linux系统的安全设定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_linux_E7_B3_BB_E7_BB_c103_644982.htm 1.禁止Ctrl Alt Delete重新启动机器命令 修改/etc/inittab文件，将"ca::ctrlaltdel:/sbin/shutdown -t3 -r now"一行注释掉。 2.禁止在ssh下直接用root登录 编辑/etc/ssh/sshd_config文件 把PermitRootLogin yes前面的“ # ”去掉，把“ yes ”改为“ no ” 有关ssh登录的安全设定还有很多，更详细的ssh安全配配置请参考我的《SSH服务简介》。 3.限制su名单 编辑/etc/pam.d/su文件，加入： auth required /lib/security/$ISA/pam_wheel.so use_uid （不少linux发行版中可能省略pam_wheel.so文件的路径名，为节省篇幅，下文也可能省略路径，但使用绝对路径是不会错的！） 执行下面语句将用户user1加入wheel组： #gpasswd -a user1 wheel 这将使wheel组中的用户才可以执行su命令，root例外。 auth sufficient /lib/security/$ISA/pam_wheel.so trust use_uid 此行使wheel组的用户在执行su时不用输入密码，很方便，但是很危险！！慎用！ 说明：pam_wheel.so是专门用于su的模块，用来阻止非指定组成员执行su，默认为GID 0，可使用选项group＝group_name来指定某个组的用户可以su，或再加上选项deny来“ 取反 ”，即禁止某些组使用su。上文中的“ use_uid ”是系统中就定义好的，具体什么意思/etc/pam.d/su文件里有说明。 4.限制 ssh 使用者名单 编辑/etc/pam.d/sshd 文件，（其中/etc/ssh_users为使用者名单的文件名） auth required pam_listfile.so item=user sense=allow file=/etc/ssh_users onerr=fail 建立/etc/ssh_users文件，执行以下语句： echo user1

gt. /etc/ssh_users 只有/etc/ssh_users文件中列出的用户能用ssh登录主机。 说明： item选项表示指定文件中数据的类型。可用值为：user,group,tty,shell,ruser,rhost。一般用user或group，四个值不常用，有兴趣自己测试。 sense选项表示对指定文件中的数据的访问权限。可用值为deny和allow，不用介绍了吧。 file选项表示存放相关数据的文件位置。 onerr=fail表示本pam模块的认证出现任何错误，则返回拒绝访问。注意：返回值不是“ 访问失败 ”，而且返回“ 拒绝访问 ”不一定能阻止或允许用户登录，还要看第二个字段的参数。本例中使用了required，如果返回值为拒绝访问，则直接阻止用户登录。