操作系统安全防护技巧介绍之Linux篇 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022__E6_93_8D_E4_BD_9C_E7_B3_BB_E7_c103_145345.htm 系统安全性对于用户来说至关重要，Linux用户也不例外。笔者就自己使用Linux的经历，总结了一些增强Linux安全防护的小窍门，在此介绍给大家。 1．为LILO增加开机口令 在/etc/lilo.conf文件中增加选项，从而使LILO启动时要求输入口令，以加强系统的安全性。具体设置如下： boot=/dev/hdamap=/boot/mapinstall=/boot/boot.btime-out=60 #等待1分钟promptdefault=linuxpassword=#口令设置image=/boot/vmlinuz-2.2.14-12label=linux initrd=/boot/initrd-2.2.14-12.img root=/dev/hda6 read-only此时需注意，由于在LILO中口令是以明码方式存放的，所以还需要将 lilo.conf的文件属性设置为只有root可以读写。 # chmod 600 /etc/lilo.conf当然，还需要进行如下设置，使lilo.conf的修改生效。 # /sbin/lilo -v2．设置口令最小长度和 最短使用时间 口令是系统中认证用户的主要手段，系统安装时默认的口令最小长度通常为5，但为保证口令不易被猜测攻击，可增加口令的最小长度，至少等于8。为此，需修改文件/etc/login.defs中参数PASS_MIN_LEN。同时应限制口令使用时间，保证定期更换口令，建议修改参数PASS_MIN_DAYS。 3．用户超时注销 如果用户离开时忘记注销账户，则可能给系统安全带来隐患。可修改/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。 4．禁止访问重要文件 对于系统中的某些关键性文件如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。 首先改变文件属性为600： # chmod 600 /etc/inetd.conf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。 只有root重新设置复位标志后才能进行修改： # chattr -i /etc/inetd.conf5．允许和禁止远程访问 在Linux中可通过/etc/hosts.allow 和/etc/hosts.deny 这2个文件允许和禁止远程主机对本地服务的访问。通常的做法是：(1)编辑hosts.deny文件，加入下列行： # Deny access to everyone. ALL: ALL@ALL则所有服务对所有外部主机禁止，除非由hosts.allow文件指明允许。 (2)编辑hosts.allow 文件，可加入下列行: #Just an example: ftp: 202.84.17.11 xinhuanet.com则将允许IP地址为202.84.17.11和主机名为xinhuanet.com的机器作为Client访问FTP服务。 (3)设置完成后，可用tcpdchk检查设置是否正确。 6．限制Shell命令记录大小 默认情况下，bash shell会在文件$HOME/.bash_history中存放多达500条命令记录(根据具体的系统不同，默认记录条数不同)。系统中每个用户的主目录下都有一个这样的文件。在此笔者强烈建议限制该文件的大小。 您可以编辑/etc/profile文件，修改其中的选项如下：HISTFILESIZE=30或HISTSIZE=30。 7．注销时删除命令记录 编辑/etc/skel/.bash_logout文件，增加如下行： rm -f $HOME/.bash_history这样，系统中的所有用户在注销时都会删除其命令记录。 如果只需要针对某个特定用户，如root用户进行设置，则可只在该用户的主目录下修改/$HOME/.bash_history 文件，增加相同的一行即可。