辅导Windows服务器安全设置经验详谈三 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/62/2021_2022__E8_BE_85_E5_AF_BCWind_c40_62250.htm 防止Serv-U权限提升 其实，注销了Shell组件之后，侵入者运行提升工具的可能性就很小了，但是prel等别的脚本语言也有shell能力，为防万一，还是设置一下为好。 用Ultraedit打开ServUDaemon.exe查找Ascii：LocalAdministrator，和#l@$ak#.lk.0@P，修改成等长度的其它字符就可以了，ServUAdmin.exe也一样处理。 另外注意设置Serv-U所在的文件夹的权限，不要让IIS匿名用户有读取的权限，否则人家下走你修改过的文件，照样可以分析出你的管理员名和密码。 利用ASP漏洞攻击的常见方法及防范 一般情况下，黑客总是瞄准论坛等程序，因为这些程序都有上传功能，他们很容易的就可以上传ASP木马，即使设置了权限，木马也可以控制当前站点的所有文件了。另外，有了木马就然后用木马上传提升工具来获得更高的权限，我们关闭shell组件的目的很大程度上就是为了防止攻击者运行提升工具。 如果论坛管理员关闭了上传功能，则黑客会想办法获得超管密码，比如，如果你用动网论坛并且数据库忘记了改名，人家就可以直接下载你的数据库了，然后距离找到论坛管理员密码就不远了。 作为管理员，我们首先要检查我们的ASP程序，做好必要的设置，防止网站被黑客进入。另外就是防止攻击者使用一个被黑的网站来控制整个服务器，因为如果你的服务器上还为朋友开了站点，你可能无法确定你的朋友会把他上传的论坛做好安全设置。这就用到了前面所说的那一大堆东西，做了那些权限设置和防提升之后，黑客

就算是进入了一个站点，也无法破坏这个网站以外的东西。
后记 也许有安全高手或者破坏高手看了我的文章会嘲笑或者窃喜，但我想我的经验里毕竟还是存在很多正确的地方，有千千万万的比我知道的更少的人像我刚开始完全不懂的时候那样在渴求着这样一篇文章，所以我必须写，我不管别人怎么说我，我也不怕后世会有千千万万的人对我唾骂，我一个人承担下来，我也没有娘子需要交代的…… 因为这其实只是抛砖引玉的做法，从别人的笑声中，我和我的读者们都可以学到更多有用的东西。 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