

Forum:[Hack Forums](#)

Thread: [how to direct connect to site when cloud flare is on ?](#)

LosT512 - February 1, 2019, 3:38 pm

hey all ,

im hacking a site , and it have #cloud_flare service , so i get the real ip for site , but the ip in share-hosting , i mean the ip contain alot of sites

and when i try to enter the ip direct from browser its show me an error , how can i enter the ip and the site that i need ?

fake96 - March 19, 2019, 1:21 am

goto your c:\windows\system32\drivers\etc\ edit the "hosts" file and make a DNS entry as prntscr .com/mzur9c

Toasties - March 23, 2019, 1:26 am

(Mar 19, 2019 01:21 AM)fake96 Wrote: [\[CITE\]](#) goto your c:\windows\system32\drivers\etc\ edit the "hosts" file and make a DNS entry as prntscr .com/mzur9c

I highly doubt it will work

BTC - March 23, 2019, 1:31 am

<https://securitytrails.com/>

This is your best option

Toasties - March 23, 2019, 1:35 am

(Mar 23, 2019 01:31 AM)Apex Wrote: [\[CITE\]](#) <https://securitytrails.com/>

This is your best option

Is this so if they have registered their site without cloudflare you can see the historical ip?

BTC - March 23, 2019, 1:38 am

(Mar 23, 2019 01:35 AM)Toasties Wrote: [\[CITE\]](#) Is this so if they have registered their site without cloudflare you can see the historical ip?

Depending the website, if there is any historical records for DNS they used in the past (before using cloudflare perhaps) then you could possibly find the true DNS or hostname.

For example, in the tool if you search ? .org (most popular torrent site) you can see their hosting servers in Luxembourg, which they still use to date. Although they currently use CloudFlare and I believe have been since 2017/2018.

This obviously is subjective, and there likely would be no data for websites that never gained much traffic in history.

Toasties - March 23, 2019, 1:43 am

(Mar 23, 2019 01:38 AM)Apex Wrote: [\[CITE\]](#) Depending the website, if there is any historical records for DNS they used in the past (before using cloudflare perhaps) then you could possibly find the true DNS or hostname.

For example, in the tool if you search ? .org (most popular torrent site) you can see their hosting

servers in Luxembourg, which they still use to date. Although they currently use CloudFlare and I believe have been since 2017/2018.

This obviously is subjective, and there likely would be no data for websites that never gained much traffic in history.

Thata a very cleaver idea I never thought about before.

godjustice555 - July 17, 2019, 2:48 am

if u already found a suspicious ip and want to test it, (without changing the host file)

use

Code curl -H "Host: www.sample.com" [url=https://#/2Uo]http://100.100.100.10[/url]0substitute sample.com with the target domain name
substitutue 100.100.100.100 with ur suspected IP

13R20 - July 17, 2019, 11:23 am

(Mar 23, 2019 01:31 AM)BTC Wrote: [\[CITE\] The World's Largest Repository of Historical DNS data](#)

This is your best optionCheck this out. Its a work in progress

[GitHub - s0md3v/Striker: Striker is an offensive information and vulnerability scanner.](#)

joaok1ng0 - July 29, 2019, 12:08 am

try to get the real ip

in crimeflare db, sometimes work