第26章　Linux系统的用户安全性

本章从用户角度讨论Linux系统安全，阐述口令、文件保护、目录保护、与用户程序有关的某些特殊特性和使用crypt命令加密，并给出一些重要的安全忠告，以帮助用户保护自己的帐户安全。

26.1　口令安全

Linux系统中的/etc/passwd文件含有全部系统需要知道的关于每个用户的信息（加密后的口令也可能存于/etc/shadow文件中）。/etc/passwd中包含用户的登录名、经过加密的口令、用户号、用户组号、用户注释、用户主目录和用户所用的外壳程序。其中用户号（ UID）和用户组号（GID）用于Linux系统唯一地标识用户和同组用户及用户的访问权限。 /etc/passwd中存放的加密的口令用于与用户登录时输入的口令经计算后相比较，符合则允许登录，否则拒绝用户登录。用户可用passwd命令修改自己的口令，不能直接修改/etc/passwd中的口令部分。

一个好的口令应当至少有6个字符长，不要取用个人信息（如生日、名字、反向拼写的登录名、房间中可见的东西），普通的英语单词也不好（因为可用字典攻击法），口令中最好有一些非字母（如数字、标点符号、控制字符等），还要好记一些，不能写在纸上或计算机中的文件中，选择口令的一个好方法是将两个不相关的词用一个数字或控制字符相连，并截断为 8个字符。当然，如果你能记住8位乱码自然更好。

不应使用同一个口令在不同机器中使用，特别是在不同级别的用户上使用同一口令，会引起全盘崩溃。用户应定期改变口令，至少 6个月要改变一次，系统管理员可以强制用户定期做口令修改。为防止他人窃取口令，在输入口令时应确保无人在身边。

26.2　文件许可权

文件属性决定了文件的被访问权限，即谁能存取或执行该文件。用 ls -l可以列出详细的文件信息，如：

-rwxrwxrwx 1 pat cs440 70 Jul 28 21：12 zombin

包括了文件许可、文件联结数、文件所有者名、文件相关组名、文件长度、上次存取日期和文件名。

其中文件许可分为四部分：

-：表示文件类型。

第一个rwx：表示文件属主的访问权限。

第二个rwx：表示文件同组用户的访问权限。

第三个rwx：表示其他用户的访问权限。

若某种许可被限制则相应的字母换为-。

在许可权限的执行许可位置上，可能是其他字母， s、S、t、T。s和S可出现在所有者和同组用户许可模式位置上，与特殊的许可有关，后面将要讨论， t和T可出现在其他用户的许可模式位置上，与“ 粘贴位 ”有关而与安全无关。小写字母（ x，s，t）表示执行许可为允许，负号或大写字母（-，S或T）表示执行许可为不允许。改变许可方式可使用 chmod命令，并以新

许可方式和该文件名为参数。新许可方式以3位8进制数给出，r为4，w为2，x为1。如rwxr-xr--为754。chmod也有其他方式的参数可直接对某组参数修改，在此不再多说，详见 Linux系统的联机帮助。

文件许可权可用于防止偶然性地重写或删除一个重要文件（即使是属主自己）！

改变文件的属主和组名可用chown和chgrp，但修改后原属主和组员就无法修改回来了。

26.3 目录许可

在Linux系统中，目录也是一个文件，用 ls -l列出时，目录文件的属性前面带一个 d，目录许可也类似于文件许可，用ls列目录要有读许可，在目录中增删文件要有写许可，进入目录或将该目录作路径分量时要有执行许可，故要使用任一个文件，必须有该文件及找到该文件的路径上所有目录分量的相应许可。仅当要打开一个文件时，文件的许可才开始起作用，而 rm、mv只要有目录的搜索和写许可，不需文件的许可，这一点应注意。

26.4 umask命令

umask设置用户文件和目录的文件创建缺省屏蔽值，若将此命令放入 .profile文件，就可控制该用户后续所建文件的存取许可。 umask命令与chmod命令的作用正好相反，它告诉系统在创建文件时不给予什么存取许可。

