

Forum:[Hack Forums](#)

Thread: [\[Tut\] Finding real backend server IP hidden behind Cloudflare and other firewalls](#)

StackFramed - August 15, 2017, 4:47 pm

Server Logging

The most commonly used method. Set up a logger on the site and get the server to embed it. Sometimes when you post an image on a site (a forum for example) the server will visit the image URL to preview it or host it on the forum on it's own. We can use this to our advantage by getting the server to visit the logger.

A good example for this would be image IP logging. You can create an image IP logger and embed the image onto the site. If it wants to host the image on it's own server, it'll have to visit the link to do so. Upon going to your link to retrieve the image, the server's backend should be logged. (Keep in mind that this doesn't always require you to use an image IP logger. As long as you can get the site to embed the link it should still give you it's IP)

Image IP loggers (Without the dashes):

<https://iplo-gger.org/>

<http://www.fug-lekos.com/ip-grabber/index.html>

<https://gra-bify.link/>

Email Resolving

You can use an email hosted with the site to find the backend server's IP by looking at it's headers. You'll just have to trigger the site to send an automated email to you.

A few of the most common ways you can do this is registering an account to your email, requesting password resets, or contacting administrators.

Header tracking tools:

<http://whatismyipaddress.com/trace-email>

Hosting History

If the site has been hosted on it's actual IP for a while prior to using a firewall, it's possible that crawlers have accessed it before and cached the information. Look up the site's hosting history and you might be able to find something.

Site report lookups:

http://toolbar.netcraft.com/site_report

<http://viewdns.info/iphistory/>

<http://www.domainhistory.net/>

Subdomain Resolving

The site could have subdomains whose records are under the real server's IP and not protected by the firewall. Try resolving the subdomains instead.

E.g. connecting to example.com will have an IP address belonging to Cloudflare, but mail.example.com is not protected by Cloudflare. Use that to your advantage.

Mass Scanning The Site's Host

The most advanced and challenging method to mitigate of them all. If you somehow know what host the site is using you can scan the entire host for matching content from a range of IP addresses.

E.g. if the site's host is Digital Ocean, what we can do is find the full range of IP addresses connected to Digital Ocean (<http://bgp.he.net/search?search%5Bsearch%5D=Digital+Ocean&commit=Search>). We can then take these IP addresses and compare them to the content on the site such as the page title or body using tools such as Nmap or Zmap.

IP Range Lookup:

<http://bgp.he.net/>

Useful Tools

<http://skypegrab.net/cf.php>

<http://www.crimeflare.com/cfs.html>

<http://iphostinfo.com/cloudflare/>

<https://webresolver.nl/tools/cloudflare>

<http://www.skypeipresolver.net/cloudflare.php>

<https://www.cutesetools.net/cloudflare-resolver>

If you have anymore suggestions/methods feel free to post them below.

Punisher - August 15, 2017, 5:05 pm

Haven't had too much success with this one, but it's here if you need it;

<http://www.crimeflare.com/cfs.html>

StackFramed - August 15, 2017, 5:20 pm

(Aug 15, 2017 05:05 PM)Error Wrote: [\[CITE\]](#) Haven't had too much success with this one, but it's here if you need it;

<http://www.crimeflare.com/cfs.html>

Added this to the thread. Didn't realize I forgot about Crimeflare, although the first tool from Skypegrab includes results from it.

Just added the mass scan method to the thread as well.

SIM-2223238 - August 15, 2017, 5:21 pm

Should add zgrab on the thread tbh.

Forgot to tell you about it but you can add the domain to your own cloudflare to see the past DNS settings before it got added.

phenasty - *September 8, 2017, 9:11 am*

Forgot to tell you about it but you can add the domain to your own cloudflare to see the past DNS settings before it got added.

inv3ctus - *September 9, 2017, 5:04 am*

Thanks for the tut, will come back to this

mariasimmons99 - *October 16, 2017, 12:11 pm*

Nice, nice, nice, nice thanks a lot