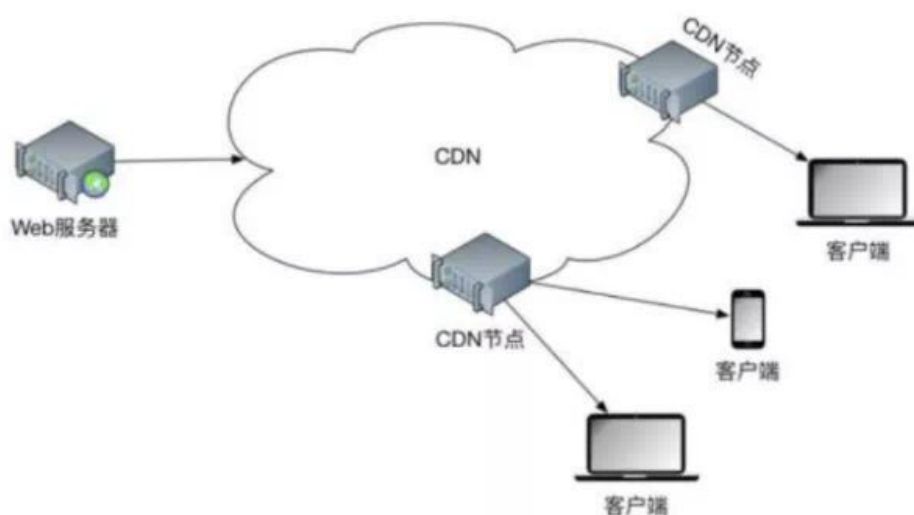


Day07 信息收集-CDN相关技术

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。



0x00实验室

7.1 判断是否有CDN

看响应时间工具: <http://tool.chinaz.com/speedtest>



Ping IP或域名，看是否会出现变化。

无：

```
C:\Users\Master>ping xiaodi8.com
```

正在 Ping xiaodi8.com [47.75.212.155] 具有 32 字节的数据：

来自 47.75.212.155 的回复： 字节=32 时间=60ms TTL=108

来自 47.75.212.155 的回复： 字节=32 时间=59ms TTL=108

来自 47.75.212.155 的回复： 字节=32 时间=58ms TTL=108

来自 47.75.212.155 的回复： 字节=32 时间=55ms TTL=108

47.75.212.155 的 Ping 统计信息：

数据包：已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，

往返行程的估计时间(以毫秒为单位)：

最短 = 55ms，最长 = 60ms，平均 = 58ms

0x00实验室

有：

```
C:\Users\Master>ping www.bilibili.com
```

正在 Ping a.w.bilicdn1.com [123.159.205.1] 具有 32 字节的数据：

来自 123.159.205.1 的回复： 字节=32 时间=38ms TTL=51

来自 123.159.205.1 的回复： 字节=32 时间=92ms TTL=51

来自 123.159.205.1 的回复： 字节=32 时间=33ms TTL=51

来自 123.159.205.1 的回复： 字节=32 时间=32ms TTL=51

123.159.205.1 的 Ping 统计信息：

数据包：已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，

往返行程的估计时间(以毫秒为单位)：

最短 = 32ms，最长 = 92ms，平均 = 48ms


0x00实验室

nslookup域名，看是否会有很多结点：

```
C:\Users\Master>nslookup bilibili.com
服务器:  localhost
Address:  192.168.43.1
```

非权威应答:

```
名称:      bilibili.com
Addresses:  119.3.238.64
            120.92.174.135
            120.92.78.97
            110.43.34.66
            119.3.70.188
            139.159.241.37
```

 0x00实验室

7.2 CDN对测试有何影响&如何绕过

1. 子域名查询：有的网站主域名会做CDN，但是子域名可能不会做
2. 邮件服务查询：我们访问别人，可能通过CND，但别人访问我们通常不会走CDN
3. 国外地址请求：国外没有CDN节点的话，可能直接走原IP
4. 遗留文件，扫描全网
5. 黑暗引擎搜索特定文件
6. DNS历史记录，以量打量：CDN节点是有流量上限的，用光之后就会直通原机，这也是一种流量攻击