26.5 设置用户ID和同组用户ID许可

用户ID许可（SUID）设置和同组用户ID许可（SGID）可给予可执行的目标文件（只有可执行文件才有意义）当一个进程执行时就被赋于 4个编号，以标识该进程隶属于谁，分别为实际和有效的UID，实际和有效的GID。有效的UID和GID一般和实际的UID和GID相同，有效的UID和GID用于系统确定该进程对于文件的存取许可。而设置可执行文件的 SUID许可将改变上述情况，当设置了SUID时，进程的有效UID为该可执行文件的所有者的有效UID，而不是执行该程序的用户的有效UID，因此，由该程序创建的都有与该程序所有者相同的存取许可。这样，程序的所有者将可通过程序的控制在有限的范围内向用户发表不允许被公众访问的信息。同样，SGID是设置有效GID。

用chmod u+s 文件名和chmod u-s文件名来设置和取消SUID设置。用chmod g+s 文件名和chmod g-s文件名来设置和取消 SGID设置。当文件设置了 SUID和SGID后，chown和chgrp命令将全部取消这些许可。

26.6 cp mv ln和cpio命令

cp拷贝文件时，若目的文件不存在，则将同时拷贝源文件的存取许可，包括 SUID和SGID许可。新拷贝的文件属拷贝的用户所有，故拷贝他人的文件时应小心，不要被其他用户的SUID程序破坏自己的文件安全。mv移文件时，新移的文件存取许可与原文件相同， mv仅改变文件名。只要用户有目录的写和搜索许可，就可移走该目录中某人的 SUID程序且不改变其存取许可。若目录许可设置不正确，则用户的 SUID程序可被移到一个他不能修改和删除的目录中，将出现安全漏洞。

ln为现有文件建立一个链，即建立一个引用同一文件的新名字。如目的文件已经存在，则该文件被删除而代之以新的链，或存在的目的文件不允许用户写它，则请求用户确认是否删除

该文件，只允许在同一文件系统内建链。若要删除一个 SUID文件，就要确认文件的链接数，只有一个链才能确保该文件被删除。若 SUID文件已有多个链，一种方法是改变其存取许可方式，将同时修改所有链的存取许可；另一种方法以 chmod 000 文件名，不仅取消了文件的SUID和SGID许可，而且也取消了文件的全部链。要想找到谁与自己的 SUID程序建立了链，不要立刻删除该程序，系统管理员可用ncheck命令找到该程序的其他链。

cpio命令用于将目录结构拷贝到一个普通文件中，然后可再用 cpio命令将该普通文件转成目录结构。用-i选项时，cpio从标准输入设备读文件和目录名表，并将其内容按档案格式拷贝到标准输出设备，使用-o选项时，cpio从标准输入设备读取事先已建好的档案，重建目录结构。cpio命令常用以下命令做一完整的目录系统档案：

```
find fromdir -print|cpio -o > archive
```

根据档案文件重建一个目录结构命令为：

```
cpio -id < archive
```

cpio的安全约定如下：

1) 档案文件存放每个文件的信息，包括文件所有者、小组用户、最后修改时间、最后存取时间、文件存取许可方式。

- 根据档案建立的文件保持存放于档案中的存取许可方式。
- 从档案中提取的每个文件的所有者和小组用户设置给运行 cpio -i命令的用户，而不是设置给档案中指出的所有者和小组用户。
- 当运行cpio -i命令的用户是root时，被建立的文件的所有者和小组用户是档案文件所指出的。
- 档案中的SUID/SGID文件被重建时，保持SUID和SGID许可，如果重建文件的用户不是root，SUID/SGID许可是档案文件指出的用户/小组的许可。

2) 现存文件与cpio档案中的文件同名时，若现存文件比档案中的文件更新，这些文件将不被重写。

3) 如果用修改选项U，则同名的现存的文件将被重写。可能会发生一件很奇怪的事：如被重写的文件原与另一个文件建了链，文件被重写后链并不断开，换言之，该文件的链将保持，因此，该文件的所有链实际指向从档案中提取出来的文件，运行 cpio无条件地重写现存文件以及改变链的指向。

