第3章 用户和组管理

Linux操作系统是一种多用户、多任务的分时操作系统。本章将介绍Linux操作系统的用户和组管理命令。主要包括三方面的内容：Linux用户账户的添加、删除与修改，用户组账户的添加、删除与修改，用户和用户组密码的管理。


视频讲解

3.1 用户和组管理概述

Linux系统对用户与组的账户登录通过ID(Identity)号实现，在登录系统时，输入的用户名与密码将会自动将用户名转换为ID号判断其是否存在，然后与存储的加密后的密码进行比对。

在Linux中，用户ID称为UID，组ID号称为GID。UID为0时表示超级用户，取值范围为1～999的UID，系统会预留给系统的虚拟用户。使用超级用户权限创建普通用户的UID从1000开始编号，取值大于或等于1000，例如，本书安装Ubuntu操作系统时创建的ubuntu用户的UID为1000。

Linux中的组分为基本组(私有组)和附加组(公共组)。一个用户同一时刻只能属于一个基本组，但可以同时加入多个附加组；创建用户时，默认会自动创建同名的组。

3.1.1 Linux用户角色划分

Linux系统是分角色管理用户的。角色的不同，用户权限和所完成的任务也不同。另外，需要注意的是，用户和组的角色是可以分别通过UID和GID识别的。

1. 超级用户

超级用户(super user)，也称为根用户(root user)，其UID值为0。超级用户是Linux系统中唯一拥有最高权限的用户，可以操作任何文件，执行任何命令。超级用户在安装操作系统时创建，默认情况下，超级用户只能在本地登录，而不能远程登录。在Ubuntu操作系统中，一般不使用超级用户直接登录系统。

2. 虚拟用户

虚拟用户也称为程序用户，其UID的取值范围是1～999。与真实用户区分开来，这类用户的最大特点是安装系统后默认就会存在，并且默认情况下是不能登录系统的。它们的存在是为了方便Linux系统管理，与系统进程密切相关，是系统正常运行必不可少的一部分。例如，系统默认创建的daemon、bin、sys、mail、ftp用户等都是虚拟用户，其中，daemon用户由系统的守护进程创建。

3. 普通用户

普通用户是在系统安装完成后由系统管理员创建的，其 UID 的取值范围是大于或等于 1000。普通用户能够管理自身的文件并拥有超级用户赋予的权限，可以直接登录或者远程登录 Linux 系统。安装 Ubuntu 操作系统时，可以设置一个被称为 Ubuntu 系统管理员的普通用户，例如，本书中的 ubuntu 用户。Ubuntu 系统管理员属于 sudos，即超级用户组，可以临时使用超级用户权限。

3.1.2　id 命令查看用户账户 ID

命令功能：查看 Linux 系统各个用户的 UID 和 GID。

命令语法：id ［用户名］。

【例 3-1】 id 命令查看用户账户 ID。

输入以下命令：

```
id  root
id  ubuntu
id
id  daemon
id  bin
id  sys
id  mail
id  ftp
```

以上命令的执行效果如图 3-1 所示。从图 3-1 中可以发现，root 用户的用户 ID(UID)、组 ID(GID)和组序号都为 0。本书安装 Ubuntu 操作系统时创建的 ubuntu 的用户 ID(UID)、组 ID(GID)和组编号都为 1000。直接输入无参数的 id 命令会显示当前登录用户，即 ubuntu 用户的 ID 信息。接着，使用 id 命令继续显示虚拟用户，包括 daemon、bin、sys、mail、ftp 用户的 ID 信息。可以发现，虚拟用户的 UID 的取值范围是 1～999。

```
(base) ubuntu@ubuntu:~$ id root
用户id=0(root) 组id=0(root) 组=0(root)
(base) ubuntu@ubuntu:~$ id ubuntu
用户id=1000(ubuntu) 组id=1000(ubuntu) 组=1000(ubuntu),4(adm),24(cdrom),27(sudo),
30(dip),46(plugdev),120(lpadmin),132(lxd),133(sambashare)
(base) ubuntu@ubuntu:~$ id
用户id=1000(ubuntu) 组id=1000(ubuntu) 组=1000(ubuntu),4(adm),24(cdrom),27(sudo),
30(dip),46(plugdev),120(lpadmin),132(lxd),133(sambashare)
(base) ubuntu@ubuntu:~$ id daemon
用户id=1(daemon) 组id=1(daemon) 组=1(daemon)
(base) ubuntu@ubuntu:~$ id bin
用户id=2(bin) 组id=2(bin) 组=2(bin)
(base) ubuntu@ubuntu:~$ id sys
用户id=3(sys) 组id=3(sys) 组=3(sys)
(base) ubuntu@ubuntu:~$ id mail
用户id=8(mail) 组id=8(mail) 组=8(mail)
(base) ubuntu@ubuntu:~$ id ftp
用户id=130(ftp) 组id=135(ftp) 组=135(ftp)
```