7.3 测试

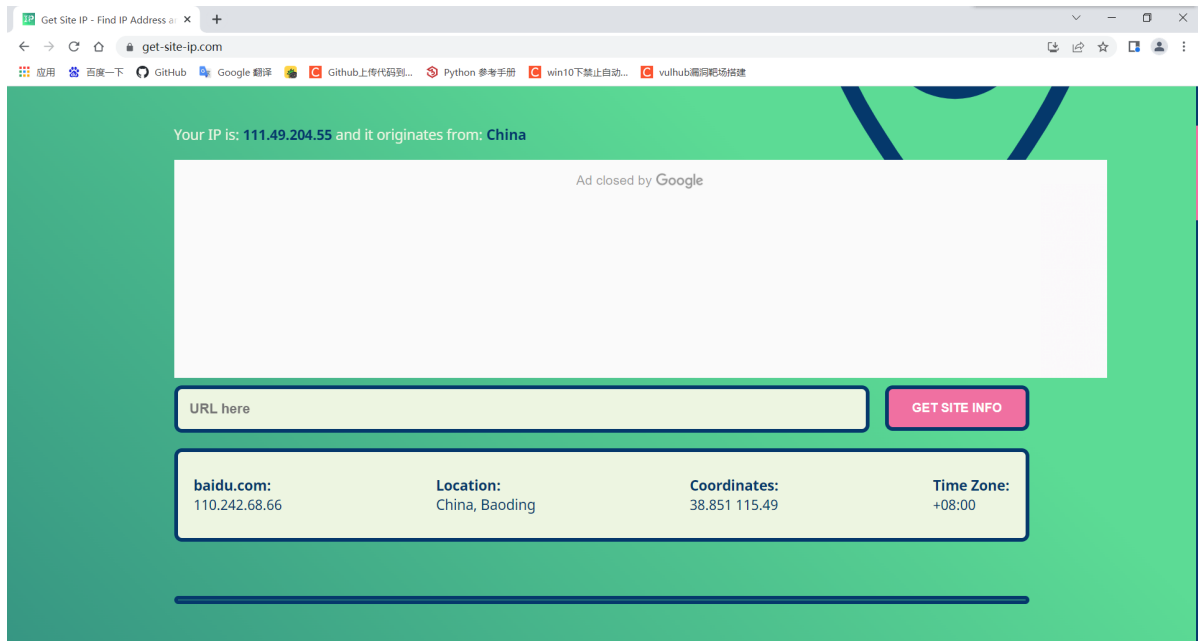
7.3.1子域名上面的小技巧

- 二级域名和三级域名查到的结果可能不一样
- 主域名和子域名查询到的可能不一样
- DNS历史记录=第三方接口(接口查询)
- 采集/国外请求(同类型访问)

