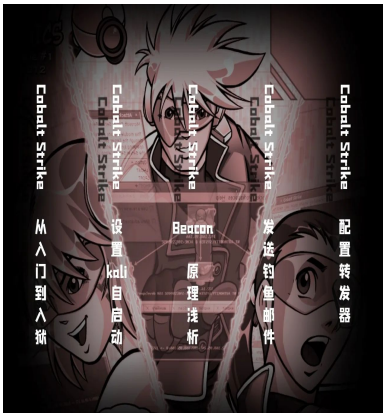
Cobalt Strike | DNS Beacon

CS小能手 物联网IOT安全 2020-03-08 21:00:00

听说Cobalt Strike被HelpSystems收购了，恭喜作者财富自由哇，关于收购信息详细文章可以**参见下文黑鸟师傅的文章**

如果还有小伙伴没有阅读过之前的文章可以**点击下方图片跳转到相应文章**，先看看前面的总归是好的 ~

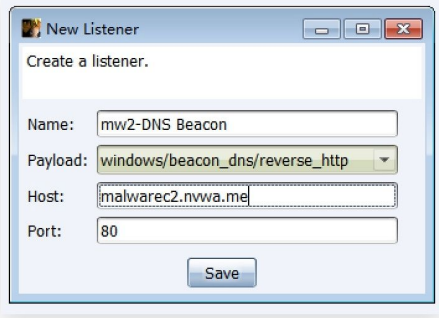
回到顶部



我们首先来看看DNS Beacon**的第一种情况：使用DNS记录来检查是否有新任务但传输器是运行在HTTP之上的**

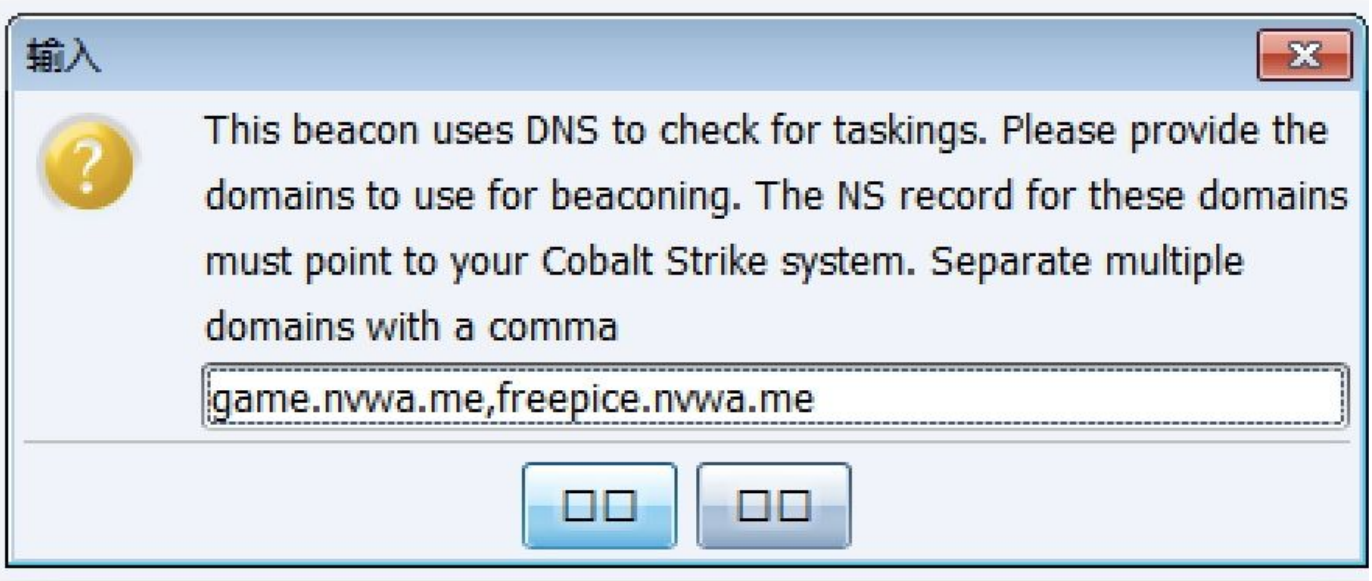
这种情况也需要我们自己设置域名服务器，如下图所示：

新建一个DNS Beacon监听器



我们在此处输入刚刚设置的NS记录域名

回到顶部



接下来**验证基础环境是否正常工作**:

前面自我感觉配置的都非常好，但是到了验证基础环境的时候就发现。

无法查找到这个IP地址是什么鬼，我们先来Team Server查看一下开放端口:

回到顶部

```
ubuntu@vm10-0-0-2:~$ sudo netstat -nlp
sudo: unable to resolve host vm10-0-0-2
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      27927/sshd
tcp        0      0 0.0.0.0:50050           0.0.0.0:*               LISTEN      2195/java
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      2195/java
tcp6       0      0 :::22                   :::*                    LISTEN      27927/sshd
udp        0      0 0.0.0.0:53              0.0.0.0:*                           2195/java
udp        0      0 0.0.0.0:68              0.0.0.0:*                           947/dhclient
udp        0      0 0.0.0.0:68              0.0.0.0:*                           854/dhclient
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     478445   12559/systemd        /run/user/1000/systemd/private
unix  2      [ ACC ]     SEQPACKET  LISTENING     9717     1/init               /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     16845    1347/AgentMonitor    /dev/sd_sdmanager_command
unix  2      [ ACC ]     STREAM     LISTENING     17143    1383/KsyunAgent      /dev/js_cloudhelper_update
unix  2      [ ACC ]     STREAM     LISTENING     13572    1/init               /var/lib/lxd/unix.socket
unix  2      [ ACC ]     STREAM     LISTENING     13566    1/init               /run/snapd.socket
unix  2      [ ACC ]     STREAM     LISTENING     13567    1/init               /run/snapd-snap.socket
unix  2      [ ACC ]     STREAM     LISTENING     13575    1/init               /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     13576    1/init               /run/acpid.socket
unix  2      [ ACC ]     STREAM     LISTENING     13577    1/init               /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     13654    1074/iscsid          @ISCSIADM_ABSTRACT_NAMESPACE
unix  2      [ ACC ]     STREAM     LISTENING     9706     1/init               /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     9710     1/init               /run/systemd/journal/stdout
unix  2      [ ACC ]     STREAM     LISTENING     9713     1/init               /run/systemd/fsck.progress
unix  2      [ ACC ]     STREAM     LISTENING     9929     1/init               /run/lvm/lvmetad.socket
unix  2      [ ACC ]     STREAM     LISTENING     9930     1/init               /run/lvm/lvmpolld.socket
```

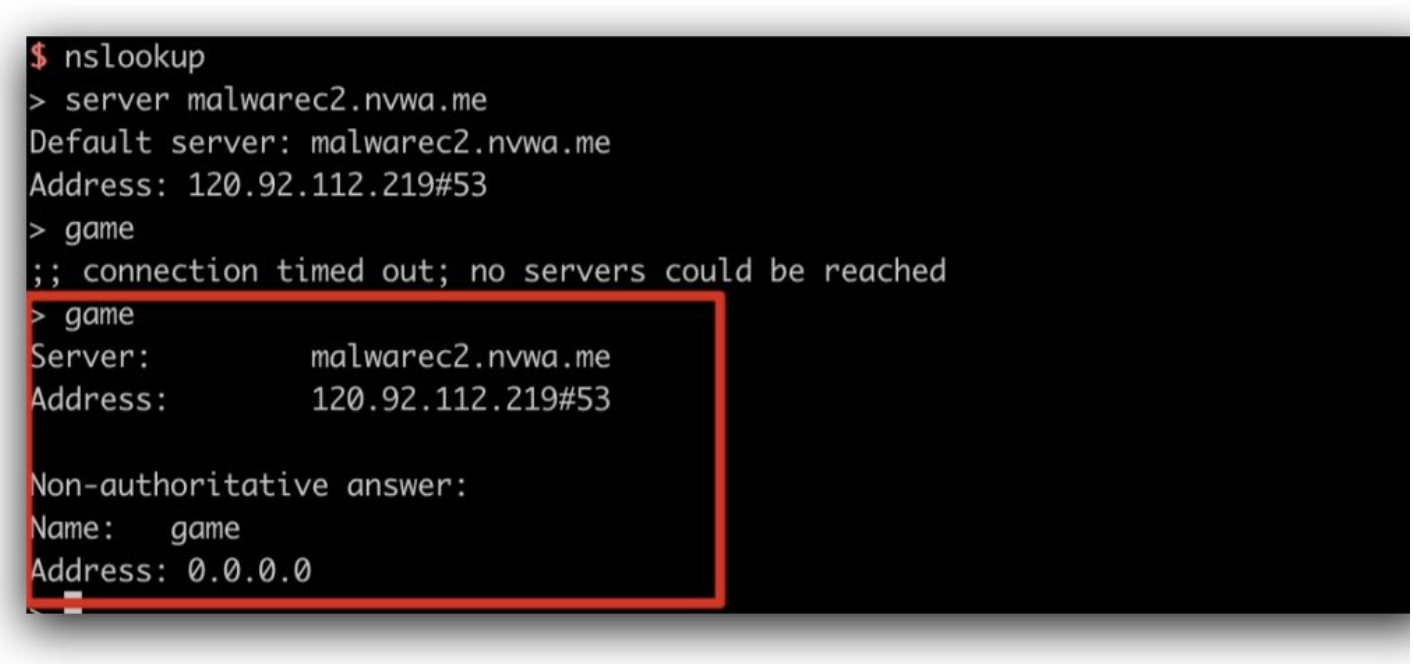
显然cobalt strike的DNS服务已经起来了，难道是防火墙？

```
ubuntu@vm10-0-0-2:~$ sudo ufw disable
sudo: unable to resolve host vm10-0-0-2
Firewall stopped and disabled on system startup
```

