基于HOOK和MMF的Windows密码渗透技术 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/271/2021_2022__E5_9F_BA_E4_BA_8EHOOK_c97_271877.htm 摘 要 随着计算机与网络的普及，信息安全越来越成为人们所普遍关心的大事。密码的渗透与反渗透在此领域表现的愈演愈烈。本文深入分析了各个版本windows密码的特点，尤其是针对windws2K/XP安全性提高的情况下，提出了获取windows密码的关键技术及方法。并进一步分析了windows钩子(Hook)和内存映像文件(MMF)的技术细节。在基于MMF的核心类CIPC中为钩子句柄在内存中的共享提供了方法，并且解决了线程间的同步问题。然后深入讨论了WM_COPYDATA消息的特点。接着分析了实例程序重要代码及注解并演示了结果。最终给出一些反密码渗透的应对策略。 关键词 内存映像文件.windows钩子.进程间通信.多线程 1、引言 上世纪90年纪使用过windows3.x的人可能很少有人了解这类操作系统中存在着密码保护的漏洞，如果选择密码控件中的“ **** ”文本然后复制到剪贴板上，那么看到的将不是“ **** ”而是密码的原始文本。微软发现了windows3.x这个问题并在新的版本window95中修改了这个漏洞。但是windows95存在着新的安全漏洞，可以设计出间谍程序从当前运行的程序中得到密码控件中的密码，这些间谍程序并非是如同softice一样的破解程序。然而，微软在window2000中又修补了这个问题，如何通过MMF与HOOK技术获取任何版本windows 密码控件的内容，这正是本文讨论的重点问题。 图1 Windows 2K/XP密码校验 获取Windows密码技术主要是利用了windows的安全漏洞。在windows

NT/95/98/ME等操作系统下，如果在间谍程序中发送WM_GETTEXT消息到密码控件，返回的文本将不再是“ **** ”而是实际的文本内容，而在windows2K/XP系统中微软加了安全控制，如果发送WM_GETTEXT到密码控件，系统将校验请求的进程判断该进程是否有许可权，如图1所示：如果请求进程与密码控件所在进程是同一进程，那么WM_GETTEXT消息将仍旧返回密码的真实文本。如果两个进程不一样，就返回一个ERROR_ACCESS_DENIED的错误。所以获取windows2K/XP密码的关键技术在于：从密码控件所在的进程中获取WM_GETTEXT消息，而不是在渗透进程中得到。而这种在其它进程中运行用户代码的技术完全可以利用windows 钩子(hook)技术来实现。首先我们需要了解一下什么是钩子。 2、Windows钩子 Windows系统是建立在事件驱动的机制上的，即整个系统都是通过消息的传递来实现的。钩子(hook)是一种特殊的消息处理机制，钩子可以监视系统或进程中的各种事件消息，截获发往目标窗口的消息并进行处理。这样，我们就可以在系统中安装自定义的钩子，监视系统中特定事件的发生，完成特定的功能，比如截获键盘、鼠标的输入，屏幕取词，日志监视等等。钩子的种类很多，每种钩子可以截获并处理相应的消息，如键盘钩子可以截获键盘消息，外壳钩子可以截取、启动和关闭应用程序的消息等。如图2是一全局钩子示意图。 在实例程序中运用WH_GETMESSAGE钩子，这个钩子监视投递到消息队列中的Windows消息。 图2 全局钩子的原理图 3、Windows钩子在此处的应用 安装钩子的函数为SetWindowsHookEx，利用这个函数可以为整个系统或为某一特定进程安装钩子，不同的钩

子监视特定钩子事件的发生，当某一事件触发后，与之对应的代码就会被系统调用。