尝试破解Windows系统EFS加密文件 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/259/2021_2022__E5_B0_9D_E8_AF_95_E7_A0_B4_E8_c100_259138.htm 本文记录的是我偶然的一次破解EFS文件加密技术的经历。这仅是我偶然发现的一个方法，而不是一种破解技术，因为内中的原理我仅能推测，而使用的软件也都是别人设计的。我顶多算是比别人更早地找到了组合利用某些既有工具的方法而已。题记EFS(Encrypting File System，加密文件系统)加密是一种基于NTFS磁盘技术的加密技术。EFS加密基于公钥策略。在使用EFS加密一个文件或文件夹时，系统首先会生成一个由伪随机数组成的FEK(File Encryption Key，文件加密钥匙)，然后将利用FEK和数据扩展标准X算法创建加密后的文件，并把它存储到硬盘上，同时删除未加密的原始文件。接下来系统利用你的公钥加密FEK，并把加密后的FEK存储在同一个加密文件中。而在访问被加密的文件时，系统首先利用当前用户的私钥解密FEK，然后利用FEK解密出文件。在首次使用EFS时，如果用户还没有公钥/私钥对(统称为密钥)，则会首先生成密钥，然后加密数据。如果你登录到了域环境中，密钥的生成依赖于域控制器，否则它就依赖于本地机器。说起来非常复杂，但是导适褂霉讨芯兔挥心敲绰桦沉恕FS加密的用户验证过程是在登录Windows时进行的，只要登录到Windows，就可以打开任何一个被授权的加密文件。换句话说，EFS加密系统对用户是透明的。这也就是说，如果你加密了一些数据，那么你对这些数据的访问将是完全允许的，并不会受到任何限制。而其他非授权用户试图访问你加密过的数据时，就会收

到“ 访问拒绝 ”的错误提示。 我的电脑一般来说不会有别人使用，而我经常重装系统，又懒得备份密钥，所以我从来没有使用过windows 2003或者windows xp的EFS功能。今天读到了一些关于EFS密钥没有备份因而数据无法恢复的求助帖子，所以突然想出一个点子想试着解开EFS的加密。 我构造的试验环境是在windows xp Pro SP2系统中的一块NTFS磁盘上建立一个test文件夹，启用EFS加密。文件夹中是一个加密过的文本文件1.txt。现在我先用另一个帐户去尝试读取这个文件，然后在第二个系统中(相当于重装系统没有证书的情况)再次尝试读取这个文件。 第一步，启用我系统中的GUEST帐户。此时从资源管理器中是不能访问test文件夹的。 打开cmd，在任务管理器中终止explorer.exe进程，打开PsExec尝试用system登录。 失败。提示进程无法创建。看来全县不够。 回到管理员帐户，新建一个管理员帐户test并以之登录。 在test帐户中运行资源管理器可以访问test文件夹，但是不能打开1.txt加密文件。 此时再用上法以system登录。此时打开文件为乱码! 运行IceSword.exe，在 文件 中定位test文件夹。右键选择1.txt，复制到桌面，文件名任意，后缀不变。 双击打开文件，正常读出!第一步破解EFS成功! 第二步，登陆Windows Server 2003 SP1系统(管理员身份)。 使用上述方法再次复制1.txt到桌面，打开后出现乱码，和system读取时情况一致。第二种尝试失败。 总结： 本方法意义： 目前仅适用于察看系统中其他人使用EFS加密过的文件(请读者务必不要做违法及危害他人权利的事!)，在系统重装或私钥丢失情况下的文件恢复有待进一步地探索。 本方法使用的两个软件： PsExec IceSword。前者是国外非常流行的远程控制软件，命令行界面。后者则是PJF制

作的国内著名隐藏进程察看软件冰刃。 本方法适用条件： 1. 需要足够运行上述两个软件的权限(如果可以结合net user命令的话应该不难，这只是一个小提示，读者还请自律^_^)。 2. 系统内还有该EFS加密文件对应的密钥(这一条件是基于我的初步推测) 本方法成功的原因浅析： 1. 利用了system帐户特有的内核级权限，这可能是能够读取管理员或其他正常用户密钥的条件。 2. IceSword特有的读取加密文件的技术。关于这一点，是我最百思不得其解的地方，真希望能听到PJF亲自阐述一下这是如何实现的0.0 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