通过监控Linux下进程来保证系统安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/260/2021_2022__E9_80_9A_E8_BF_87_E7_9B_91_E6_c103_260894.htm 通过综合采用用户级别的top、ps等系统工具以及Linux内核防护技术，我们可以从用户/内核两个层次全方位地保护Linux系统中重要系统进程以及用户进程的安全性。 经典的信息保密性安全模型Bell-LaPadula模型指出，进程是整个计算机系统的一个主体，它需要通过一定的安全等级来对客体发生作用。进程在一定条件下可以对诸如文件、数据库等客体进行操作。如果进程用作其他不法用途，将给系统带来重大危害。在现实生活当中，许多网络黑客都是通过种植“ 木马 ”的办法来达到破坏计算机系统和入侵的目的，而这些“ 木马 ”程序无一例外的是需要通过进程这一方式在机器上运行才能发挥作用的。另外，许多破坏程序和攻击手段都需要通过破坏目标计算机系统的合法进程尤其是重要系统进程，使得系统不能完成正常的工作甚至无法工作，从而达到摧毁目标计算机系统的目的。作为服务器中占绝大多数市场份额的Linux系统，要切实保证计算机系统的安全，我们必须对其进程进行监控和保护。 用户级进程监控工具 Linux系统提供了who、w、ps和top等察看进程信息的系统调用，通过结合使用这些系统调用，我们可以清晰地了解进程的运行状态以及存活情况，从而采取相应的措施，来确保Linux系统的安全。它们是目前在Linux下最常见的进程状况查看工具，它们是随Linux套件发行的，安装好系统之后，用户就可以使用。 1.who命令:该命令主要用于查看当前在线上的用户情况。系统管理员可以使用who命

令监视每个登录的用户此时此刻的所作所为。 2.w命令:该命令也用于显示登录到系统的用户情况，但是与who不同的是，w命令功能更加强大，它不但可以显示有谁登录到系统，还可以显示出这些用户当前正在进行的工作，w命令是who命令的一个增强版。 3.ps命令:该命令是最基本同时也是非常强大的进程查看命令。利用它可以确定有哪些进程正在运行及运行的状态、进程是否结束、进程有没有僵死、哪些进程占用了过多的资源等。ps命令可以监控后台进程的工作情况，因为后台进程是不和屏幕键盘这些标准输入/输出设备进行通信的，如果需要检测其情况，可以使用ps命令。下面是一个ps命令的例子 $ ps x PID TTY STAT TIME COMMAND 5800 ttyp0 S 0:00 -bash 5813 ttyp1 S 0:00 -bash 5921 ttyp0 S 0:00 man ps 5922 ttyp0 S 0:00 sh -c /usr/bin/gunzip -c /var/catman/cat1/ps.1.gz/ 5923 ttyp0 S 0:00 /usr/bin/gunzip -c /var/catman/cat1/ps.1.gz 5924 ttyp0 S 0:00 /usr/bin/less -is 5941 ttyp1 R 0:00 ps x 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