隐藏管理员账号三分钟搞定 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022__E9_9A_90_E8_97_8F_E7_AE_A1_E7_c100_460789.htm 对regedit.exe大家都很熟悉，但却不能对注册表的项键设置权限，而regedt32.exe最大的优点就是能够对注册表的项键设置权限。nt/2000/xp的帐户信息都在注册表的HKEY_LOCAL_MACHINE＼SAM＼SAM键下，但是除了系统用户SYSTEM外，其它用户都无权查看到里面的信息，因此我首先用regedt32.exe对SAM键为我设置为“ 完全控制 ”权限。这样就可以对SAM键内的信息进行读写了了。具体步聚如下： 1、假设我们是以超级用户administrator登录到开有终端服务的肉鸡上的，首先在命令行下或帐户管理器中建立一个帐户：hacker$，这里我在命令行下建立这个帐户 net user hacker$Content$nbsp；1234 /add 2、在开始/运行中输入：regedt32.exe并回车来运行regedt32.exe. 3、点“ 权限 ”以后会弹出窗口点添加将我登录时的帐户添加到安全栏内，这里我是以administrator的身份登录的，所以我就将administrator加入，并设置权限为“ 完全控制".这里需要说明一下：最好是添加你登录的帐户或帐户所在的组，切莫修改原有的帐户或组，否则将会带来一系列不必要的问题。等隐藏超级用户建好以，再来这里将你添加的帐户删除即可。 4、再点“ 开始 ”→“ 运行 ”并输入"regedit.exe" 回车，启动注册表编辑器regedit.exe. 打开键：HKEY_LOCAL_MAICHINE＼SAM＼SAM＼Domains＼account＼user＼names＼hacker$" 5、将项hacker$、00000409、000001F4导出为hacker.reg、409.reg、1f4.reg，用记事本分别

打这几个导出的文件进行编辑，将超级用户对应的项000001F4下的键"F"的值复制，并覆盖hacker$对应的项00000409下的键"F"的值，然后再将00000409.reg与hacker.reg合并。 6、在命令行下执行net user hacker$Content$nbsp；/del将用户hacker$删除：net user hacker$Content$nbsp；/del 7、在regedit.exe的窗口内按F5刷新，然后打文件-导入注册表文件将修改好的hacker.reg导入注册表即可 8、到此，隐藏的超级用户hacker$已经建好了，然后关闭regedit.exe.在regedt32.exe窗口内把HKEY_LOCAL_MACHINE＼SAM＼SAM键权限改回原来的样子（只要删除添加的帐户administrator即可）。 9、注意：隐藏的超级用户建好后，在帐户管理器看不到hacker$这个用户，在命令行用“ net user ”命令也看不到，但是超级用户建立以后，就不能再改密码了，如果用net user命令来改hacker$的密码的话，那么在帐户管理器中将又会看这个隐藏的超级用户了，而且不能删除。