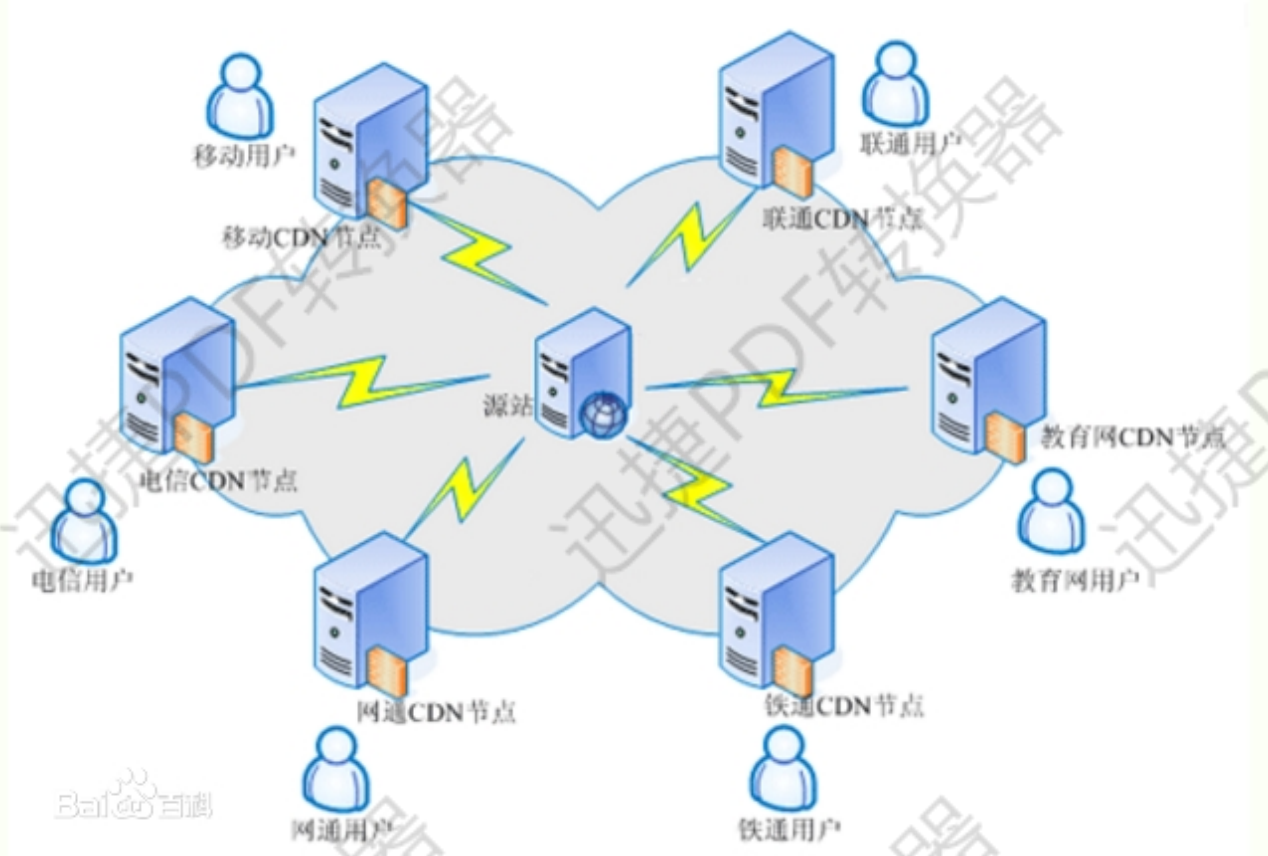
信息收集-CDN 绕过

CDN 的全称是 Content Delivery Network，即内容分发网络。CDN 是构建在现有网络基础之上的智能虚拟网络，依靠部署在各地的边缘服务器，通过中心平台的负载均衡、内容分发、调度等功能模块，使用户就近获取所需内容，降低网络拥塞，提高用户访问响应速度和命中率。但在安全测试过程中，若目标存在 CDN 服务，将会影响到后续的安全测试过程。



