[【原创】] **绕过 CDN 查找网站真实 IP 方法收集**

总在 T00ls 中看到人在问如何绕过 CDN 查找网站真实 IP，而下面回复却说这是月经帖，每个月都有人问同样

0x01 验证是否存在 CDN

方法 1

很简单，使用各种多地 ping 的服务，查看对应 IP 地址是否唯一，如果不唯一多半是使用了 CDN， 多地 P

```
1. http://ping.chinaz.com/
2. http://ping.aizhan.com/
3. http://ce.cloud.360.cn/
```

复制代码

方法 2

使用 nslookup 进行检测，原理同上，如果返回域名解析对应多个 IP 地址多半是使用了 CDN。有 CDN 的

```
1. > www.163.com
2. 服务器:  public1.114dns.com
3. Address:  114.114.114.114
4.
5. 非权威应答:
6. 名称:    163.xdwscache.ourglb0.com
7. Addresses:  58.223.164.86
8.           125.75.32.252
9. Aliases:  www.163.com
10.          www.163.com.lxdns.com
```

复制代码

无 CDN 的示例：

```
1. > xiaix.me
2. 服务器:  public1.114dns.com
3. Address:  114.114.114.114
4.
5. 非权威应答:
```

```
6. 名称:    xiaix.me

7. Address:  192.3.168.172
```
复制代码

方法 3

使用各种工具帮助检测目标网站是否使用了 CDN，可以参见如下网站：

```
1. http://www.cdnplanet.com/tools/cdnfinder/

2. http://www.ipip.net/ip.html
```
复制代码

0x02 绕过 CDN 查找网站真实 IP

2.1 查询历史 DNS 记录

查看 IP 与 域名绑定的历史记录，可能会存在使用 CDN 前的记录，相关查询网站有：

```
1. https://dnsdb.io/zh-cn/

2. https://x.threatbook.cn/

3. http://toolbar.netcraft.com/site_report?url=

4. http://viewdns.info/
```
复制代码

2.2 查询子域名

毕竟 CDN 还是不便宜的，所以很多站长可能只会对主站或者流量大的子站点做了 CDN，而很多小站子站点
IP。

2.3 利用网站漏洞

这个就没什么好说的了，目的就是让目标服务器主动来连接我们，这样我们就知道其真实 IP 了，可用的比如 X

2.4 服务器合法服务主动连接我们

同上一样的思路就是让服务器主动连接我们告诉我们它的 IP，不过使用的是合法的服务，如 RSS 邮件订阅，

2.5 使用国外主机解析域名

国内很多 CDN 厂商因为各种原因只做了国内的线路，而针对国外的线路可能几乎没有，此时我们使用国外的

2.6 目标敏感文件泄露

也许目标服务器上存在一些泄露的敏感文件中会告诉我们网站的 IP，另外就是如 phpinfo 之类的探针了。

2.7 从 CDN 入手

无论是用社工还是其他手段，反正是拿到了目标网站管理员在 CDN 的账号了，此时就可以自己在 CDN 的配置

2.8 用 Zmap 扫全网？

这个我没试过不知道...据说 Zmap 44 分钟扫描全网？

好吧，还是稍微详细说下吧，比如要找 xiaix.me 网站的真实 IP，我们首先从 apnic 获取 IP 段，然后使用

写 xiaix.me。

大概就这些了吧，其他的什么像 DDoS 把 CDN 流量打光的这种就算了吧，最好还是别干扰到人家网站的正

原文地址：http://xiaix.me/rao-guo-**cdn**cha-zhao-wang-zhan-zhen-shi-ip/