Linux平台下安全防护十大招数[1] PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/270/2021_2022_Linux_E5_B9_B3_E5_8F_c67_270384.htm 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/hda map=/boot/map install=/boot/boot.b time-out=60 #等待1分钟 prompt default=linux password= #口令设置 image=/boot/vmlinuz-2.2.14-12 label=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 -v 2．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.conf 5．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 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