Linux网络安全之经验谈(3) PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/143/2021_2022_Linux_E7_BD_91_E7_BB_c103_143835.htm 关于su命令 如果你不想任何人能够su为root的话,你应该编辑/etc/pam.d/su文件，加下面几行：auth sufficient /lib- /security/pam_rootok- .so debug auth required /lib- /security/pam_wheel- .so group=isd 这意味着仅仅isd组的用户可以su作为root。如果你希望用户admin能su作为root.就运行下面的命令： usermod -G10 admin suid程序也是非常危险的，这些程序被普通用户以euid=0（即root）的身份执行，只能有少量程序被设置为suid。用这个命令列出系统的suid二进制程序： suneagle# find / -perm -4000 -print 你可以用chmod -s去掉一些不需要程序的suid位。 关于账户注销 如果系统管理员在离开系统时忘了从root注销，系统应该能够自动从shell中注销。那么，你就需要设置一个特殊的 Linux 变量“ tmout ”，用以设定时间。 同样，如果用户离开机器时忘记了注销账户，则可能给系统安全带来隐患。你可以修改/etc/profile文件，保证账户在一段时间没有操作后，自动从系统注销。 编辑文件/etc/profile，在“ histfilesize= ”行的下一行增加如下一行: tmout=600 则所有用户将在10分钟无操作后自动注销。注意：修改了该参数后，必须退出并重新登录root，更改才能生效。 关于系统文件 对于系统中的某些关键性文件如passwd、passwd.old、passwd._、shadow、shadown._、inetd.conf、services和lilo.conf等可修改其属性，防止意外修改和被普通用户查看。 如将inetd文件属性改为600：# chmod 600 /etc/inetd.conf 这样就保证文件的属主为root,

然后还可以将其设置为不能改变: # chattr i /etc/inetd.conf 这样，对该文件的任何改变都将被禁止。 你可能要问：那我自己不是也不能修改了？当然，我们可以设置成只有root重新设置复位标志后才能进行修改: # chattr -i /etc/inetd.conf 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