#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

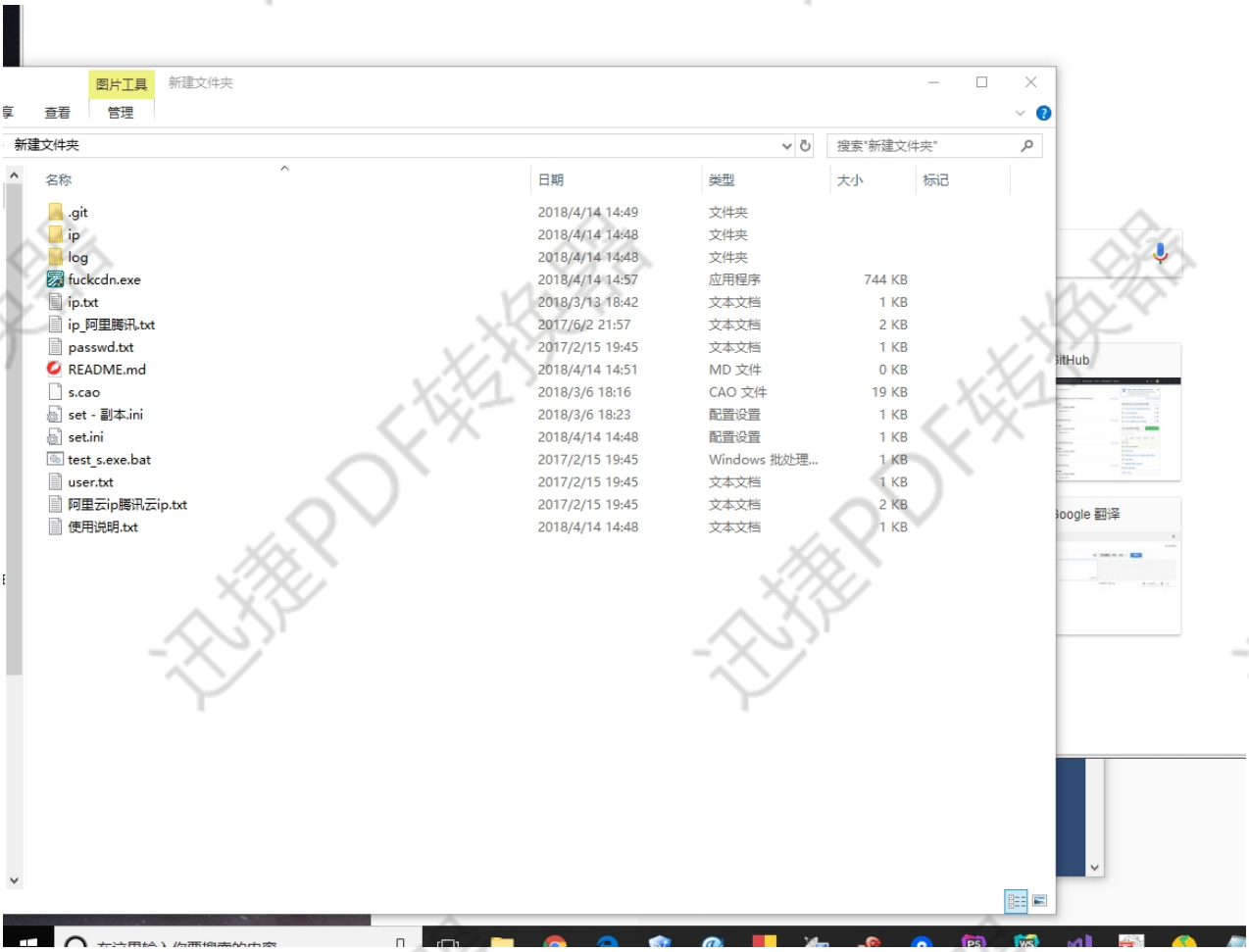
#CDN 对于安全测试有那些影响？

#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
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

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）

扫全网
fuckcdn，w8fuckcdn，zmap 等
#Python2 开发别搞错了执行环境
#安装 mmh3 失败记得先安装下这个#Microsoft Visual C++ 14.0
#https://pan.baidu.com/s/12TcFkZ6KFLhofCT-osJOSg 提取码：

```
import mmh3
import requests

response = requests.get('http://www.xx.com/favicon.ico')
favicon = response.content.encode('base64')
hash = mmh3.hash(favicon)
print 'http.favicon.hash:'+str(hash)
```

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

---