关掉防火墙还是不行，我们**查看一下VPS的网络安全组策略**：

TCP协议的确是没有任何限制的，但是**DNS是走UDP的呀**，所以修改为如下：

再来尝试一下：



果然现在就正常了。我们还可以使用`dig +trace`命令来追踪DNS解析过程。

回到顶部

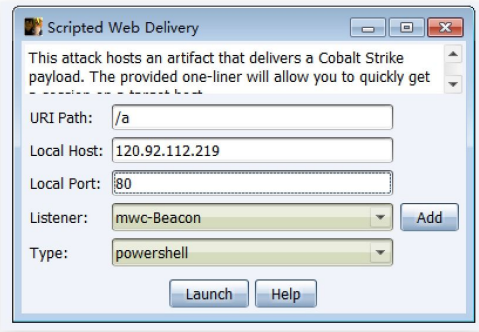
```
IpT6ALqubzhRe/iPccuI3eh1uI4sKdF5gs8rFVMi xJMu/A==
;; Received 733 bytes from 199.7.91.13#53(d.root-servers.net) in 247 ms

nvwa.me.                86400   IN      NS      ns53.domaincontrol.com.
nvwa.me.                86400   IN      NS      ns54.domaincontrol.com.
fsip6fkr2u8cf2kkg7scot4glihao6s1.me. 8400 IN NSEC3 1 1 1 D399EAAB FSJ06FFJ5GK2
ARHLBV052E4AB9V77M  NS SOA RRSIG DNSKEY NSEC3PARAM
fsip6fkr2u8cf2kkg7scot4glihao6s1.me. 8400 IN RRSIG NSEC3 7 2 8400 202003051016
 20200213091659 39077 me. QG8d06687qOhKF3x3iZFSf8hFIaCxGddKTwLsARGrTMHQ4j3dbjc
1A 8IMznzdRHaq45VH7LqMFPM3TPHsfjHy/R8THB8dLvu3OkWKc6myYOIMS r8vJqmsGzl0NfUr0Bn
L6oGB8CstIVh6wvvojIoq8JAl2X3vowCgML4 wxU=
4rjrhdggmnbu038lork3sdjkkge9rk0t.me. 8400 IN NSEC3 1 1 1 D399EAAB 4RP6390ETFIO
55BTPBVKE3O24CUMIM
4rjrhdggmnbu038lork3sdjkkge9rk0t.me. 8400 IN RRSIG NSEC3 7 2 8400 202003040749
 20200212064951 39077 me. aJ10QD5Ade6kNOY5UQTHylzFk/3uTdH24pP3ls3tAyWMFEQN/jnn
ro hkLcyaF4s8sHN8mSHrwhnm/sS4iyubY1Gd87cg4S061kQOvIVrKRNrAs kxOTnx9NNRrhrvr6Z3
98sUpAoieI8AcBvMmykETufX29+a5TPdaggb tK8=
;; Received 591 bytes from 199.249.127.1#53(b2.nic.me) in 303 ms

game.nvwa.me.           1800    IN      NS      malwarec2.nvwa.me.
;; Received 93 bytes from 173.201.74.27#53(ns54.domaincontrol.com) in 253 ms

thisisatest.game.nvwa.me. 1     IN      A       0.0.0.0
;; Received 82 bytes from 120.92.112.219#53(malwarec2.nvwa.me) in 24 ms
```

