

Forum:[Hack Forums](#)

Thread: [Best ways of collecting ip addresses](#)

EnsoXo - June 7, 2023, 4:20 am

What are some of the best methods on collecting large lists of ips?

Dread.Reaper - June 7, 2023, 4:31 am

(Jun 7, 2023 04:20 AM)EnsoXo Wrote: [\[CITE\]](#) What are some of the best methods on collecting large lists of ips?

... For what purposes?

EnsoXo - June 7, 2023, 6:12 am

(Jun 7, 2023 04:31 AM)Dread.Reaper Wrote: [\[CITE\]](#) ... For what purposes?

Ssh brute force

Dread.Reaper - June 7, 2023, 6:22 am

(Jun 7, 2023 06:12 AM)EnsoXo Wrote: [\[CITE\]](#) Ssh brute force

Scan enterprise netblocks...

DramaKing - June 7, 2023, 4:53 pm

Shodan, Censys, Thingful... Or just do something that isn't a waste of time.

Piplup - June 7, 2023, 8:47 pm

Shodan and scanning candidate netblocks. Easy scripts to write, given that IPs are easily enumerable.

Ducky - June 7, 2023, 9:05 pm

You mentioned looking for ssh targets - look into masscan, I think you'll find what you're looking for.

Disarray"" - June 7, 2023, 9:51 pm

Yeah sounds like you would like masscan.

walle - June 7, 2023, 11:35 pm

iplogger php on some well known site

DramaKing - June 8, 2023, 5:35 am

(Jun 7, 2023 11:35 PM)walle Wrote: [\[CITE\]](#) iplogger php on some well known site

If OP wanted random IPs, he could make them up himself.

Dread.Reaper - June 8, 2023, 5:40 am

(Jun 8, 2023 05:35 AM)DramaKing Wrote: [\[CITE\]](#) If OP wanted random IPs, he could make them up himself.

To be fair all OPs said is he wants to SSH brute.

He does not seem to have much more of a designation after that point. lol

Hacker0x00 - June 8, 2023, 5:42 am

Code `zmap -p 22 > ips.list`

This one liner might start to solve many of your problems.

Dread.Reaper - June 8, 2023, 6:00 am

(Jun 8, 2023 05:42 AM)Hacker0x00 Wrote: [\[CITE\]](#) Code `zmap -p 22 > ips.list`

This one liner might start to solve many of your problems.

ah yes... the magical ip.list

Tell me good sir, would that file not contain the exact same thing OP is asking to obtain to begin with?

... Not suite sure how this helps OPs case in any sort of manner.

Hacker0x00 - June 17, 2023, 8:27 am

(Jun 8, 2023 06:00 AM)Dread.Reaper Wrote: [\[CITE\]](#) ah yes... the magical ip.list

Tell me good sir, would that file not contain the exact same thing OP is asking to obtain to begin with?

... Not suite sure how this helps OPs case in any sort of manner.

zmap is a popular network scanner that when ran with the options I specified in that one liner (port 22, a common SSH server port) will SYN scan the entire IPv4 network space on port 22 and write the responding IP addresses into a file called ip.list.

Surprising this just so happens to be the magical IP list he was looking for if he figures out how to install zmap on his system.

Dread.Reaper - June 17, 2023, 8:39 am

(Jun 17, 2023 08:27 AM)Hacker0x00 Wrote: [\[CITE\]](#) zmap is a popular network scanner that when ran with the options I specified in that one liner (port 22, a common SSH server port) will SYN scan the entire IPv4 network space on port 22 and write the responding IP addresses into a file called ip.list.

Surprising this just so happens to be the magical IP list he was looking for if he figures out how to install zmap on his system.

You gonna scan the entirety of IPv4....

Have fun with that.

Hacker0x00 - June 17, 2023, 8:43 am

(Jun 17, 2023 08:39 AM)Dread.Reaper Wrote: [\[CITE\]](#) You gonna scan the entirety of IPv4....

Have fun with that.

People do it all the time, every day, 365 days a year.

A 1 Gbps network line pushes 1.2 million packets per second. Since we know there are only 4 billion IPv4 addresses we can easily estimate it would take around 4000 seconds or a little more than an hour to SYN scan the entire internet on a common 1 Gbps dedicated line.

Dread.Reaper - June 17, 2023, 8:47 am

(Jun 17, 2023 08:43 AM)Hacker0x00 Wrote: [\[CITE\]](#) People do it all the time, every day, 365 days a year.

A 1 Gbps network line pushes 1.2 million packets per second. Since we know there are only 4 billion IPv4 addresses we can easily estimate it would take around 4000 seconds or a little more than an hour to SYN scan the entire internet on a common 1 Gbps dedicated line.

Come back in an hour with an accurate list please.

Hacker0x00 - June 17, 2023, 8:55 am

(Jun 17, 2023 08:47 AM)Dread.Reaper Wrote: [\[CITE\]](#) Come back in an hour with an accurate list please.

How much are you going to pay for that list?

Shouldn't we talk business within private messages?

Since you doubt that it's possible, it's likely you have never tried using a network scanner outside of a small netblock before.

Dread.Reaper - June 17, 2023, 8:59 am

(Jun 17, 2023 08:55 AM)Hacker0x00 Wrote: [\[CITE\]](#) How much are you going to pay for that list?

Shouldn't we talk business within private messages?

Since you doubt that it's possible, it's likely you have never tried using a network scanner outside of a small netblock before.

Theres no business here, if its that easy and only takes an hour should have no problem running a scan to show us. ?

DramaKing - June 17, 2023, 12:18 pm

(Jun 17, 2023 08:43 AM)Hacker0x00 Wrote: [\[CITE\]](#) People do it all the time, every day, 365 days a year.

A 1 Gbps network line pushes 1.2 million packets per second. Since we know there are only 4 billion IPv4 addresses we can easily estimate it would take around 4000 seconds or a little more than an hour to SYN scan the entire internet on a common 1 Gbps dedicated line.

Theory doesn't always translate well to the real world. No computer would be able to establish close to 1.2 million connections per second (assuming that you checked the size of SYN packets specifically).

Hacker0x00 - June 17, 2023, 12:52 pm

(Jun 17, 2023 12:18 PM)DramaKing Wrote: [\[CITE\]](#) Theory doesn't always translate well to the real world. No computer would be able to establish close to 1.2 million connections per second (assuming that you checked the size of SYN packets specifically).

SYN scanners don't establish the connections. They listen for the responding SYN-ACK in the handshake and let the connection timeout client side.

This is all elementary stuff.

Dread.Reaper - June 17, 2023, 9:13 pm

(Jun 17, 2023 12:52 PM)Hacker0x00 Wrote: [\[CITE\]](#) SYN scanners don't establish the connections. They listen for the responding SYN-ACK in the handshake and let the connection timeout client side.

This is all elementary stuff.

And how is that helping op establish a list of active IP#s or corresponding services, say SSH?