第8章　建立用户帐户

如果你需要下列问题的一个快速解决方案	请查阅节号
添加一个新用户	8.2.1
添加或者修改一个口令字	8.2.2
通过linuxconf程序添加一个新用户	8.2.3
查看关于新用户的缺省设置	8.2.4
选择关于新用户的缺省设置	8.2.5
改变关于新用户的缺省设置	8.2.6
修改现有用户的信息	8.2.7
通过linuxconf程序修改现有用户的信息	8.2.8
安装shadow隐藏口令字软件包	8.2.9
转换用户系统使用shadow隐藏口令字	8.2.10
转换用户系统不再使用shadow隐藏口令字	8.2.11
查找缺省的用户配置文件	8.2.12
查找容易被破译的口令字	8.2.13
冻结一个用户	8.2.14
通过linuxconf程序冻结一个用户	8.2.15
删除一个用户	8.2.16
通过linuxconf程序删除一个用户	8.2.17
检查系统的易受攻击性	8.2.18
修改源代码使程序能够运行在使用shadow隐藏口令字功能的系统中	8.2.19
打开linuxconf程序	8.2.20

8.1　概述

不管你的Linux机器是通过网络为许多用户提供服务，还是用做一台个人桌面电脑，建立彼此分开的用户帐户都不失为一个明智之举。这样做的一个基本原因是 root帐户是一个威力极大的工具，但也仅是一个工具而已。每个人都有可能不小心犯错误。作为一个普通用户可能只是很小的一场混乱；而作为根用户犯一个大错误就有可能让你后悔当初没有及时地建立好备份。

窍门　下面是一些关于根用户和因特网应该掌握的知识：许多因特网服务在处理根用户的情况时都有一些特殊的考虑。举例来说，在缺省的情况下你是无法作为根用户使用Telnet功能进入一台Linux机器的。如果允许这样做，就会被认为是一个相当大的安全漏洞，因为某个人只要能够猜出根用户口令字（password）就可以对整个系统进行存取。如果对之要求至少需要先进入某个普通用户帐户，情况就会好得多，因为这样会使攻击进入系统的过程时间长一些，而你也就更容易发现它。

以根用户身份进入IRC（网上聊天）也有可能会遭到许多频道的拒绝或禁止。根用户权限允许用户通过某个UNIX机器运行一系列攻击性的程序功能，因此许多IRC频道不管你是否故意，干脆就不找那份麻烦。

以根用户身份发送电子邮件或者在新闻组中发布消息一般也不受欢迎，除非你正在讨论的是一个系统管理员关心的问题。但是就是在这种情况下，更多考虑的应该是有无必要如此炫耀，而不是说因为对系统有了更好的理解而可以毫无必要地充当根用户。

在第21章中有关于系统安全性方面更详细的议论，但是从下面开始是对口令字问题的简单介绍。

8.1.1 口令字

帐户口令字是计算机系统与想从其中盗取信息和资源的那些人之间一道重要的屏障，也可以降低灾难的损失。如果用户的Linux机器可以通过因特网或者调制解调器被访问的话，就必须认真地设置好口令字。对于系统管理员的根用户口令字和用户的因特网服务来说，更是如此。

窍门 一个好的口令字是不会使用字典中的单词构成的。它将包括大小写混用的字母、数字以及其他允许的字符。一个安全的口令字其长度一般要超过8个字符。

虽然你不能够完全控制用户选择什么样的口令字，但却可以教他们怎样做得更好。你还可以时不时地使用工具软件查找出哪些口令字选择得不好（参见下面的窍门）。然后你可以分别通知各个用户，让他们修改口令字，并指导他们怎样才能更安全地进行选择。

窍门 一个差的口令字常常是使用字典中的单词构成的，或者少于8个字符。另外一些比较差的口令字是那些熟悉该用户的人容易猜出来得东西，比如生日、宠物的名字或者其他类似的东西。

