Linux操作系统口令文件安全问题详细解析 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/471/2021_2022_Linux_E6_93_8D_E4_BD_c67_471288.htm 几乎所有的类Unix操作系统的口令文件的格式都雷同，Linux 亦不例外。口令安全是Linux 操作系统的传统安全问题之一。 传统口令与影子口令 /etc/passwd 是存放用户的基本信息的口令文件。该口令文件的每一行都包含由6 个冒号分隔的7 个域：&amp.nbsp ；username： passwd ： uid： gid： comments： directory： shell 以上从左到右7 个域分别叙述如下： username：是用户登陆使用的名字。 passwd：是口令密文域。密文是加密过的口令。如果口令经过shadow则口令密文域只显示一个x，通常，口令都应该经过shadow以确保安全。如果口令密文域显示为*，则表明该用户名有效但不能登陆。如果口令密文域为空则表明该用户登陆不需要口令。 uid ：系统用于唯一标识用户名的数字，uid 系统是这样分配的： 0 超级用户 1 ～10守护程序和伪用户 11～99系统保留用户 100 ～正常用户 gid ：表示用户所在默认组号。由/etc/group文件决定。 comments：描述用户的个人信息。 directory ：定义用户的初始工作目录。 shell ：就是指定用户登陆到系统后启动的外壳程序。 表1 列出了系统在安装过程中创建的标准用户，表中的内容和/etc/passwd文件的描述是一致的。 表2 列出系统安装过程中创建的标准用户组，和/etc/group文件是一致的： Linux 使用不可逆的加密算法如DES 来加密口令，由于加密算法是不可逆的，所以从密文是得不到明文的。但问题在于，/etc/passwd 文件是全局可读的，加密的算法是公开的，如果有恶意用户

取得了/etc/passwd 文件，他就可以穷举所有可能的明文通过相同的算法计算出密文进行比较，直到相同，于是他就破解了口令。因此，针对这种安全问题，Linux/Unix广泛采用了“ shadow（影子）”机制，将加密的口令转移到 /etc/shadow 文件里，该文件只为root超级用户可读，而同时/etc/passwd 文件的密文域显示为一个x，从而最大限度减少密文泄露的机会。 /etc/shadow 文件的每行是8 个冒号分割的9 个域，格式如下： username： passwd ： lastchg： min： max： warn ： inactive ： expire： flag 其中： lastchg ：表示从1970年1 月1 日起到上次修改口令所经过的天数。 min ：表示两次修改口令之间至少经过的天数。 max ：表示口令还会有效的最大天数，如果是99999 则表示永不过期。 warn：表示口令失效前多少天内系统向用户发出警告。 inactive：表示禁止登陆前用户名还有效的天数。 expire：表示用户被禁止登陆的时间。0 flag ：无意义，未使用。 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