4) cpio档案中可包含的全路径名或父目录名给出的文件。

26.7 su和newgrp命令

26.7.1 su命令

可不必注销帐户而将另一用户又登录进入系统，作为另一用户工作。它将启动一新的外壳并将有效和实际的UID和GID设置给另一用户。因此必须严格将root口令保密。

26.7.2 newgrp命令

与su相似，用于修改当前所处的组名。

26.8 文件加密

crypt命令可提供给用户以加密文件，使用一个关键词将标准输入的信息编码为不可读的杂

乱字符串，送到标准输出设备。再次使用此命令，用同一关键词作用于加密后的文件，可恢复文件内容。

一般来说，在文件加密后，应删除原始文件，只留下加密后的版本，且不能忘记加密关键词。

在vi中一般都有加密功能，用vi -x命令可编辑加密后的文件。加密关键词的选取规则与口令的选取规则相同。

由于crypt程序可能被做成特洛伊木马，故不宜用口令做为关键词。最好在加密前用 pack或compress命令对文件进行压缩后再加密。

26.9 其他安全问题

26.9.1 用户的.profile文件

由于用户的HOME目录下的.profile文件在用户登录时就被执行。若该文件对其他人是可写的 则系统的任何用户都能修改此文件，使其按自己的要求工作。这样可能使得其他用户具有该用户相同的权限。

26.9.2 ls -a

此命令用于列出当前目录中的全部文件，包括文件名以“ .”开头的文件，查看所有文件的存取许可方式和文件所有者，任何不属于自己的但存在于自己的目录中的文件都应怀疑和追究。

26.9.3 . exrc文件

为编辑程序的初始化文件，使用编辑文件后，首先查找 $HOME/.exrc文件和./.exrc文件，若该文件是在$HOME目录中找到，则可像.profile一样控制它的存取方式，若在一个自己不能控制的目录中运行编辑程序，则可能运行其他人的.exrc文件，或许该.exrc文件存在那里正是为了损害他人的文件安全。为了保证所编辑文件的安全，最好不要在不属于自己或其他人可写的目录中运行任何编辑程序。

26.9.4 暂存文件和目录

在Linux系统中暂存目录为/tmp和/usr/tmp，对于程序员和许多系统命令都使用它们，如果用这些目录存放暂存文件，别的用户可能会破坏这些文件。使用暂存文件最好将文件屏蔽值定义为007，但最保险的方法是建立自己的暂存文件和目录： $HOME/tmp，不要将重要文件存放于公共的暂存目录。

26.9.5 UUCP和其他网络

UUCP命令用于将文件从一个Linux系统传送到另一个Linux系统，通过UUCP传送的文件通常存于/usr/spool/uucppublic/login目录，login是用户的登录名，该目录存取许可为777，通过网络传输并存放于此目录的文件属于UUCP所有，文件存取许可为666和777，用户应当将通过UUCP传送的文件加密，并尽快移到自己的目录中。其他网络将文件传送到用户 HOME目录下的rjc目录中。该目录应对其他人是可写可搜索的，但不必是可读的，因而用户的 rjc目录的存

取许可方式应为733，允许程序在其中建立文件。同样，传送的文件也应加密并尽快移到自己的目录中。

26.9.6 特洛伊木马

在Linux系统安全中，用特洛伊木马来代表一种程序，这种程序在完成某种具有明显意图的功能时，还破坏用户的安全。如果 PATH设置为先搜索系统目录，则受特洛伊木马的攻击会大大减少。如模拟的crypt程序。

26.9.7 诱骗

类似于特洛伊木马，模拟一些东西使用户泄漏一些信息，不同的是，它由某人执行，等待无警觉的用户来上当。如模拟的login。

26.9.8 计算机病毒

计算机病毒是通过把其他程序变成病毒从而传染系统的，可以迅速地扩散，特别是系统管理员的粗心大意，作为 root运行一个被感染的程序时。实验表明，一个病毒可在一个小时内（平均少于30分钟）取得root权限。

26.9.9 要离开自己已登录的终端

除非能对终端上锁，否则一定要注销帐户。

26.9.10 智能终端

由于智能终端有send和enter换码序列，告诉终端把当前行送给系统，就像是用户敲入的一样。这是一种危险的能力，其他人可用write命令发送信息给本用户终端，如果信息中含有以下的换码序列：

