 当黑客入侵一台主机后，会想方设法保护自己的“ 劳动成果 ”，因此会在肉鸡上留下种种后门来长时间得控制肉鸡,其中使用最多的就是账户隐藏技术。在肉鸡上建立一个隐藏的账户，以备需要的时候使用。账户隐藏技术可谓是最隐蔽的后门，一般用户很难发现系统中隐藏账户的存在，因此危害性很大，本文就对隐藏账户这种黑客常用的技术进行揭密。 在隐藏系统账户之前，我们有必要先来了解一下如何才能查看系统中已经存在的账户。在系统中可以进入“ 命令提示符 ”，控制面板的“ 计算机管理 ”，“ 注册表 ”中对存在的账户进行查看，而管理员一般只在“ 命令提示符 ”和“ 计算机管理 ”中检查是否有异常，因此如何让系统账户在这两者中隐藏将是本文的重点。 一、“ 命令提示符 ”中的阴谋 其实，制作系统隐藏账户并不是十分高深的技术，利用我们平时经常用到的“ 命令提示符 ”就可以制作一个简单的隐藏账户。 点击“ 开始 ”→“ 运行 ”，输入“ CMD ”运行“ 命令提示符 ”，输入“ net user piao$ 123456 /add ”，回车，成功后会显示“ 命令成功完成 ”。接着输入“ net localgroup administrators piao$ /add ”回车，这样我们就利用“ 命令提示符 ”成功得建立了一个用户名为“ piao$ ”，密码为“ 123456 ”的简单“ 隐藏账户 ”,并且把该隐藏账户提升为了管理员权限。 我们来看看隐藏账户的建立是否成功。在“ 命令提示符 ”中输入查看系统账户的命令“ net user ”，回车后会显示当前系统中存在的账户。从返回

的结果中我们可以看到刚才我们建立的“ piao$ ”这个账户并不存在。接着让我们进入控制面板的“ 管理工具 ”，打开其中的“ 计算机 ”，查看其中的“ 本地用户和组 ”，在“ 用户 ”一项中，我们建立的隐藏账户“ piao$ ”暴露无疑。 可以总结得出的结论是：这种方法只能将账户在“ 命令提示符 ”中进行隐藏，而对于“ 计算机管理 ”则无能为力。因此这种隐藏账户的方法并不是很实用，只对那些粗心的管理员有效，是一种入门级的系统账户隐藏技术。 二、在“ 注册表 ”中玩转账户隐藏 从上文中我们可以看到用命令提示符隐藏账户的方法缺点很明显，很容易暴露自己。那么有没有可以在“ 命令提示符 ”和“ 计算机管理 ”中同时隐藏账户的技术呢？答案是肯定的，而这一切只需要我们在“ 注册表 ”中进行一番小小的设置，就可以让系统账户在两者中完全蒸发。 1、峰回路转，给管理员注册表操作权限 在注册表中对系统账户的键值进行操作，需要到“ HKEY_LOCAL_MACHINE\SAM\SAM ”处进行修改，但是当我们来到该处时，会发现无法展开该处所在的键值。这是因为系统默认对系统管理员给予“ 写入D AC ”和“ 读取控制 ”权限，没有给予修改权限，因此我们没有办法对“ SAM ”项下的键值进行查看和修改。不过我们可以借助系统中另一个“ 注册表编辑器 ”给管理员赋予修改权限。 点击“ 开始 ”→“ 运行 ”，输入“ regedt32.exe ”后回车，随后会弹出另一个“ 注册表编辑器 ”，和我们平时使用的“ 注册表编辑器 ”不同的是它可以修改系统账户操作注册表时的权限（为便于理解，以下简称regedt32.exe）。在regedt32.exe中来到“ HKEY_LOCAL_MACHINE\SAM\SAM ”处，点击“ 安全 ”

菜单→“ 权限 ”，在弹出的“ SAM的权限 ”编辑窗口中选中“ administrators ”账户，在下方的权限设置处勾选“ 完全控制 ”，完成后点击“ 确定 ”即可。然后我们切换回“ 注册表编辑器 ”，可以发现“ HKEY_LOCAL_MACHINE\SAM\SAM ”下面的键值都可以展开了。 提示：上文中提到的方法只适用于Windows NT/2000系统。在Windows XP系统中，对于权限的操作可以直接在注册表中进行，方法为选中需要设置权限的项，点击右键，选择“ 权限 ”即可。 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