是否需要对口令字进行检查取决于系统的易受攻击性（请阅读本章后面 8.2.18节的内容）、系统的知名度以及希望达到的安全强度。当你为某些人分配了一个新口令字（临时性的或者其他情况），或者当某个用户修改了他或她自己的口令字的时候， passwd程序确实可以指出哪些明显是比较差的口令字。但是，如果这个用户比较顽固，他或她也完全可以忽视警告，继续使用那个比较差的口令字。请记住，使用可以被 passwd程序轻易检查出来的口令字会对系统安全性造成潜在的危害。

窍门 在命令行和GUI状态下都有管理用户方面的工具软件。具体使用哪一类工具软件只是个个人爱好问题。linuxconf程序通常是使用最多的选择。虽然本章的讨论集中在命令行模式下的工具软件，但也会简单地涉及到怎样在linuxconf程序中完成这类任务。

shadow口令字

保存在/etc/passwd文件中的口令字是经过加密编码的，因此不像平白的文本那样容易被读出来。这就意味着你并不能通过查看这个文件来找出别人的口令字，这也是为加强系统安全性迈出的第一步。但是这种加密编码的方法并不是很保险。一旦它们从这个文件中被获取，解开口令字的加密编码并不是很困难的事。

因为/etc/passwd文件对任何人都是可读的。一个侵入者需要做的只是在设法闯入任何一个用户帐户之后 —— 通过使用黑客程序处理某个字典单词集破译了口令字、通过掌握了某个用户设置口令字的习惯或者通过在第 21章中介绍的其他方法 —— 就可以简单地拷贝一份/etc/passwd文件并把其中的加密编码解开。这个漏洞看起来好像只需要修改该文件的存取权限就可以很容易地弥补上，但是这往往并不起作用。因为在 /etc/passwd文件中包含着重要的数据，比如用户信息、分组信息、还有 shell信息等等 —— 而又有太多的程序需要对这个文件

进行存取，因此你很难把它设置为只对根用户可读。

解决这个问题最常用的一个办法是安装shadow（隐藏）口令字软件。这个软件将把全部口令字都转移到只对根用户可读的某个文件中，这样就避免了某些人简单地通过盗取 /etc/passwd 文件而可能造成的损失。但是，正如你也能想到的，把所有的口令字都转移到一个新文件中有可能引发潜在的问题，因为有一些程序和服务需要对这个文件进行存取。如果用户可以接触到源代码（请阅读8.2.19节中的内容），或者程序的自身设置中有一个项目可以让用户通知它系统使用了shadow口令字功能，这就不会构成太大的问题。但是在下面的一些情况中是不能使用shadow口令字功能的：

- Linux机器所在LAN需要通过NIS与网络中其他的机器交换用户名和口令字。
- Linux机器被当做通过NFS、NIS或者其他方法验证用户身份的终端服务器。
- 用户必须使用的某些软件要求验证用户身份，但是又没有办法获得 shadow口令字专用的版本，也没有办法取得源代码。

请阅读8.2.10节的内容设置机器使用shadow口令字功能。在本章中还介绍了如何去掉这个功能（请阅读8.2.11节的内容），以免此功能影响到用户需要完成的其他工作。

8.1.2 编写添加用户命令脚本程序

许多系统管理员发现在建立新用户时，他们经常是在重复着相同的操作。为了减少这些繁琐工作，他们中的许多人选择了建立一个 shell命令脚本程序的方法把这一系列工作纳入到一个比较顺畅的过程中去。

在添加用户的时候，请随时记下你必须做的工作。你的安装设置越复杂，这个时候需要投入得就越多。比如说，你可能需要为他们建立一个 Web目录或者FTP目录；也许还需要修改他们的PATH语句以便把他们通常需要存取的文件路径包括进去。

一旦把这些数据都准备好了，就可以开始编写命令脚本程序了。编写 shell命令脚本程序的详细讨论请阅读第18章。

8.2 快速解决方案

8.2.1 添加一个新用户

有两种不同的命令可以用来添加用户： adduser和useradd命令。两个命令工作的方式是完全相同的。请输入“ adduser username ”开始添加一个新用户。