图 3-1　id 命令查看用户账户 ID 信息

3.1.3 用户和组配置文件

Linux 系统的用户配置文件包括/etc/passwd 文件和/etc/shadow 文件,用户组配置文件包括/etc/group 文件和/etc/gshadow 文件。/etc/passwd 文件存储的是用户账户信息,/etc/shadow 文件存储的是用户密码设置信息,/etc/group 文件存储的是的组账户信息,/etc/gshadow 文件存储的是组密码设置信息。

1. /etc/passwd 用户账户信息文件

/etc/passwd 文件的每行保存一位用户账户的信息,包括七个字段,每个字段使用冒号":"隔开,具体格式为:用户账户名:密码域:UID:GID:注释信息:主目录:命令解释器。/etc/passwd 文件各字段具体含义如表 3-1 所示。

表 3-1 /etc/passwd 文件各字段含义

字 段 名	含 义
用户账户名	用户登录系统时使用的用户名。用户名在系统中是唯一的
密码域	用 x 表示,密码已经被映射到/etc/shadow 影子文件中
UID	用户 ID,整数表示。每个用户 ID 在系统中是唯一的。超级用户的 UID 是 0,虚拟用户的 UID 取值范围是 1～999,普通用户的 UID 取值范围是大于或等于 1000
GID	组 ID,整数表示。每个组 ID 在系统中是唯一的
备注	用户账户的一些注释信息,如用户全名
主目录	用户登录系统后的默认目录
命令解释器	用户使用的 Shell,默认为/bin/bash

2. /etc/shadow 用户密码影子文件

/etc/shadow 文件的每行保存一位用户账户的密码设置信息,包括九个字段,每个字段使用冒号":"隔开,具体格式为:用户账户名:加密后的密码:最后一次修改时间:最小时间间隔:最大时间间隔:警告时间:不活动时间:失效时间:保留字段。/etc/shadow 文件各字段的具体含义如表 3-2 所示。

表 3-2 /etc/shadow 文件各字段含义

字 段 名	含 义
用户账户名	用户登录系统时使用的用户名,与/etc/passwd 文件中的用户账户名字段含义一样
加密后的密码	加密后的密码由三个部分组成,由 $ 分隔,具体格式为:$ 加密算法序号 $ 加盐值 $ 加密后的密码。加密算法序号表示为:0:DES 对称加密算法,1:MD5 哈希算法,2:Blowfish 加密算法,5:SHA-256 哈希算法,6:SHA-512 哈希算法。如果密码是"!",则表示还没有设置密码;如果密码是"*",则表示不会使用这个用户账户登录,通常是后台进程
最后一次修改时间	上次修改密码的天数(从 1970 年 1 月 1 日开始计算,到修改密码时的天数)
最小时间间隔	两次修改密码之间所需的最小天数,在这段时间内不允许修改密码,如果是 0,表示可以随时修改密码
最大时间间隔	密码保持有效的最大天数,超过这个天数后密码将失效,系统将强制用户修改密码;如果是 99999,表示密码不需要重新输入

