

Forum:[Hack Forums](#)

Thread: [how to bypass cloud-flare](#)

Mr evil - April 1, 2017, 6:12 am

how to bypass cloud-flare and find the real ip of the website ?

Charger - April 1, 2017, 6:13 am

The only way is if you check the Whois history from when they were not using cloudflare.

Hecate - April 1, 2017, 6:33 am

You can try use simple script in .bat format. ?

Spoiler ([Click to View](#))

If you got text: Tracing route to yourhostname [1.1.1.1]

That 1.1.1.1 is your resolved cf ip address

Code @echo off

```
:start
cls
title CloudFlare exploit
color 02
echo.
echo                                CloudFlare resolver !
echo                                Dorks list updated  3/23/2017
echo.
echo                                Enter hostname without " http: // www "
set /P host=:
```

```
cls
echo.
title Run exploit on %host%
color 02
echo                                Searching ip leaks from:  %host%
```

```
echo.
tracert -h 1 -d -h 1 -d ftp.%host%
echo.
tracert -h 1 -d mail.%host%
echo.
tracert -h 1 -d direct.%host%
echo.
tracert -h 1 -d direct-connect.%host%
echo.
tracert -h 1 -d cpanel.%host%
echo.
tracert -h 1 -d admin.%host%
echo.
tracert -h 1 -d pop.%host%
echo.
```

```
tracert -h 1 -d imap.%host%
echo.
tracert -h 1 -d forum.%host%
echo.
tracert -h 1 -d beta.%host%
echo.
tracert -h 1 -d portal.%host%
echo.
pause
goto:start
```

Mr evil - April 1, 2017, 6:36 am

yes i try CloudFlare resolver but it did not work lol

Charger - April 1, 2017, 6:38 am

(Apr 1, 2017 06:36 AM)Mr evil Wrote: [\[CITE\]](#) yes i try CloudFlare resolver but it did not work lol
All you can do is check the whois or see what dns records they have.

Hecate - April 1, 2017, 6:40 am

(Apr 1, 2017 06:36 AM)Mr evil Wrote: [\[CITE\]](#) yes i try CloudFlare resolver but it did not work lol
If you check the Whois history from when they were not using cloudflare, and using resolver did not find ip address soo you will not get much out of nowhere.

Mr evil - April 1, 2017, 6:46 am

darm so what you would do in this situation ? lol

Hecate - April 1, 2017, 6:54 am

(Apr 1, 2017 06:46 AM)Mr evil Wrote: [\[CITE\]](#) darm so what you would do in this situation ? lol
As I understand it, you want to get the IP address from the website.
And you will use the IP addresses for attacking website using layer4 attacking methods.
If yes, The last option is use layer7 methods.

alqtri - April 1, 2017, 11:25 am

try this site

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

:)

a horse - April 1, 2017, 4:50 pm

ignoring the skids above

- 1) attempt to look for dns leakage - request all dns entries, then bf sub-domains (specifically services that CF doesn't cover)
- 2) if the website is dynamic, attempt out-of-bounds info leak, meaning cause the service to phone back to you. For example, sending a confirm email from the server using the server's SMTP service will obviously reveal the IP in the headers

lalapwn - April 1, 2017, 9:48 pm

- (Apr 1, 2017 04:50 PM)a horse Wrote: [\[CITE\]](#) ignoring the skids above
- 1) attempt to look for dns leakage - request all dns entries, then bf sub-domains (specifically services that CF doesn't cover)
 - 2) if the website is dynamic, attempt out-of-bounds info leak, meaning cause the service to phone back to you. For example, sending a confirm email from the server using the server's SMTP service

will obviously reveal the IP in the headers

2) will not work if the site owner is using external SMTP.

@OP, your best bet is to check the historic DNS entries.

Mr evil - April 2, 2017, 3:13 am

This cloud-flare thingy really sucks the evil eyez

Mr evil - April 3, 2017, 5:38 am

fierce is the alternative to find the ip

godjustice555 - July 17, 2019, 2:45 am

ok, there are more ways.

what didn't discuss above is the SSL way. previously, u need to know how to use the right query to find it in censys. now, just head to crt.sh and from the cert it will link to censys, and from censys u can look for the ipv4 machine that uses the cert.

as of tools, u can use cloudflair to achieve the above.

and there's another way that is a tweak of the above. i've proven it to work but it requires huge amount of resources. (think brute forcing)

and i'm sure i can find the real ip of any sites with my algorithm.

13R20 - July 17, 2019, 11:24 am

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

[The World's Largest Repository of Historical DNS data](#)