

利用Domain+CDN隐藏VPS真实IP

5h4d0w FreeBuf 今天

引言

在攻防演练中,目标在内网cs上线如果不做任何保护,自己的VPS很容易泄露IP。我们利用简单的域+CDN来做一个简单的隐匿,增加防守溯源的一些难度。



正文

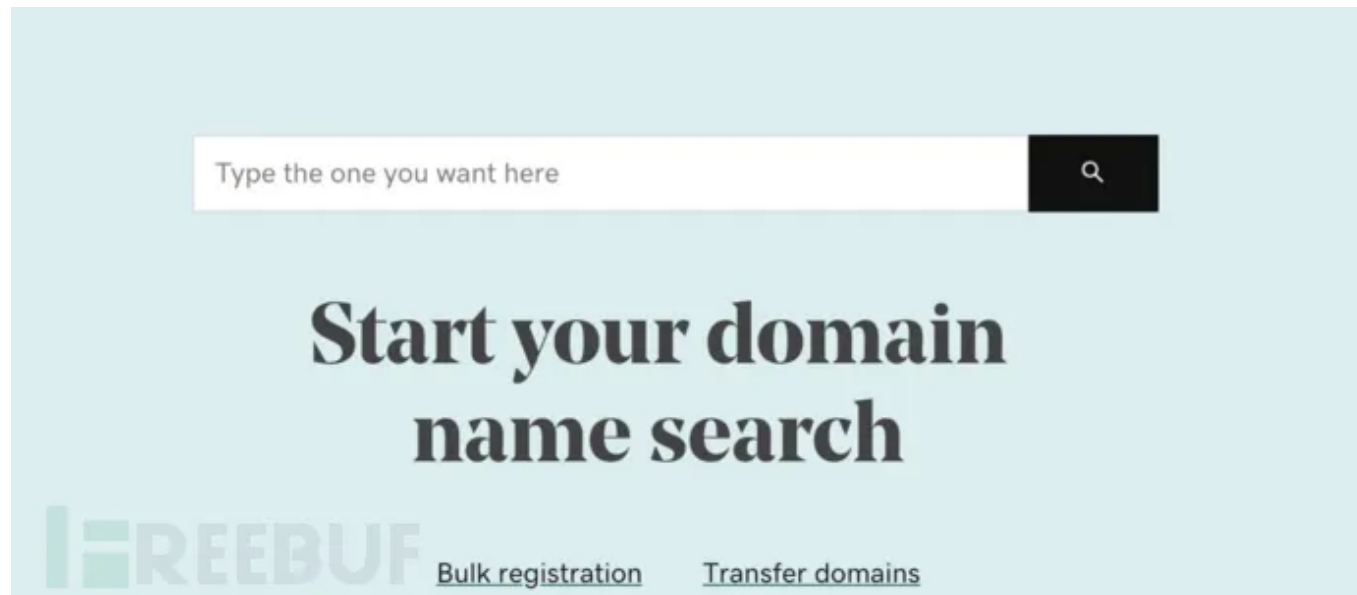
先说一下什么是CDN,CDN的基本原理是广泛采用各种缓存服务器,将这些缓存服务器分布到用户访问相对集中的地区或网络中,在用户访问网站时,区域负载均衡设备会为用户选择一台合适的缓存服务器提供服务,选择的依据包括:根据用户IP地址,判断哪一台服务器距用户最近;根据用户所请求的URL中携带的内容名称,判断哪一台服务器上有用户所需内容;查询各个服务器当前的负载情况,判断哪一台服务器尚有服务能力。基于以上这些条件的综合分析之后,区域负载均衡设备会向全局负载均衡设备返回一台缓存服务器的IP地址,客户最终得到的是CDN缓存服务器的地址。

需要准备：

1. 一台VPS最好是免备案的推荐virmach、vultr(这俩还不错前者价格实惠延迟稍高、后者相对好点也相对贵一点这都不是重点)
2. 域名申请，同样免备案这里推荐godaddy毕竟大厂大概一年5块钱，在这里也踩了不少坑用了namecheap, freenom等了好几天愣是没响应….



