Windows中多种隐藏超级用户方法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/275/2021_2022_Windows_E4_B8_AD_c67_275703.htm 一、如何在图形界面建立隐藏的超级用户 图形界面下适用本地或开3389终端服务的肉鸡上。上面我提到的那位作者说的方法很好，但是较为复杂，还要用到psu.exe(让程序以系统用户身份运行的程序)，如果在肉鸡上的话还要上传psu.exe。我说的这个方法将不用到psu.exe这个程序。因为Windows2000有两个注册表编辑器：regedit.exe和regedt32.exe。XP中regedit.exe和regedt32.exe实为一个程序，修改键值的权限时在右键中点“ 权限 ”来修改。对regedit.exe我想大家都很熟悉，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_MacHINESAMSAM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$,这里我在命令行下建立这个帐户 net user hacker$ 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_MAICHINESAMSAMDomainsaccountusernameshacker___FCKpd___1quot. 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$ /del将用户hacker$删除： net user hacker$ /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$已经建好了，然后关闭regedit.exe。在regedt32.exe窗口内把HKEY_LOCAL_MACHINESAMSAM键权限改回原来的样子(只要删除添加的帐户administrator即可)。 9、注意：隐藏的超级用户建好后，在帐户管理器看不到hacker$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。 一、如何在图形界面建立隐藏的超级用户 图形界面下适用本地或开3389终端服务的肉鸡上。上面我提到的那位作者说的方法很好，但是较为复杂，还要用到psu.exe(让程序以系统用户身份运行的程序)，如果在肉鸡上的话还要上传psu.exe。我说的这个方法将不用到psu.exe这

个程序。因为Windows2000有两个注册表编辑器：regedit.exe和regedt32.exe。XP中regedit.exe和regedt32.exe实为一个程序，修改键值的权限时在右键中点“ 权限 ”来修改。对regedit.exe我想大家都很熟悉，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_MacHINESAMSAM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$,这里我在命令行下建立这个帐户 net user hacker$ 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_MAICHINESAMSAMDomainsaccountusernameshacker___FCKpd___1quot. 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$对应的项00000409下的键“ F ”的值,然后再将00000409.reg与hacker.reg合并。 6、在命令行下执行net user hacker$ /del将用户hacker$删除： net user hacker$ /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$已经建好了，然后关闭regedit.exe。在regedt32.exe窗口内把HKEY_LOCAL_MACHINESAMSAM键权限改回原来的样子(只要删除添加的帐户administrator即可)。 9、注意：隐藏的超级用户建好后，在帐户管理器看不到hacker$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$的密码的话，那么在帐户管理器中将又会看这个隐藏的超级用户了，而且不能删除。 三、如果肉鸡没有开3389终端服务，而我又不想用命令行，怎么办? 这种情况下，你也可以用界面方式来远程为肉鸡建立隐藏的超级用户。因为regedit.exe、regedt32.exe都有连接网络注册表的功能，你可以用regedt32.exe来为远程主机的注册表项设置权限，用regedit.exe来编辑远程注册表。帐户管理器也有一项连另一台计算机的功能，你可以用帐户管理器为远程主机建立和删除帐户。具体步聚与上面介绍的相似，我就不多说了，只它的速度实在是令人难以忍受。 是这里有两个前提：1、先用net use 肉鸡ipipc$ "密码" /user:"超级用户名"来与远程主机建立连接以后，才能用regedit.exe regedt32.exe及帐户管理器与远程主机连接。 2、远程主机必须开启远程注册表服务(没有开启的话，你也可以远程开启，因为你有超级用户的密码了)。

四、利用被禁用的帐户建立隐藏的超级用户 我们可以用肉鸡上被禁止的用户来建立隐藏的超组用户.方法如下： 1.想办法查看有哪些用户被细心的管理员禁止，一般情况下，有些管理员出于安全考虑，通常会将guest禁用，当然了会禁用其它用户。在图形界面下，非常容易，只要在帐户管理器中就可以看到被禁用的帐户上有一个红叉.而在命令行下，我还没有想到好的办法，只能在命令行下用命令：“ net user 用户名 ”一个一个来查看用户是否被禁用。 2.在这里，我们假设用户hacker被管理员禁用。首先，我先用小榕的超组用户克隆程序CA.exe，将被禁用的用户hacker 克隆成超级用户(克隆之后，被禁用的用户hacker就会自动被激活了)： CA.EXE 肉鸡ip Administrator 超级用户密码 hacher hacher密码。 3.如果你现在一个cmdshell，如利用telnet服务或SQLEXEC连接肉鸡的msSQL的默认端口1433得到的shell都可以，这时你只要输入命令： net user hacker /active:no 这样用户hacker就被禁用了(至少表面上是这样的)，当然你也可以将用户hacher换成其它的被禁用的用户。 4.这时如果你在图形界面下看帐户管理器中的用户时,会发现用户hacker被禁用了，但事实上是这样的吗?你用这个被禁用的用户连接一下肉鸡看看是否能连上?用命令：net user 肉鸡ipipc$ "hacker密码" /user:"hacker" 连一连看看。我可以告诉大家，经过我多次试验，次次都能成功，而且还是超级用户权限。 5.如果没有cmdshell怎么办?你可以我上面介绍的at命令来禁用用户hacker.命令格式：at 肉鸡ip 时间 net user hacker /active:no 6.原理：具体的高深的原理我也说不上来，我只能从最简单的说。你先在图形界面下在帐户管理器中禁用一下超级用户administrator看看，肯定会弹出一对话框，

并禁止你继续禁用超级用户administrator，同样，因为在克隆时，hacker在注册表的“ F ”键被超级用户administrator在注册表的“ F ”键所替代，因而hacker就具有了超级用户的权限了，但是由于hacker在注册表内“ C ”健还是原来的“ C ”键，所以hacker还是会被禁用，但是它的超级用户权限却不会被禁用，因此被禁用的用户hacker还是可以连接肉鸡，而且还具有超级用户的权限。具体我也说不明白，大家权且这么理解吧。 五、注意的几点事项 1、隐藏的超级用户建立以后，在帐户管理器中和命令行下均看不到这个用户，但这个用户却存在。 2、隐藏的超级用户建立以后，就不能再修改密码了，因为一旦修改密码，这个隐藏的超级用户就会暴露在帐户管理器中，而且不能删除。 3、如在本机上试验时，最好用系统自带的备份工具先备份好本机的“ 系统状态 ”主要是注册表的备份，因为本人做试验时，曾出现过帐户管理器中看不到任何用户，组中也看不到任何组的现象，但它们却存在。幸好我有备份,呵呵。SAM键是毕竟系统最敏感的部位。 4、本方法在2000/XP上测试通过，未在NT上测试。 