Windows登陆密码破解解析Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/643/2021_2022_Windows_E7_99_BB_c100_643966.htm Windows登陆密码破解是如何办到的呢？这里向你全面介绍了Windows登陆密码破解的原理以及具体的操作和注意事项，让我们开始逐一讲述吧： Windows登陆密码破解原理： windows的身份验证一般最终都是在lsass进程，默认模块是msv1_0.dll，而关键在其导出函数LsaApLogonUserEx2， 本程序通过注入代码到lsass进程hook LsaApLogonUserEx2，截取密码。只要有身份验证的过程，LsaApLogonUserEx2就会触发，如ipc$,runsa,3389远程桌面登陆等。 程序对不同系统做了处理，在2000,2003,xp,vista上都可以截取， 在2000,2003,xp中，通过UNICODE_STRING.Length 的高8位取xor key,如果密码是编码过的，则通过ntdll.RtlRunDecodeUnicodeString解码， vista则通过AdvApi32.CredIsProtectedW判断密码是否编码过，解码用AdvApi32.CredUnprotectW。 可以自己调试器挂lsass跑一下:)本文来源:百考试题网 Windows登陆密码破解之接口问题： HRESULT WINAPI DllInstall(BOOL bInstall, LPCWSTR pszCmdLine). 这是本dll导出的一个函数原型，请不要被名字蛊惑了，这个程序是绿色的。 这个函数内部并没有做任何自启动安装的动作，没有修改注册表或系统文件。只是想选一个符合regsvr32调用的接口而已。 第一个参数本程序没用到，第二个参数请指定一个文件路径(注意是UNICODE的)，记录到的数据将保存到这里（是Ansi的）。 文件路径可以像这样C:\x.log， 也可以像\\.\pipe\your_pipename,\\.\mailslot\yourslot

，www. Examda.CoM考试就到百考试题 所以你可以自己写loader来调用这个dll，让dll截取到密码时通过pipe或mailslot将数据发给你的程序。数据就是一个字符串（是Ansi的）
Windows登陆密码破解的测试： 你可以不急着写自己的loader来调用，用regsvr32作为loader来测试一下：(你可能需要关闭某些主动防御) regsvr32 /n /i:c:\xxx.log c:\pluginWinPswLogger.dll
正常的话regsvr32弹出一个提示成功。 这时候你可以切换用户或锁定计算机，然后重新登陆进去，这个过程密码信息就被拦截下来了并保存到c:\xxx.log。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com