web渗透测试系列 之 信息收集（2）

千锋网络...
白帽极客的黄埔军校-千锋网络安全学院

小伙伴们~大家好

我们继续上一篇的内容今天来聊聊关于在信息收集碰到的CDN相关的问题，先举个栗子先

不知道大家有没有碰到过这样的情况，在我们信息收集的时候，最简单的就是通过域名来反映出来IP地址，突然发现在PING回包的时候，突然回应的IP地址有变化，这时就对刚刚入门的小伙伴们带来一些困惑，其实这就是该网站使用了CDN技术造成的，导致我们获得到的不是真实IP地址。那么我们先来科普一下

CDN（Content Delivery Network）翻译过来叫做内容分发网络。简单来说，他的作用是干什么的呢？其目的就是让我们在不同的地理位置访问该网站，都能达到一个非常快的速度，比如，我们在北京访问深圳腾讯总部的网站，如果不做CDN的话，需要通过互联网穿过几千公里跑到深圳的腾讯服务器里面提取网站页面，在这样的距离上，中间会有各种各样的网络设备来中转，势必会可能有些网络因素导致访问变慢的情况，这样就会对我们的用户体验造成不好的体验，那么，如果把深圳腾讯的服务器复制一个副本放在北京这边的网络边缘上，那么首先距离与中转设备就没有那么多了，我们访问网站的速度也会加快，简单的来讲CDN就是个这样的玩意。

那么问题又来了，对于我们渗透时候的信息收集，怎么去绕过CDN呢？

下面我们就聊聊

首先是CDN 加速的问题

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 Ping 网站有：

ping.aizhan.com/

ce.cloud.360.cn/

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 的示例：

> 163.com

服务器: public1.114dns.comAddress: 114.114.114.114

非权威应答:

名称: 163.xdwscache.ourglb0.comAddresses: 58.223.164.86

125.75.32.252Aliases: 163.com

163.com.lxdns.com

无 CDN 的示例：

> xiaix.me

服务器: public1.114dns.comAddress: 114.114.114.114

非权威应答:

名称: xiaix.meAddress: 192.3.168.172

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：

cdnplanet.com/tools/cdn...

ipip.net/ip.html

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：

dnsdb.io/zh-cn/

x.threatbook.cn/

toolbar.netcraft.com/si...

viewdns.info/

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，而很多小站子站点又跟主站在同一台服务器或者同一个C段内，此时就可以通过查询子域名对应的 IP 来辅助查找网站的真实IP。

2.3 利用网站漏洞

知乎

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，很多网站都自带 sendmail，会发邮件给我们，此时查看邮件源码里面就会包含服务器的真实 IP 了。

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主机直接访问可能就能获取到真实IP。

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的配置中找到网站的真实IP了。

2.8 用 Zmap 扫全网

IP2Location查询IP 地址经纬度

maxmind.com/zh/home

通过GPS 查询物理位置

gpsspg.com/maps.htm

以上即为给大家分享的关于CDN的一些知识，希望对小伙伴们有帮助，我们下次见喽~

发布于 2020-03-04

渗透测试 CDN 阿里云 CDN

▲ 赞同 4 ▼ 3 条评论 分享 喜欢 收藏 ···

知乎

渗透测试--绕过cdn获取网站真实ip详解

黑色毛衣 发表于W3bSa...

渗透测试------信息收集

黑白之间 发表于web安全...

《暴裂无声》影评

流浪千年

感谢大家

请勿转载

白云蓝天

3 条评论 切换为时间排序

写下你的评论...

kazey0mi 3 天前

给乔帮主打call

1

该隐 3 天前

乔帮主最猛

1

否提I'do 2 天前

感谢作者大大，学到了

赞

▲ 赞同 4 ▼ 3 条评论 分享 喜欢 收藏 ···