

永远不要运行的危险Linux命令！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__E6_B0_B8_E8_BF_9C_E4_B8_8D_E8_c103_644804.htm 文中列出的命令绝对不可以运行，即使你觉得很好奇也不行，除非你是在虚拟机上运行（出现问题你可以还原），因为它们会实实在在的破坏你的系统。所以不在root等高级管理权限下执行命令是很好的习惯。早晚有一天，Linux系统会像Windows那样流行，用的人越来越多，包括对计算机不是很了解的人，本文的目的就是告诉大家：在Linux给你最大程度自由度的同时，也使得破坏系统变得更加容易，如果你不了解某些命令的意义，下载执行包含恶意命令的脚本，或者被骗运行某些命令，很容易让你哭都来不及。这并不是说明Linux不安全，只是说明在不了解Linux，和很不小心的人面前，Linux十分不安全。Windows也好，Linux也好，人本身才是最大的不安全因素。来源：考试大 下面的命令会删除你硬盘上的文件，rm的-r递归删除，和-f强制删除是很危险的选项，即使日常操作，也会遇到误删文件的情况。sudo rm -rf / 删除根分区全部的文件 sudo rm -rf . 删除当前目录下的所有文件 sudo rm -rf * 同上 rm -rf * or rm -rf *.* 同上 rm -rf ~ / gt. /dev/sda 用随意的数据破坏硬盘上面的sda、sdb也可能是其他类似的名称。Linux的/dev系统给操纵硬件提供了很方便和强大的功能，同时也使得破坏变得更容易。fork命令打开一个子进程，如果把fork放在无限循环中，最终子进程会耗尽所有内存资源：:(){:|:amp. ”。百考试题论坛 python 一类的脚本语言，同样可以拿来搞破坏：python -c import os.

`os.system(''.join([chr(ord(i)-1) for i in "sn!.sg! "]))` 这段程序实际上会执行 `rm -rf *`，也许你很奇怪上面程序结尾的“sn!.sg!”是什么意思，实际上就是 `rm -rf *` 每个字母的下一个！那么我们如何避免运行恶意程序呢？第一不要用 root 作为日常使用的用户，上面的程序，如果当前用户不是 root，危害的波及范围就会小很多。第二要知道哪些命令是干什么用的，不知道的命​​令不要冒然运行。运行有潜在破坏能力的程序，要小心检查自己的输入。第三要保证软件、脚本的来源正规。来源：考试大的美女编辑们 最后一点，虽然比较消极，但是确实十分重要的一点：经常备份你的数据！！编辑特别推荐：[Linux系统通过手机GPRS上网设置简介](#) [提高Apache服务器性能四个建议](#) [Linux认证能帮助你找到一份好工作吗](#) [linux面试题参考答案](#) [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