so you attack your own server and capture traffic from?.

TheNeutron - February 18, 2013, 11:50 pm

Pretty cool & interesting tutorial... Thanks mate :)

phlow - February 18, 2013, 11:57 pm

Very interesting. Thanks for the tutorial.

ItsFluffy - February 19, 2013, 12:22 am

talk about a well done tut
nice work man

regexks_ - February 19, 2013, 6:05 am

Thanks for the good feedback guys. Keep it coming

CarrotMilk - February 19, 2013, 11:49 am

Actually a really cool tutorial there, bud. Nice work :)

Deadlydennis - February 19, 2013, 3:20 pm

Thanks for posting this very nice well written tutorial. Nice work

regexks_ - February 20, 2013, 12:06 am

Thanks for the feed back nerds. Keep it coming and let me know if you've stolen some good lists!

ca9a2536fd8b17df76f7ee082 - February 20, 2013, 12:07 am

Nice job, Keep up the HQ posts man!

Mindpower - February 20, 2013, 12:16 am

Wow this was a very good tutorial, Good job! :)

Dolan. - February 20, 2013, 12:21 am

Thanks for the tutorial, going to bookmark it for future use c:

RyanC - February 20, 2013, 12:35 am

I'd be rather shocked if this wouldn't be obvious to anyone with a brain.

#Skyline - February 20, 2013, 1:25 am

Don't forget, you need there FTP password to actually hack.

Spoiler ([Click to View](#)) lol

Hikki - February 20, 2013, 1:28 am

Thanks for this. Helped me alot ?

KyleWTF - February 20, 2013, 7:11 am

(Feb 20, 2013 01:35 AM)Who? Wrote: [\[CITE\]](#) I'd be rather shocked if this wouldn't be obvious to anyone with a brain.

We are on HackForums ?

In all seriousness, this isn't really a hacking site..

regexks_ - February 20, 2013, 8:39 am

(Feb 20, 2013 01:35 AM)Who? Wrote: [\[CITE\]](#) I'd be rather shocked if this wouldn't be obvious to anyone with a brain.

Well then, be shocked since brains are a luxury

RyanC - February 20, 2013, 8:51 am

(Feb 20, 2013 08:11 AM)KyleWTF Wrote: [\[CITE\]](#) We are on HackForums ?

In all seriousness, this isn't really a hacking site..

That statement will be true once there's more posts in the "LOL I LACK A SOCIAL LIFE IRL SO I'LL

BLOG ABOUT IT ON HACKFORUMS" section than the hacking sections.

regexks_ - February 23, 2013, 3:57 pm

Back to the top.

I'd like to see someone put this to use and show us some logs and stats!

În??DiOuS - March 28, 2013, 2:31 pm

Vouch for this, just beaware don't do dstats with randoms! they will steal your amps!

regexks_ - March 28, 2013, 2:32 pm

(Mar 28, 2013 02:31 PM)_ÎnSiDiOuS_ Wrote: [\[CITE\]](#) Vouch for this, just beaware don't do dstats with randoms! they will steal your amps!

A quick vouch for this! Strangers will touch your attacks in places and they will take your whole list :(even the ones you've paid for!

În??DiOuS - March 28, 2013, 2:53 pm

(Mar 28, 2013 02:32 PM)regexks_ Wrote: [\[CITE\]](#) A quick vouch for this! Strangers will touch your attacks in places and they will take your whole list :(even the ones you've paid for!

As I found out the hard way :(

Oh well, :(

PandaVenom - March 29, 2013, 7:50 am

Sweet! This could get insanely good AMP lists

regexks_ - March 30, 2013, 7:06 am

(Mar 29, 2013 07:50 AM)Suedadam Wrote: [\[CITE\]](#) Sweet! This could get insanely good AMP lists
You just need to know how to filter them :D

Gabrielix - March 30, 2013, 7:10 am

Great tutorial, seriously.

It's worth your while looking at: <http://openresolverproject.org/> too

regexks_ - March 30, 2013, 9:07 am

(Mar 30, 2013 07:10 AM)Gabrielix Wrote: [\[CITE\]](#) Great tutorial, seriously.

It's worth your while looking at: <http://openresolverproject.org/> too

Lol, I'm thinking of starting a project like that listing some of the millions of open revolvers I've scanned over time.

on-silo - March 30, 2013, 9:10 am

Awesome share, really interesting, interested in testing this.

Sib3r - April 18, 2013, 7:31 am

This is a amazing idea man good job explaining it.