窍门 你可能会发现赋给新用户的缺省值并不是你想使用的。如果情况确实如此，请阅读8.2.4节的内容。

比如说，如果想添加新用户帐户 mary，输入“ useradd mary ”命令即可。

接下来还需要为这个新用户设置一个口令字。具体做法请阅读 8.2.2节的内容。

窍门 你必须以根用户登录进入系统才能建立新用户。

8.2.2 添加或者修改一个口令字

root帐户拥有为其他的用户添加或者修改口令字的权限。两种操作都可以使用同一个

“ passwd username ”命令来完成。

窍门 你也可以通过linuxconf程序改变口令字。请阅读8.2.2节的内容。只要你单击了想对其进行修改的用户，就可以再单击Passwd按钮修改那个用户的口令字。

比如说，如果想修改用户 birdy的口令字，输入“ passwd birdy ”即可。

窍门 即使你当前登录进入的是一个非root帐户，也可以通过passwd命令改变这个帐户的口令字。但是这个时候不再需要包括用户名了，而只要输入“ passwd ”即可。

8.2.3 通过linuxconf程序添加一个新用户

请按照下面的方法通过 linuxconf程序添加一个新用户：

1) 打开linuxconf程序（请阅读8.2.20节中关于如何操作的介绍）。

2) 沿着目录树前进到Users Accounts（用户帐户）|Normal（一般设置）子菜单。

3) 单击Users accounts（用户帐户）选项。屏幕上将出现如图 8-1所示的Users Accounts窗口。

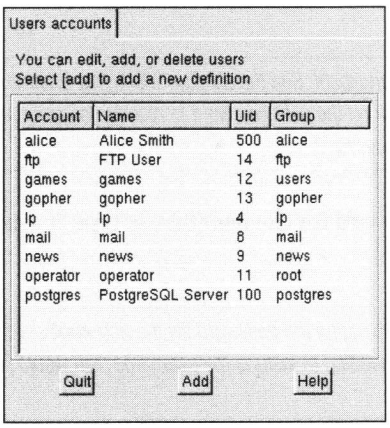

图8-1 linuxconf程序的User Account（用户帐户）窗口

4) 单击Add（添加）按钮。屏幕上将出现如图 8-2所示的User account creation（建立用户帐户）窗口，它的Base Info（基本信息）标签出现在窗口最上面。

5) 在文本输入框内填写有关的数据。你必须填写的一个数据项是帐户的名称。如有必要，请单击Privileges（优先权）标签并选择适当的选项。

6) 单击Accept（接受）按钮。屏幕上将出现如图 8-3所示的Changing password（修改口令字）窗口。

7) 输入用户的口令字。

8) 单击Accept（接受）按钮。如果口令字检查程序拒绝接受你刚才设置的口令字，屏幕上将会出现一个对话框，通知你刚才选择的口令字不好。单击 OK按钮。

9) 根据提示再次输入口令字。如果你还是决定使用刚才程序认为不好的口令字，就再把它输入一次。但是，如果系统有的时候还需要连接到因特网上的话，最好还是把口令字改为一个更加安全的。