续表

字 段 名	含 义
警告时间	密码失效前的警告天数，即用户账户的密码失效前多少天警告用户需要修改密码。普通用户默认为 7 天
不活动时间	密码过期的天数，用户账户的密码过期后多少天会被禁用
失效时间	密码失效的天数，从 1970 年 1 月 1 日开始计算，超过这个天数，用户账户的密码将无法使用
保留字段	保留、暂未使用

3./etc/group 组账户信息文件

/etc/group 文件的每行保存一个组的账户信息，包括四个字段，每个字段使用冒号“:”隔开，具体格式为：组名:组密码域:GID:组成员清单。/etc/group 文件各字段的具体含义如表 3-3 所示。

表 3-3 /etc/group 文件各字段含义

字 段 名	含 义
组名	用户组登录系统时使用的用户组名，在系统中是唯一的
组密码域	用 x 表示，组密码已经被映射到/etc/gshadow 影子文件中
GID	用户组 ID
组成员清单	以逗号分隔的组成员清单

4. /etc/gshadow 组密码影子文件

/etc/gshadow 文件的每行保存一个组的账户密码设置信息，包括四个字段，每个字段使用冒号“:”隔开，具体格式为：组名:组密码:GID:组成员清单。/etc/gshadow 文件各字段的具体含义如表 3-4 所示。

表 3-4 /etc/gshadow 文件各字段含义

字 段 名	含 义
组名	用户组登录系统时使用的用户组名，在系统中是唯一的
组密码	加密后的组密码，如果密码是“!”，则表示还没有设置密码，通常不需要设置组密码；如果密码是“*”，则表示不会使用这个用户账户登录
GID	用户组 ID
组成员清单	以逗号分隔的组成员清单

3.1.4 sudo 命令

命令功能：使用超级用户权限。

命令语法：sudo 命令名。

【例 3-2】 sudo 命令查看用户账户和密码信息。

本例将查看 Linux 系统的用户账户信息文件/etc/passwd 和密码影子文件/etc/shadow 中 root 用户和 ubuntu 用户的信息。查看用户账户信息文件不需要超级用户权限，而查看密码影子文件则需要，因此，需要使用 sudo 命令，即使用超级用户权限。输入以下命令：

```
head  -n1  /etc/passwd
cat  /etc/passwd  | grep ubuntu
sudo  head  -n1  /etc/shadow
sudo  cat  /etc/shadow| grep ubuntu
```

以上命令的执行效果如图 3-2 所示。因为 etc/passwd 和/etc/shadow 文件的内容较多,如果只是想查看某个用户的信息,如 root 用户,可以使用 head 命令显示第一行的内容,如果想查看其他用户,如 ubuntu,那么,需要结合管道和 grep 命令进行过滤。查看/etc/shadow 文件时,需要使用 sudo 命令

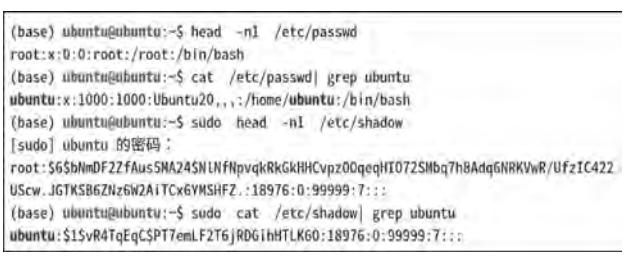

图 3-2　sudo 命令查看用户账户和密码信息

【例 3-3】 sudo 命令查看组账户和密码信息。

与查看用户账户信息和影子文件一样,查看/etc/group 组账户信息文件不需要超级用户权限,而查看/etc/gshadow 组密码影子文件则需要。输入以下命令:

```
head  -n4  /etc/group
sudo  cat  /etc/gshadow | grep root
sudo  cat  /etc/gshadow | grep sudo
```

