Finding IP address behind Cloudfare

In today's digital landscape, many websites and online services leverage the power of content delivery networks (CDNs) and reverse proxy services like Cloudflare to enhance performance, security, and reliability. While these services provide numerous benefits, they can also obfuscate the true IP addresses of the underlying web servers, making it challenging for hackers like us to conduct effective reconnaissance.

Cloudflare, in particular, is a widely adopted service that acts as a reverse proxy, shielding the actual IP addresses of web servers from public view. This can pose a significant obstacle during the reconnaissance phase of a penetration testing engagement, as identifying the real IP addresses is crucial for mapping the attack surface and planning subsequent phases of the assessment.

During this section, we will explore how we can find the real IP address behind Cloudfare protection.

So, lets get started

For this demonstration, i will take patreon.com as target as i already knew it uses cloudfare.

- **Find IP address behind Cloudflare**

```
python3 cloudfail.py -t <domain>
```
