用户口令文件存取权限及安全性 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/233/2021_2022__E7_94_A8_E6_88_B7_EF_B9_91_E5_c67_233935.htm 用户主目录超级用户及增加其他用户 对一般用户而言，硬盘上可以进行写操作的地方可能只有自己的主目录，它位于“ /home/用户名 ”下。/home目录是保存所有用户文件的，其中包括用户设置、程序配置文件、文档、数据、netscape的缓存文件以及用户邮件等等。普通用户仅仅可以在自己的主目录下创建新的子目录来组织您的文件。并且在没有赋予其他用户普通用户权限的情况下，其他用户是无权读写您主目录下的内容的。 除了自己的主目录外，一般用户是可以查找读执行系统内其它目录中的文件的，但是一般情况下，他们不能修改或移动这些文件。 超级用户(也称为“ root ”)是一个具有修改系统中任何一个文件权力的特别账号。在日常工作中，最好不要使用超级用户账号进入系统，因为任何错误操作都可能导致巨大的损失。由于超级用户账号是系统建立后提供的唯一一个账号，因此，您需要建立和使用一个一般用户账号进行日常工作。 超级用户root可以创建新的用户账号，例如下面的命令将建立一个名为joe的新用户。 # adduser joe # passwd joe (键入joe的口令) root可以在不知道用户当前口令的前提下，修改任何一个用户的口令(口令是用一个单向加密算法加密的，并且将加密结果保存在文件/etc/passwd中，而原始口令并不保存)。当您注册时，键入的口令同样被一个单向加密算法计算，并将结果与保存在/etc/passwd中的值进行比较。 Linux采用了将管理员和一般用户分开的策略，这种策略保证了系统的健壮性，

同时也使Linux下的病毒难以编写(用户编写的程序仅对自己的目录有写权限，而与操作系统的其它部分是隔离开的)。 一般情况下，用户在第一次注册时需要立即修改自己的口令。命令如下： $ passwd (current)Unix Password [键入老的口令字] New Unix Password [键入新的口令字] Retype New UNIX password [再一次键入新的口令字] 出于安全考虑，您键入的口令是不会回显在屏幕上的。 口令的安全性 脆弱的口令是系统不安全的最主要原因，下面是一些不安全的口令的例子。1．把单词“ password ”作为口令；2．把自己或他人的姓名或注册名作为口令；3．把公司名，部门名或组名作为口令；4．把生日作为口令；5．把口令写在日历上或计算机旁边；6．使用某个字典里的单词或常用词语；一个好的口令字应该是至少6个字母长，其中包含了字母和数字，并且应该经常修改。 系统管理员可以通过配置程序来设定口令的安全策略。例如，您可以以root身份启动linuxconf实用程序： # linuxconf 在菜单user account ê policies ê password &amp. account policies下配置口令。 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