以上命令的执行效果如图 3-3 所示。从图 3-3 中可以看出,使用 head 命令显示/etc/group 文件前 4 行的内容,即显示了 root 组、daemon 组、bin 组和 sys 组的账户信息,并使用 sudo 命令查看了/etc/shadow 文件,结合管道和 grep 命令过滤出 root 组和 sudo 组密码设置信息。可以发现,这两个组的密码都显示为 *,表示没有设置密码。图 3-3 最后一行显示查看 sudo 组的密码设置信息,可以发现,目前 sudo 组的组成员只有 ubuntu 用户。

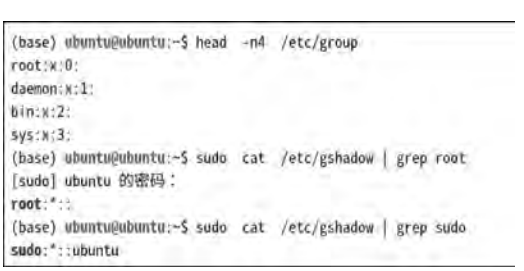

图 3-3　sudo 命令查看组账户和密码信息

需要注意的是,sudo 组是一个比较特殊的组,它是一个超级用户组,如果要临时使用超级用户权限,即使用 sudo 命令,需要将该用户加入 sudo 组。本书在后续的实例中将会运用这个知识点

3.2　用户管理命令

3.2.1　su 切换用户和 exit 回退命令

su 命令功能：切换用户。

su 命令语法：su　用户名。

exit 命令功能：回退原用户。

exit 命令语法：exit。

【例 3-4】 su 命令切换用户和 exit 命令回退原用户。

输入以下命令：

```
su  root
exit
```

以上命令的执行效果如图 3-4 所示。从图 3-4 中可以看出，使用 su 命令切换到 root 用户，输入密码，提示符从 $ 变成了 #，用户名也变成了 root。当输入 exit 命令后，回到原来的用户 ubuntu，提示符恢复 $ 。

```
(base) ubuntu@ubuntu:~$ su root
密码：
root@ubuntu:/home/ubuntu# exit
exit
(base) ubuntu@ubuntu:~$
```

图 3-4　su 命令切换用户和 exit 命令回退原用户

3.2.2　useradd 添加用户命令

命令功能：useradd 命令可以添加一个新用户，或者添加一个新用户并更新其配置信息。

命令语法：useradd ［选项］ 用户名。

常用参数：useradd 命令的常用参数及其含义如表 3-5 所示。

表 3-5　useradd 命令参数含义

参　数	含　义
-m	如果用户主目录不存在，则创建该主目录
-s	指定用户登录的 Shell 环境，默认是/bin/sh
-d	指定用户登录的主目录
-u	指定用户账户的 UID，但必须唯一
-r	创建一个系统账户
-p	指定用户密码，不推荐使用该参数，因为使用该参数对其他用户可见
-c	指定备注信息，将保存在/etc/passwd 文件的备注栏上
-e	指定失效时间，默认永久有效

续表

参　数	含　义
-f	指定不活动时间,即密码过期后,账户被彻底禁用之前的天数。0 表示立即禁用,-1 表示禁用这个功能
-G	指定用户所属的基本组或者 GID,但该组必须存在
-g	指定用户所属的附属组

【例 3-5】 添加“你的姓名 1”普通用户,并创建默认主目录。

本例使用“你的姓名 1”作为用户名,使用超级用户权限和 useradd-m 命令创建该普通用户,并创建默认主目录,以及查看用户账户信息文件和用户密码影子文件。输入以下命令:

```
sudo  useradd  -m  你的姓名 1
id  你的姓名 1
cat  /etc/passwd | grep 你的姓名 1
sudo  cat  /etc/shadow | grep  你的姓名 1
ls  /home
```