- 邮件源码测试对比第三方查询(地区分析)

```
Received: from ucmail287.sendcloud.org (ucmail287.sendcloud.org [117.50.60.213])
  by newxmmszb1-18.qq.com (NewMX) with SMTP id 3CDB168A
  for <1137783204@qq.com>; Mon, 23 May 2022 15:15:13 +0800
X-QQ-mid: xmmxzb1-18t1653290224tc89o15n6
X-QQ-XMAILINFO: NKab1Zz1fwK8VS7MkBgYvKHv7yxpHuCTWJXd/hyhrfunCag1z9q1P5fnQoB4fm
  kqAwPc+1j0tVnCVqrOVNjyS+7R6pVJ91vnwspnznvN9TrfZjLCfMYyFwmh70Ihe3Pi0jsQAjEEWZ
  P1LRc2jmwJC8a3rHV1Hmd1KVCZm0I1Qj1ULsgMSyKxV/G275m10b+95FhmEOYxDIHc710XKtrWG
  4ND6NjFUntLLHEa4Ze10X3px2tfuG1i/h3fbezQPiXTK8uaeV7PJZGXg3VXi1eT11G/f7RD7GEIT
  9fic6cnldUfqjkYCFnKNNdVtoApbxqeuLSf/g64m5GD9e1eHJ00Nei0EWYXWLV+EYrITsBJHhspA
  VrGAAq8vo+3pq66/Ag8nkXfaM81Iu0QqKFL+qq1Yja/j7pWODJJndbV0mOCBRhig0BcfVWK4YCrQ
  okydOKnKj0Ts2/G+h7QSDQH3/sgIkIInR/hVtfSVV/M7mjvDz0Uaor5R11oealk95JYykhF00rsJ
  80JZDsKZmL8L1t0VN000tE3WfcjiTdYFBjpmONt2h8Yb/u1x8vbeQm1VKGfKeLYvpGADv1Yg+pm3
  CrV68g+DoVqFhE7LweqiRMm5u2BMjzJU1DZmFDLWYAInwE5+Tox9NPUcc0EagHBK94bQ7uQyCCVK
  xiYFiC78S75B93/hhjQm2j3xfgd1z1EV/ndirK7ZclJmgAOhzk4cEaoj6JtUW3Z/+OpWkZRG2zoH
  OahRZkCs5wGCi7LkHT6Pjc/LItSu6qR02ZQPG9NHAcH1qesE9pMcEUosW0652GAPoz3zzFR414zc
  6pn5zVVW7Z9x6RR47TebEJ00mSugoiD+eXkPZYVgKZocWLZtB21EyVnzCwpYiK09ZIU479HS/Py
  DD2oOXj5MLVsSuL3sNF1aI25c0kNFtsRx5n0ECDsRnYL0WimX25EzHnyeTwP11Hrur/iofstVov/
  30Mpv4xueS9dYGUjg8EscFX/OZTvgD13XVAGPSDjdshTAPePkJEumh9R2fU0ic8Mo5X5eSH8awrB
  EXWwAVU9Cg9fWqJmQ3sTdOfCL5zGhEG8V1FqghvIEHF2oR/cbIYua/el1fGmf44pLWGrI8jkIwOxk
  UtpkctcmuL660ELf3QNV9JX7yI9TT/N2rbrEDt0+W+jCMeYdSh++k6UF8Brtq0T6/1vKGW1VQqxp
  ihQmoUDFkI3fpqjhwMGTK+Eqs9Nd+sz12ibvGYo4hnyYhwESU6d4jBrWQV7v4m/4b4M6COBijaZm
  RL1PurF01pFnP6
Sender: 590a7604-da68-11ec-8785-525400450766@sc2.haitou.cc
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=sc2.haitou.cc;
  i=@sc2.haitou.cc; q=dns/txt; s=mail; t=1653290224; h=message-id : date
  : subject : from : to : mime-version : content-type : reply-to :
  list-unsubscribe : from;
  bh=VypoHxm2xpu6325Yli8n4F0sAcSTuGS4AyaYnH9DHIM=;
  b=D06gjlVfVqmsSU40XnB8GpPvnrJSj5DI10NXqRpEZAMppFRY/5H0B7pDRKt2MyzJcQRID
  xKaYGIQ2CLsQbc1B+qVv1s5fblGnJn5thFFmh5mVBTAdIjv30migYaAM8cctwLxRh9cEEiS
  cGXBAS5w3HB2xforZOWi82Sv5xmdt+H8=
```

- 黑暗引擎(shodan搜指定hash文件)
- 扫全网 fuckcdn, w8fuckcdn, zmap等
- 工具扫描



- 认为判定, 根据网站的域名备案推测
- 本地清下DNS, 然后hosts里写上得到的IP和域名, 如果是CDN可能会出现刷新异常, 如果打开很快大概率是原机

资源



```
1  https://www.shodan.io
2  https://x.threatbook.cn
3  http://ping.chinaz.com
4  https://www.get-site-ip.com/
5  https://asm.ca.com/en/ping.php
6  https://github.com/boy-hack/w8fuckcdn
```