LinuxSU命令安全的几点建议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_ti2020/619/2021_2022_LinuxSU_E5_91_BD_c103_619620.htm 首先我们看su在man帮助页中的解释su - run a shell with substitute user and group IDs, 也就是说通过su我们不用提供用户和组名就可以启动一个shell程序. su是一个二进制的可执行文件, 命令所在的文件路径是/bin/su, 下面是通过命令行查询su文件的类型及所在路径: 例一: islab$ which su /bin/su 例二: islab$ file /bin/su /bin/su: setuid ELF 32-bit LSB shared object, Intel 80386, version 1 (SYSV), for GNU/Linux 2.6.9, stripped 例三: islab$ll /bin/su -rwsr-xr-x 1 root root 24060 Jan 10 2007 /bin/su 例三和例二中我们可以看到su是一个setuid程序(setuid位可以使用chmod u s进行设置, 如ls显示su文件所有者属性起用了setuid位), 在这种情况下, su可以获得比其所有者更高的权限, 也就是说su运行的时候, 您的权限会被提升, 将与root的权限等同. 例三中我们可以看到文件的类型是ELF 32-bit LSB shared object(设置了setuid位), 也就是说程序需要libc这样的函数库, 也需要使用了ELF解释器, 并遵守LSB 规范. 问一: 普通用户可以从其linux认证更多详细资料它机器拷贝su命令. 答: 他们可以从其它机器拷贝su命令, 但是他们将不能对su进行正确的权限设置比如chown root和chmod u s等等. 所以拷贝过来su不能够正常工作. 问二: 如何防止普通用户执行su命令. 答: 1). 你可以建立一个专门的组, 只有组成员才能执行su命令 islab# groupadd wheel islab# useradd wheel islab# chown root:mysql /bin/bash islab# chmod 4750 /bin/su 2). 只有root用户才能执行su命令. islab# chmod 4700 /bin/su 3). 通过pam库实现

只有wheel组成员才能执行su命令, 下面例子中增加了zhaoke帐号到wheel组中. islab# groupadd wheel islab# useradd wheel islab# usermod -G wheel zhaoke islab# ll /lib/security/pam_wheel.so -rwxr-xr-x 1 root root 5692 Feb 22 2007 /lib/security/pam_wheel.so islab# vi /etc/pam.d/su 增加下面一行 auth required /lib/security/pam_wheel.so use_uid 然后保存退出su配置文件. 问三: 普通用户虽然不能执行su命令, 但是还有可能通过蛮力攻击获得root的密码 答: 普通用户可以在shell或者ssh方式对root帐户进行蛮力攻击.我们可以考虑使用一些安全工具如pam_abl来对ssh进行保护. pam_abl将能在设定的时间内对错误登陆的帐户进行进行临时封禁. 当然普通用户也可以通过程序漏洞提升权限, 比如缓冲区溢出。