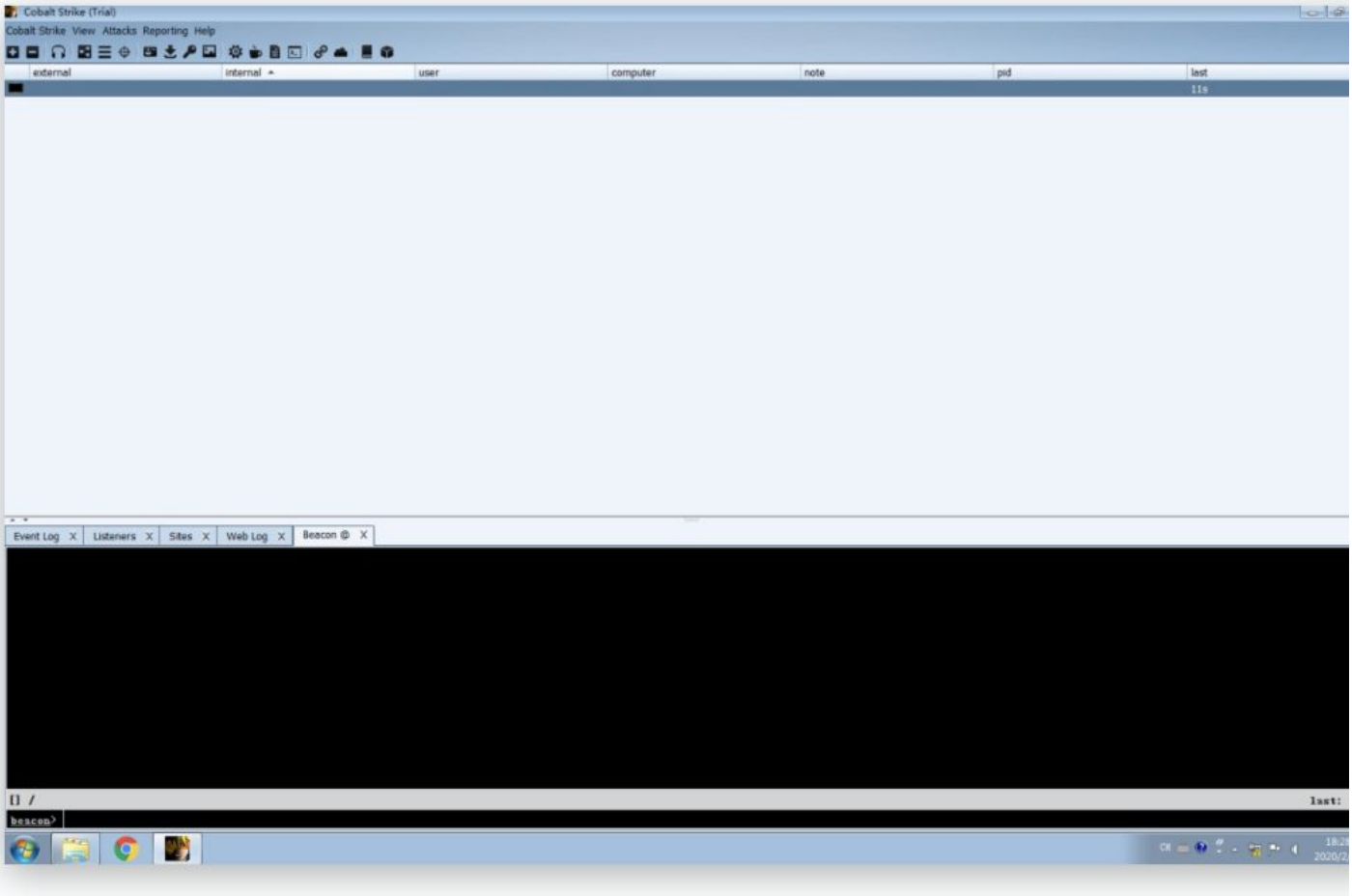
接下来我们还是生成一个powershell脚本：



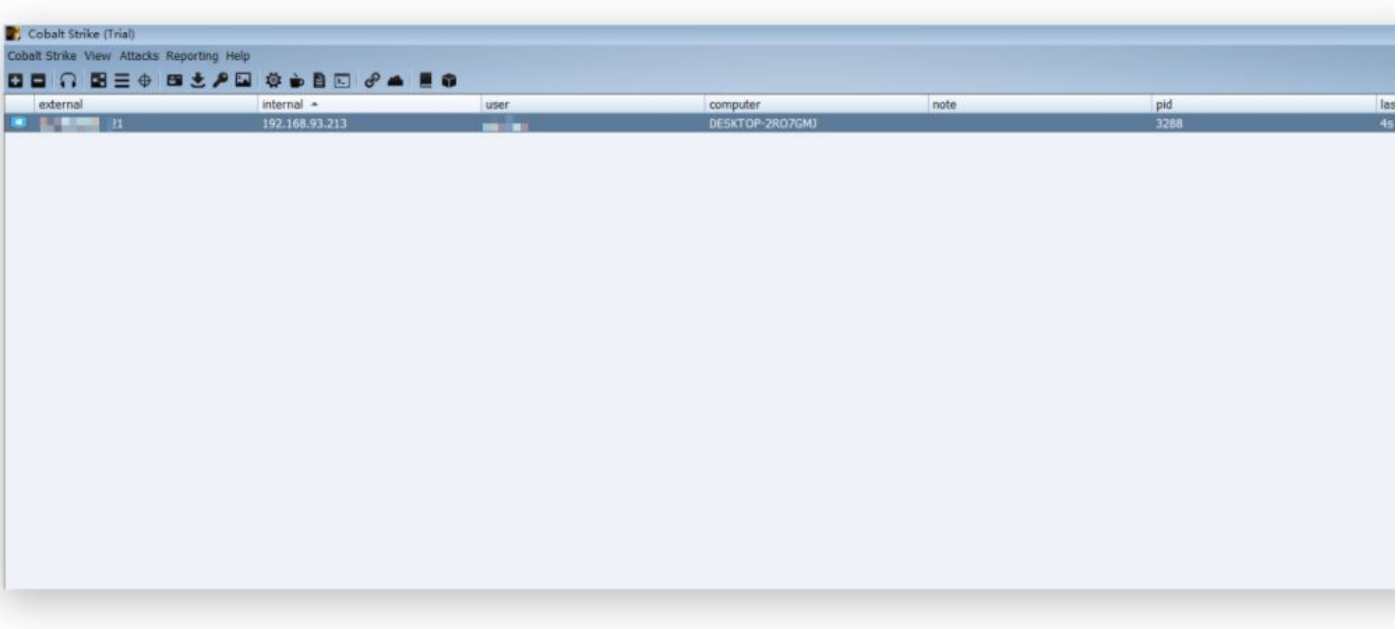
因为域名没备案，所以这里local host写的是IP地址，正常的话是要写malwarec2.nvwa.me

回到顶部

运行后主机上线：



回到顶部



bravo，当然还有另一种DNS Beacon是使用DNS TXT记录获取task任务，**欢迎小伙伴在下方留言哦～**

点我留言

长按二维码　关注我们

END

回到顶部

公告

关于微信安全公众号年度数据报告图表已经出炉，http://wechat.doonsec.com/year_report/ 访问查阅。
有好的数据分析建议，可在留言板中提出。

2020年

公众号文章

Cobalt Strike | DNS Beacon

微信原文链接

物联网IOT安全

u200b【IOT安全】IOT固件安全基础-固件仿真介绍

微信原文链接

物联网IOT安全

内网渗透的一次记录

微信原文链接

物联网IOT安全

Cobalt Strike | 配置转发器

微信原文链接

物联网IOT安全

【代码审计】PHP代码审计之CTF系列(1)

微信原文链接

物联网IOT安全

看我如何用Python操作单片机（一）

微信原文链接

物联网IOT安全

Cobalt Strike | Beacon原理浅析

微信原文链接

物联网IOT安全

Cobalt Strike番外 | 设置kali2020自启动

微信原文链接

物联网IOT安全

Cobalt Strike | 从入门到入狱

微信原文链接

物联网IOT安全

聚力战“疫”，赋能安全暨2020信息安全网络峰会开启报名！

微信原文链接

物联网IOT安全

回到顶部