

如何在非root状态下用root身份执行命令 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/181/2021_2022__E5_A6_82_E4_BD_95_E5_9C_A8_E9_c103_181667.htm 用非root身份运行X

大多数人犯下的第一个错误是：一开始就以root身份运行X，无意中一切都变得非常简单能够直接访问到所有的文件，系统管理任务可以轻松地搞定，能够安装新的软件，等等。问题在于有许多程序是不应该用root身份运行的。如果你用自己的身份（非root身份）启动文件管理器，然后删除/home，你会丢失自己的所有文件，然后一边寻找备份文件一边不停地抱怨自己。万幸的是所有其他用户的文件都还安然无恙。但是，如果你用root来做同样的事情，马上就会陷入众人的抱怨和诅咒之中。文件共享程序也同样不应该用root身份运行。如果有人找出了Irc或者Gnutella程序的漏洞，他们最多只能偷窃你自己的文件。但如果你用root来运行这些程序，所有用户的文件将完全暴露在他们的眼前，包括最最重要的/etc/shadow密码文件，以及你同事的私人邮件。这可不是什么好事。所以，请务必用你自己的帐号来运行X，用本文下面介绍的方法来运行那些必须使用root才能运行的任务。su和su - 假设有人占据了拨号线路，我们想知道那个家伙到底是谁。tcpdump会显示出线路上的数据包传输情况，我们来试试下面这个命令：[wstearns@sparrow wstearns]\$ tcpdump -i ppp0 -qtntcpdump: socket: Operation not permitted 哦，对了。这个shell和所有其他X下的程序一样，都用wstearns运行。你会想我可以从命令行提示看出来，不是吗？:-) 不过，我可不想只为了一个命令从X完全退出。su命令让我们用另外一个用户

临时地替代当前用户。如果不指定自己想成为哪一个用户，则su默认我们想成为root。不要吓起哄说什么黑客技术，除非当前用户就是root，否则还是老老实实给su提供目标用户的密码。:-)[wstearns@sparrow wstearns]\$ tcpdump -i ppp0

```
-qnttcpdump: socket: Operation not permitted[wstearns@sparrow
wstearns]$ su - Password: [root@sparrow /root]# tcpdump -i ppp0
-qUser level filter, protocol ALL, datagram packet sockettcpdump:
listening on ppp0 ME.33085: tcp 1448 (DF) [tos 0x10]> ME.33085
> reflectix.xs4all.nl.29788: tcp 0 (DF) ME.33085: tcp 1448 (DF) [tos
0x10]> ME.33085 > reflectix.xs4all.nl.29788: tcp 0 (DF) ME.33085:
tcp 1448 (DF) [tos 0x10]> ME.33085 > reflectix.xs4all.nl.29788: tcp
0 (DF) ME.33085: tcp 1448 (DF) [tos 0x10]7 packets received by
filter[root@sparrow /root]# exit[wstearns@sparrow wstearns]$ 哦，
原来是我自己下载文件占用了拨号线路。呵呵。你或许已经
注意到，上面这个例子使用的是su -而不是su。“-”将提供
目标用户的环境来替代当前用户的环境。下面这个例子很明
确地说明了这一点，不用su -时shell不能在/sbin和/usr/sbin下找
到我们要执行的命令：[wstearns@sparrow wstearns]$
suPassword: [root@sparrow wstearns]# tcpdump -i ppp0 -qtbash:
tcpdump: command not found[root@sparrow wstearns]#
exit[wstearns@sparrow wstearns]$ 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
```