以上命令的执行效果如图 3-5 所示。从图 3-5 中可以看出,使用超级用户权限和 useradd -m 命令添加一个 yujian1 的用户账户,并创建默认主目录。通过 id 命令查看到该用户的 UID、GID 和组编号均为 1001,组名为 yujian1(与用户名同名);其在/etc/passwd 文件中的信息显示该用户的默认主目录为/home/yujian1,使用 ls/home 命令验证了这一点;默认 Shell 环境为/bin/sh;其在/etc/shadow 影子文件中的加密密码是“!”,说明该用户还没有设置密码;另外,显示最后一次修改时间为 19 004 天,最小时间间隔为 0 天,最大时间间隔为 99 999 天,警告时间为 7 天。

```
(base) ubuntu@ubuntu:~$ sudo useradd -m yujian1
(base) ubuntu@ubuntu:~$ id yujian1
用户id=1001(yujian1) 组id=1001(yujian1) 组=1001(yujian1)
(base) ubuntu@ubuntu:~$ cat  /etc/passwd | grep yujian1
yujian1:x:1001:1001::/home/yujian1:/bin/sh
(base) ubuntu@ubuntu:~$ sudo  cat  /etc/shadow| grep yujian1
yujian1:!:19004:0:99999:7:::
(base) ubuntu@ubuntu:~$ ls /home
ubuntu  yujian1
```

图 3-5　添加“你的姓名 1”普通用户,并创建默认主目录

【例 3-6】 添加“你的姓名 2”普通用户,并将其加入超级用户组。

本例使用“你的姓名 2”作为用户名,使用超级用户权限和 useradd -g 命令创建该普通用户,并加入 sudo 超级用户组,最后查看用户账户信息文件和用户密码影子文件。输入以下命令:

```
sudo  useradd  -g  sudo 你的姓名 2
id  你的姓名 2
cat  /etc/passwd  |grep 你的姓名 2
sudo  cat  /etc/shadow|grep 你的姓名 2
```

以上命令的执行效果如图 3-6 所示。从图 3-6 中可以看出，使用超级用户权限和 useradd -g 命令添加一个 yujian2 的用户账户，并将该用户加入超级用户组，通过 id 命令查看到该用户的 UID 为 1002、GID 和组编号均为 27，组名为 sudo；其在/etc/passwd 文件中的信息显示该用户的默认主目录为/home/yujian2，但由于没有使用-m 参数，因此实际上并没有创建该默认目录，使用 ls/home 命令验证了这一点；查看该用户在/etc/shadow 文件的信息除用户账户名外，其他内容与例 3-5 相同，因此此处不再赘述。

```
(base) ubuntu@ubuntu:~$ sudo  useradd  -g  sudo yujian2
[sudo] ubuntu 的密码：
(base) ubuntu@ubuntu:~$ id yujian2
用户id=1002(yujian2) 组id=27(sudo) 组=27(sudo)
(base) ubuntu@ubuntu:~$ cat  /etc/passwd| grep yujian2
yujian2:x:1002:27::/home/yujian2:/bin/sh
(base) ubuntu@ubuntu:~$ sudo  cat  /etc/shadow| grep yujian2
yujian2:!:19004:0:99999:7:::
(base) ubuntu@ubuntu:~$ ls /home
ubuntu  yujian1
```

图 3-6　添加“你的姓名 2”普通用户，并加入超级用户组

【例 3-7】 添加“你的姓名 3”普通用户，并指定登录主目录。

假设系统管理员打算添加一位远程登录的普通用户，并限制他只能登录到某个指定的主目录。为解决这一问题，本例使用“你的姓名 3”作为用户名，使用超级用户权限和 useradd -d 命令创建该普通用户，并指定登录主目录为已经创建好的目录/ftp，最后查看用户账户信息文件和用户密码影子文件。输入以下命令：

```
sudo  mkdir  -p  /ftp
sudo  useradd  -d  /ftp  你的姓名 3
id  你的姓名 3
cat  /etc/passwd | grep  你的姓名 3
sudo  cat  /etc/shadow | grep  你的姓名 3
```