10) 单击Accept（接受）按钮。你将返回到Users Accounts（用户帐户）窗口。

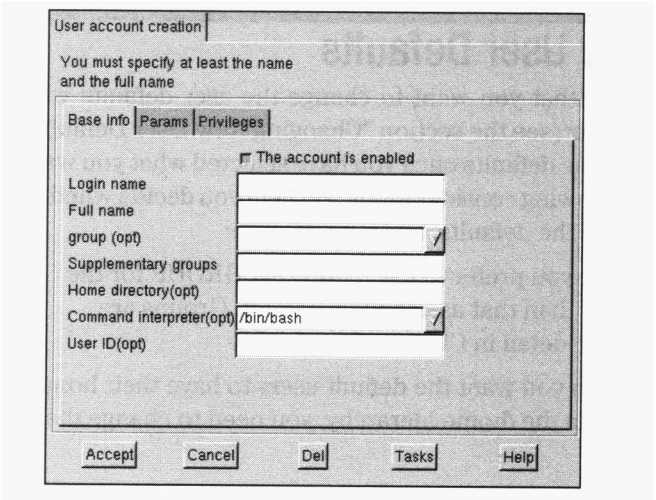

图8-2 linuxconf程序的User account creation（建立用户帐户）窗口

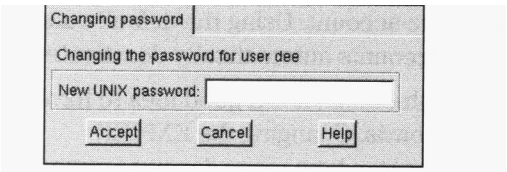

图8-3 linuxconf程序的Changing Password（修改口令字）窗口

8.2.4 查看关于新用户的缺省设置

如果想查看关于新用户的缺省设置，需要使用adduaer或者useradd命令的-D参数，如下所示：

```
useradd -D
```

8.2.5 选择关于新用户的缺省设置

你可能会发现需要使用 adduaer或者useradd命令来修改关于新用户的缺省设置（一旦选定需要修改哪些个数据，请阅读 8.2.6节中关于具体操作步骤的介绍内容）。下面的内容将帮助你决定是否需要对其缺省值进行修改；如果要修改，改些什么：

- 你可能会发现自己更喜欢把那些普通的新用户分配到缺省设置值以外的另一个分组（GROUP）。分组的概念在第5章中有详细的介绍。
- 如果因为某些原因希望把新用户的用户目录设置在 /home目录树以外的位置，就需要修改HOME（用户目录）项目的设置值。
- 当出现用户不修改他们过期失效口令字情况的时候，你可能会想要把这类用户的帐户冻结（inactive）起来。这就需要修改INACTIVE（冻结）项目的设置值。办法是输入一个以按天数计算的数字。这个数字表示在用户口令字失效之后、彻底关闭该帐户之前系统将要等待的时间。如果使用了缺省的数值 0天，就表示你并不希望自动冻结那些帐户。
- 如果你的系统比较容易受到攻击，定期使原来的口令字失效是一个好办法。请把EXPIRE（失效）项目修改为一个数字，这样就可以通知系统每循环经过多少天，原来

的口令字就将失效；而在此之前，系统必须强迫用户修改他们的口令字。

- 缺省的SHELL项目设置值一般都是/bin/bash。如果想改变这一点，就必须输入新的缺省shell的完整路径名。
- 许多聪明的系统管理员通过使用框架（ skeleton）目录来定制新用户的目录。这个框架目录中包括着那些准备安排到每一个新建帐户的目录中去的文件。如果你想把框架目录设置为缺省值（通常是/etc/skel目录）以外的某个位置，就需要把SKEL（框架目录）项目的设置值修改为新的框架目录的完整路径名。

8.2.6 改变关于新用户的缺省设置

在建立新用户的时候，如果需要改变关于新用户的缺省设置，可以使用 adduser和useradd命令的对应参数。表8-1中列出了用来修改缺省用户设置值的各个参数（关于这些设置值的详细介绍，请阅读8.2.5节的内容）。

表8-1 使用adduser和useradd命令修改新用户缺省设置值参数

用户设置值	参 数	数 据 格 式
GROUP	-g	来自/etc/group文件的分组编码
HOME	-d	该帐户上一级用户目录的完整路径（比如：/home）
INACTIVE	-f	天数
EXPIRE	-e	天数
SHELL	-s	到shell的完整路径
SKEL	-k	到框架文件的完整路径

举例来说，如果想实现下面几个设置：

- 设置口令字失效期为90天。
- 如果失效口令字在30天内没有修改，就冻结该帐户。
- 把缺省的shell改为/bin/ksh。

就需要使用“ adduser -e90 -f30 -s/bin/ksh ”命令。

8.2.7 修改现有用户的信息

使用usermod命令可以修改现有用户的信息，加上必要的参数指定需要修改的项目。表 8-2列出了可以使用的参数。

警告 如果你使用了G参数，那么任何没有使用它或者g参数列出的分组将从用户分组定义中被删除。

表8-2 usermod命令中用来修改用户信息的参数

参 数	名 称	说 明
c	说明信息	用在finger文件中的说明信息。这个数据域最好是用chfn命令来修改
d	用户目录	为这个用户输入一个新的用户目录位置，新位置将自动被建立。如果在d参数后加上一个m参数，那么用户原来的用户目录中的东西将会被转移到新的目录中去
e	失效日期	如果想把用户帐户的失效日期设置为某个特定的日子，请按照MM/DD/YY的格式输入该日期