3. CND, cloudflare免费的CND够用.



注册大概需要大概半小时到一小时,注册完成后我们就可以去配置CDN了



在这里去配置我们注册域名,按他的提示修改我们在godaddy名称服务器

1.登录到您的注册机构帐户

通过 [WHOIS](#) 确定您的注册机构。

删除以下名称服务器：

dns21.hichina.com
dns22.hichina.com

2.替换为 Cloudflare 的名称服务器



名称服务器 1

marvin.ns.cloudflare.com

单击以复制



名称服务器 2

olga.ns.cloudflare.com

单击以复制

保存 所做更改。

My Domains

Domains ▾

Estimated Value (USD)



Expires on 5/10/2021



Not available

Manage DNS

Domain settings

Nameservers

Last updated 5/10/2020 2:19 PM

Using custom nameservers

Change

Nameserver

marvin.ns.cloudflare.com

olga.ns.cloudflare.com



还需要执行几个步骤才能完成设置。

隐藏

✓ 为根域添加 MX 记录，以便邮件可以到达 [\[redacted\]](#) 地址。

管理 [\[redacted\]](#) 的 DNS

+ 添加记录

Q 搜索 DNS 记录

高级

类型	名称	内容	TTL	代理状态	
A	[redacted]	45.33.121.100	自动	已代理	删除
CNAME	[redacted]	[redacted]	自动	仅限 DNS	删除
CNAME	[redacted]	[redacted]	自动	仅限 DNS	删除

修改完后我们就可以配置CDN最终解析我们的VPS了. 这里A记录名称是我们的域名内容是我们的VPS的IP. 到此整个的域名配置完成了. 当ping域名的时候ip解析的为CDN的地址(自己试吧截图太麻烦了)

域名上线

注意

Cloudflare有个问题, 只能支持几个端口其他的无法监听, 一下是支持的端口.

HTTP

80, 8080, 8880, 2052, 2082, 2086, 2095

HTTPs

443, 2053, 2083, 2087, 2096, 8443

payload 可以选择windows/beacon_http/reverser_https生成后门.

Edit Listener

Create a listener.

Name: 443

Payload: Beacon HTTPS

Payload Options

HTTPS Hosts:

+

-

×

HTTPS Host (Stager): https://

Profile: default

HTTPS Port (C2): 443

HTTPS Port (Bind):

HTTPS Host Header:

HTTPS Proxy:

Save

Help

靶机运

行查看抓包结果.

	T:	Source	Destination
1 ...		192.168.84.144	45.32.128.100
2 ...		45.32.128.100	192.168.84.144
3 ...		192.168.84.144	45.32.128.100
4 ...		192.168.84.144	45.32.128.100
5 ...		45.32.128.100	192.168.84.144
6 ...		45.32.128.100	192.168.84.144
7 ...		192.168.84.144	45.32.128.100
8 ...		45.32.128.100	192.168.84.144
9 ...		192.168.84.144	45.32.128.100
10 ...		192.168.84.144	45.32.128.100
11 ...		45.32.128.100	192.168.84.144
12 ...		192.168.84.144	45.32.128.100
13 ...		45.32.128.100	192.168.84.144
14 ...		45.32.128.100	192.168.84.144
15 ...		192.168.84.144	45.32.128.100

Internet Protocol Version 4, Src: 45.32.128.100, Dst: 192.168.84.144 0100 = Version: 4 0101 = Header Length: 20 bytes ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 40 Identification: 0x4975 (18805) ▶ Flags: 0x00 Fragment offset: 0 Time to live: 128 Protocol: TCP (6) ▶ Header checksum: 0x2e9e [validation disabled] Source: 45.32.128.100 Destination: 192.168.84.144 [Source GeoIP: Unknown] [Destination GeoIP: Unknown]	Transmission Control Protocol, Src Port: 443 (443), Dst Port: 1709 (1709), Seq: 481, Ack: 743, Len Source Port: 443
---	--

这里最终简单的隐藏了我们VPS的IP.

感谢各位表哥的阅读！

——PT-LAB

*本文作者：5h4d0w，转载请注明来自FreeBuf.COM



FreeBuf+小程序：把安全装进口袋