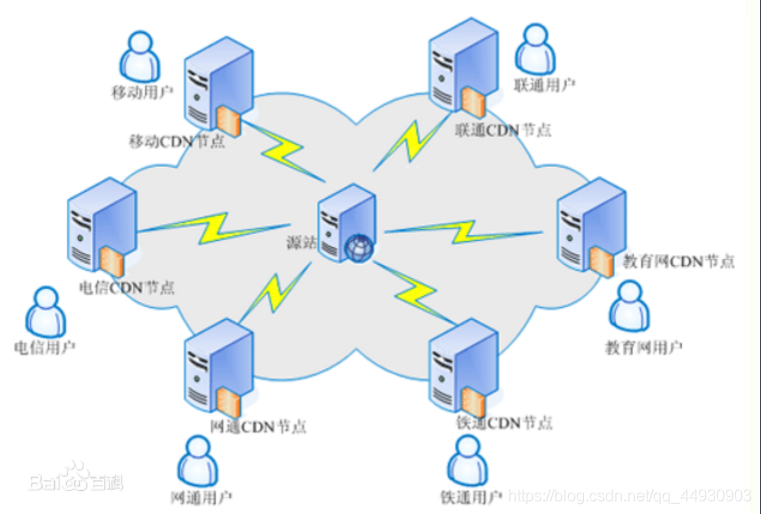
# 07 信息收集-CDN绕过



如何判断目标存在CDN服务？

利用多节点技术进行请求返回判断；比如使用ping一下域名，回应的域名有变，还有很多判读方法，上面一篇博客有说。

CDN对于安全测试有那些影响？

  看了CDN的概念之后，可以知道对方如果使用了CDN技术，我们直接访问的可能不是对方的真实ip，即访问其真实服务器的时候会受些阻碍。

目前常见的CDN绕过技术有哪些？

子域名查询

邮件服务查询

国外地址请求

遗留文件，扫描全网

黑暗引擎搜索特定文件（hash文件）

dns历史记录，以量打量

CDN真实IP地址获取后绑定指向地址

更改本地HOSTS解析指向文件

具体操作见这篇博客：01 渗透基础入门-概念名词

演示案例：

✧ 利用子域名请求获取真实IP

✧ 利用国外地址请求获取真实IP

✧ 利用第三方接口查询获取真实IP

✧ 利用邮件服务器接口获取真实IP

✧ 利用黑暗引擎搜索特定文件获取真实IP

xueersi 子域名上面的小技巧

sp910 DNS历史记录=第三方接口（接口查询）

m.sp910 子域名小技巧/采集/国外请求（同类型访问）

mozhe 邮件源码测试对比第三方查询（地区分析）

v23gg 黑暗引擎（shodan搜指定hash文件）：

python2脚本获取hash值并搜索

扫全网

fuckcdn，w8fuckcdn，zmap等

fuckcdn演示

涉及资源：

https://www.shodan.io

https://x.threatbook.cn

http://ping.chinaz.com

https://www.get-site-ip.com/

https://asm.ca.com/en/ping.php

https://github.com/Tai7sy/fuckcdn

https://github.com/boy-hack/w8fuckcdn

https://mp.weixin.qq.com/s?\_\_biz=MzA5MzQ3MDE1NQ==&mid=2653939118&idx=1&sn=945b81344d9c89431a8c413ff633fc3a&chksm=8b86290abcf1a01cdc00711339884602b5bb474111d3aff2d465182702715087e22c852c158f&token=268417143&lang=zh\_CN#rd