(续)

参　数	名　称	说　明
f	冻结期	口令字失效之后冻结该帐户之前需要等待的天数。只有在该用户没有修改其口令字的时候这个选项才被激活。如果不想使用这个选项，请输入数值-1（缺省值）
g	原始分组	分配给用户的分组名称或者编号。这个分组必须是当前存在的
G	分组	使用这个参数可以给该用户分配额外的分组。如果需要分配不止一个的话，请使用逗号而不是空格来分隔它们。比如说，如果想把wheel、root和admin等几个分组分配给该用户，需要输入“whell,root,admin”
l	登录名	使用这个参数可以修改用户的登录名。这么做的时候用户的用户目录不会自动改变。如果用户已经登录进入了系统，就不能修改用户的登录名
s	shell	如果用户要求使用另外一个登录shell，使用这个参数修改它。需要使用新shell的名称
u	UID	改变用户ID的数值。除非了解这样做的后果和系统上当前可用的ID数值范围，否则不要这样做

举例来说，如果用户chris要求把他的登录名修改为c.adams，就需要以root身登录进入系统再输入“usermod -d /home/c.adams -m -l c.adams.chris”命令。

8.2.8 通过linuxconf程序修改现有用户的信息

请按照下面的方法通过linuxconf程序修改现有用户的设置信息：

1) 打开linuxconf程序（请阅读8.2.20节中的内容）。

2) 沿着目录树前进到Users Accounts（用户帐户）|Normal（一般设置）子菜单。

3) 单击Users accounts（用户帐户）选项。屏幕上将出现如图 8-1所示的Users Accounts（用户帐户）窗口。

4) 沿着用户清单前进到需要修改的帐户处。

5) 单击需要修改的项目。屏幕上将出现如图8-4所示的User information（用户信息）窗口。

6) 根据需要修改有关的项目。

7) 单击Accept（接受）按钮。

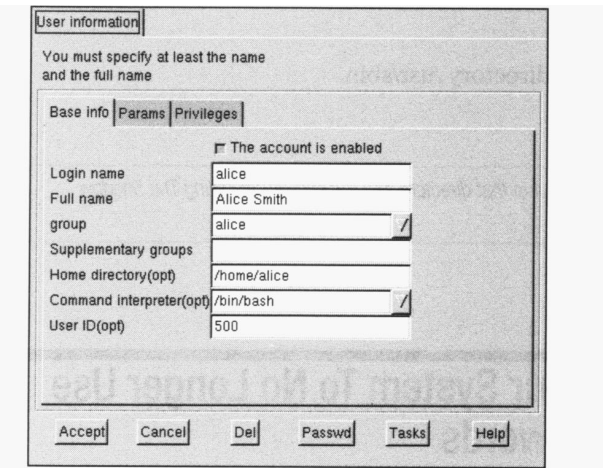

图8-4　linuxconf程序的“User Information”（用户信息）窗口

8.2.9 安装shadow口令字软件包

如果想把需要改为使用 shadow（隐藏）口令字，但是系统上还没有安装它们的话，必须先安装shadow口令字功能。如果正在使用的是 Red Hat发行版本，可以在Red Hat发行版本CD-ROM光盘中/RedHat/RPMS目录下的shadow-utils软件包中找到它们。软件包 shadow-misc保存在Caldera发行版本CD-ROM光盘的/Packages/RPMS中。请阅读第15章中关于如何安装 RPMS软件包的详细内容。