- 移光标到新行（换行）。
- 在屏幕上显示“ rm -r * ”。
- 将该行送给系统。

其结果大家可以想象。

禁止其他用户发送信息的方法是使用mesg命令，mesg n不允许其他用户发信息，mesg y允许其他用户发信息。即使如此仍是有换码序列的问题存在，任何一个用户用 mail命令发送同样一组换码序列，不同的要用 !rm -r *替换rm -r *。mail将以!开头的行解释为一条外壳命令，启动外壳，由外壳解释该行的其他部分，这被称为外壳换码。为避免 mail命令发送换码序列到自己的终端，可建立一个过滤程序，在读mail文件之前先运行过滤程序，对mail文件进行处理：

```
myname="$LOGNAME";
tr -d[\001-\007][-\013-\037]</usr/mail/$myname>>$HOME/mailbox;
> /usr/mail/$myname;
mail -f $HOME/mailbox
```

其中tr将标准输入的字符转换手写到标准输出中。这只是一个简单的思路，从原则上来说，此程序应为一个C程序，以避免破坏正发送到的文件，可用锁文件方式实现。

26.9.11 断开与系统的连接

用户应在看到系统确认登录注销后再离开，以免在用户未注销时由他人潜入。

26.9.12 cu命令

该命令使用户能从一个Linux系统登录到另一个Linux系统，此时，在远地系统中注销用户后还必须输入“ ~ ”后回车，以断开cu和远地系统的连接。

cu还有两个安全问题：

- 如果本机安全性弱于远地机，不提倡用 cu去登录远地机，以免由于本地机的不安全而影响较安全的远地机。
- 由于cu的老版本处理“ ~ ”的方法不完善，从安全性强的系统调用安全性弱的系统时，会使弱系统的用户使用强系统用户的 cu传送强系统的/etc/passwd文件，除非确定正在使用的cu是正确版本，否则不要调用弱系统。

26.10 保持帐户安全的要点

1）保持口令的安全。

- 不要将口令写下来。
- 不要将口令存于终端功能键或调制解调器的字符串存储器中。
- 不要选取显而易见的信息作口令。
- 不要让别人知道。
- 不要交替使用两个口令。
- 不要在不同系统上使用同一个口令。
- 不要让人看见自己在输入口令。

2）不要让自己的文件或目录可被他人写。

- 如果不信任本组用户，umask设置为022。
- 确保自己的.profile除自己外对他人都不可读写。
- 暂存目录最好不用于存放重要文件。
- 确保HOME目录对任何人不可写。
- uucp传输的文件应加密，并尽快私人化。

3) 若不想要其他用户读自己的文件或目录，就要使自己的文件和目录不允许任何人读。

- umask设置为006/007。
- 若不允许同组用户存取自己的文件和目录，umask设置为077。
- 暂存文件按当前umask设置，存放重要数据到暂存文件的程序，就被写成能确保暂存文件对其他用户不可读。
- 确保HOME目录对每个用户不可读。

4) 不要写SUID/SGID程序。

5) 小心地拷贝和移文件。

- cp拷贝文件时，记住目的文件的许可方式将和文件相同，包括 SUID/SGID许可在内，如目的文件已存在，则目的文件的存取许可和所有者均不变。
- mv移文件时，记住目的文件的许可方式将和文件相同，包括 SUID/SGID许可在内，若在同一个文件系统内移文件，目的文件的所有者和小组都不变，否则，目的文件的所有者和小组将设置成本用户的有效UID和GID。
- 小心使用cpio命令，它能复盖不在本用户当前目录结构中的文件，可用 t选项首先列出要被拷贝的文件。

6) 删除一个SUID/SGID程序时，先检查该程序的链接数，如有多个链，则将存取许可方式改为000，然后再删除该程序，或先写空该程序再删除，也可将该程序的 i结点号给系统管理员去查找其他链。

7) 用crypt加密不愿让任何用户（包括超级用户）看的文件。

• 不要将关键词做为命令变量。

• 用ed -x或vi -x编辑加密文件。

8) 除了信任的用户外，不要运行其他用户的程序。

9) 在自己的PATH中，将系统目录放在前面。

10）不要离开自己登录的终端。

11) 若有智能终端，当心来自其他用户，包括 write命令、mail命令和其他用户文件的信息中有换码序列。

12) 用Ctrl+D或Exit退出后，在断开与系统的联接前等待看到 login：提示。

13) 注意cu版本。

• 不要用cu调用安全性更强的系统。

• 除非确信cu不会被诱骗去发送文件，否则不要用 cu调用安全性更弱的系统。