注意 shadow隐藏口令字在Red Hat和Caldera两种发行版本中都是缺省安装的。但是，在定制安装过程中就有可能在安装过程中关闭了它们。

相关解决方案	请查阅节号
安装一个RPM软件包	15.2.1
查看一个RPM软件包中都有哪些文件	15.2.1
进入GUI	6.2.15
挂装到文件系统上	9.2.2

8.2.10 转换用户系统使用shadow口令字

如果还没有配置系统使用 shadow口令字，请按照下面的方法进行设置：

1) 以根用户身份登录进入系统。
2) 把路径切换到/usr/sbin目录。
3) 输入“ pwconv ”命令。

注意 如果该命令没有在这个目录中，请阅读8.2.9节的内容。

8.2.11 转换用户系统不再使用shadow口令字

请按照下面的方法从系统中删除口令字隐藏功能：

1) 以根用户身份登录进入系统。
2) 把路径切换到/usr/sbin目录。
3) 输入“ pwconv ”命令。
4) 然后删除shadow口令字功能。 Red Hat和Caldera两种发行版本中的软件包名称都已经分别列在8.2.9节中。

8.2.12 查找缺省的用户配置文件

普通用户的配置文件保存在 /etc/profile文件中。分配给/etc/profile文件的shell决定了你所做的修改以什么格式在其中被执行。缺省的情况下， bash shell被分配给每一个用户，所以假定它就是用户们都使用着的 shell是没有什么问题的。如果用户们选择改用其他的 shell，就可以定制各自的设置文件（即profile文件）。

窍门 可以使用一系列的if/then语句提供对其他shell的定制。请阅读第18章中关于编写shell命令脚本程序的详细讨论。

8.2.13 查找容易被破译的口令字

对系统中全部的口令字进行检查的两个常用程序是：

- www.false.com/security/john/index.html站点上的John the Ripper程序。
- ftp://info.cert.org/pub/tools/crack/站点上的crack程序。

8.2.14 冻结一个用户

请按照下面的方法在不删除它的前提下冻结一个用户的帐户：

警告 不要冻结root帐户。

1) 以根用户身份登录进入系统。
2) 编辑password文件：
- 如果没有使用shadow隐藏口令字功能，编辑/etc/passwd文件。
- 如果使用了shadow隐藏口令字功能，编辑/etc/shadow文件。

3) 在文件中找到这个帐户。
4) 把这个帐户的口令字替换为一个星号（*）。口令字在用户数据段的第二个位置。

窍门 在/etc/passwd和/etc/shadow文件中每个用户的帐户信息都在单独的一行上。这个信息被冒号（:）分隔成不同的数据域。因此第一个数据域就是这一行上的第一个被分隔的数据部分，第二个数据域就是第一个冒号之后的数据部分，以此类推。

5) 保存并退出文件。

8.2.15 通过linuxconf程序冻结一个用户

请按照下面的方法通过linuxconf程序冻结一个用户：
1) 打开linuxconf程序（请阅读8.2.20节中的内容）。
2) 在linuxconf程序中打开User information（用户信息）窗口（更多详情请阅读8.2.8节中的内容）。
3) 单击The account is enabled（本帐户已激活）选择框弃选这一项。
4) 单击Accept（接受）按钮。

8.2.16 删除一个用户

如果想把一个用户连同他或她的用户目录一起删除，需要使用“ userdel -r username ”命令。

比如说，如果想完全删除属于paula的帐户，应该输入“ userdel -r paula ”命令。

窍门 如果因为某些原因删除一个帐户但是又需要保留该用户的用户目录的话，可以使用不带-r参数的userdel命令。

8.2.17 通过linuxconf程序删除一个用户

请按照下面的方法通过linuxconf程序删除一个用户：
1) 打开linuxconf程序（请阅读8.2.20节中的内容）。

2) 在linuxconf程序中打开User Information（用户信息）窗口（更多详情请阅读8.2.8节中的内容）。

3) 单击Delete（删除）按钮。

4) 在三种删除帐户数据方法的选项中选择一个。

5) 单击Accept（接受）按钮。

8.2.18 检查系统的易受攻击性

系统的易受攻击性取决于许多因素。对下面列出的几个问题的回答只要有“是”，就需要加强对口令字的保护（回答的“是”越多，就越需要加强保护）：

- 这个计算机或者网络是否需要长时间连接到因特网上？
- 这个计算机或者网络是否有许多人能够亲身接触到？
- 你是否设置有高访问率的因特网服务？比如说，在你的用户当中有没有人设置着一个流行的Web站点但又没有他们自己的域名？
- 你是否收到许多关于某些用户在因特网论坛上言行的投诉？

8.2.19 修改源代码使程序能够运行在使用shadow口令字功能的系统中

如果某个软件包需要对用户身份进行验证，但是其版本又不支持 shadow（隐藏）口令字功能，那就有两种选择：

- 如果能够设法获得这个程序的源文件，对它们进行设置使之能够使用 shadow口令字功能。
- 如果这个软件包必不可少，却又没有办法修补这个问题，那就只好转回到不使用 shadow口令字的状态去（请阅读8.2.11节的内容）。

进行这类修改的详细操作在有关的编程教材中有更深入的讨论。下面列出的是一些需要记住的基本事项：

- /etc/shadow文件只对根用户是可读的。因此，任何需要使用这个文件对用户身份进行验证的程序都必须执行SUID root命令（请阅读第5章中更详细的介绍）或者SUID shadow命令。
- 允许任何程序执行SUID root命令都是一个安全漏洞。如果必须这样做，千万要仔细编写这个程序。
- 如果需要使用C语言编程，必需的头文件保存在/usr/include/shadow中。
- 函数库在/usr/lib/libshadowa中。

8.2.20 打开linuxconf程序

请按照下面的方法打开linuxconf程序：

1) 以根用户身份登录进入系统。

2) 如有必要，进入Linux操作系统的图形用户界面（GUI）。

窍门 如果要从命令行上手动进入GUI，请输入“startx”命令。X或者X Window是Linux操作系统（和UNIX操作系统）中对GUI使用的术语。

3) 在Control Panel（控制面板）中拖动滚动条，直到看见 System Configuration（系统配置）按钮，如图8-5所示。

4) 单击System Configuration按钮。如果这是第一次运行这个程序，就会看到一个对话框，单击OK清除它。

5) 现在屏幕上将出现如图8-6所示的linuxconf程序窗口。

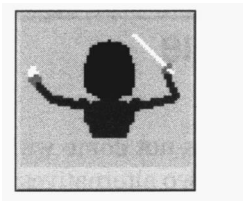

图8-5 fvwm窗口管理器程序中的Control Panel下的System Configuration按钮

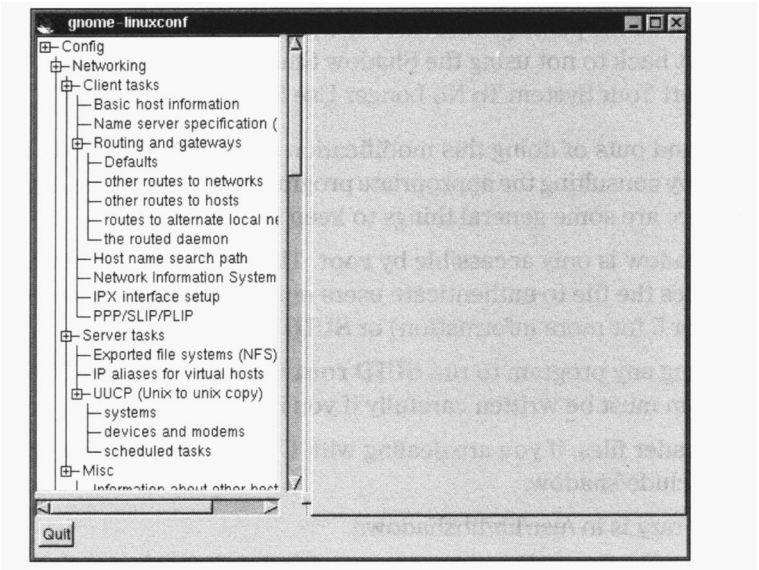

图8-6 linuxconf程序窗口