以上命令的执行效果如图 3-7 所示。从图 3-7 中可以看出，首先创建目录/ftp，使用超级用户权限和 useradd -d 命令添加一个 yujian3 的用户账户，并指定登录主目录为/ftp，通过 id 命令查看到该用户的 UID、GID 和组编号均为 1003，组名为 yujian3（与用户名同名）；其在/etc/passwd 文件中的信息显示该用户的默认主目录为/ftp，这与默认创建的在/home 下的主目录不同；查看该用户在/etc/shadow 文件的信息除用户账户名外，其他内容与例 3-5 相同，因此此处不再赘述。

```
(base) ubuntu@ubuntu:~$ sudo  mkdir  -p  /ftp
(base) ubuntu@ubuntu:~$ sudo  useradd  -d  /ftp  yujian3
(base) ubuntu@ubuntu:~$ id yujian3
用户id=1003(yujian3) 组id=1003(yujian3) 组=1003(yujian3)
(base) ubuntu@ubuntu:~$ cat  /etc/passwd | grep yujian3
yujian3:x:1003:1003::/ftp:/bin/sh
(base) ubuntu@ubuntu:~$ sudo  cat  /etc/shadow| grep yujian3
yujian3:!:19004:0:99999:7:::
```

图 3-7　添加“你的姓名 3”普通用户，并指定登录主目录

【例 3-8】 添加“你的姓名 4”普通用户并创建默认主目录,指定备注和失效时间。

本例使用“你的姓名 4”作为用户名,使用超级用户权限和 useradd -m 命令创建该普通用户,并使用-c 和-e 参数分别指定备注信息和失效时间,最后查看用户账户信息文件和用户密码影子文件。输入以下命令:

```
sudo  useradd  -m  -c"expired in 30 days" -e 30 你的姓名 4
id  你的姓名 4
cat  /etc/passwd| grep  你的姓名 4
sudo  cat  /etc/shadow| grep  你的姓名 4
ls  /home
```

以上命令的执行效果如图 3-8 所示。从图 3-8 中可以看出,使用超级用户权限和 useradd -m 命令添加一个 yujian4 的用户账户,并创建默认主目录,使用-c 参数指定备注信息为 expired in 30 days,即 30 天后过期;通过 id 命令查看到该用户的 ID、组 ID 和组编号均为 1004,组名为 yujian4(与用户名同名);使用 cat 命令显示该用户在/etc/passwd 文件中的备注和默认主目录信息,查看该用户在/etc/shadow 文件的信息除用户账户名外,其他内容与例 3-5 相同,因此,此处不再赘述;使用 ls /home 命令验证了该命令创建了默认主目录。

```
(base) ubuntu@ubuntu:~$ sudo  useradd  -m  -c " expired in 30 days " -e 30 yujian4
[sudo] ubuntu 的密码:
(base) ubuntu@ubuntu:~$ sudo userdel -rf yujian4
userdel:yujian4 信件池 (/var/mail/yujian4) 未找到
(base) ubuntu@ubuntu:~$ sudo  useradd  -m  -c "expired in 30 days" -e 30 yujian4
(base) ubuntu@ubuntu:~$ id yujian4
用户id=1004(yujian4) 组id=1004(yujian4) 组=1004(yujian4)
(base) ubuntu@ubuntu:~$ cat  /etc/passwd| grep yujian4
yujian4:x:1004:1004:expired in 30 days:/home/yujian4:/bin/sh
(base) ubuntu@ubuntu:~$ sudo  cat  /etc/shadow| grep yujian4
yujian4:!:19004:0:99999:7::30:
(base) ubuntu@ubuntu:~$ ls /home
ubuntu  yujian1  yujian4
```

图 3-8 添加“你的姓名 4”普通用户,创建默认主目录,指定备注和失效时间

【例 3-9】 添加“你的姓名 5”虚拟用户。

本例使用“你的姓名 5”作为用户名,使用超级用户权限和 useradd -r 命令创建该虚拟用户,并查看用户账户信息文件和用户密码影子文件。输入以下命令:

```
sudo  useradd  -r  你的姓名 5
id  你的姓名 5
cat  /etc/passwd | grep  你的姓名 5
sudo  cat  /etc/shadow | grep 你的姓名 5
```

以上命令的执行效果如图 3-9 所示。从图 3-9 中可以看出,使用超级用户权限和 useradd -r 命令添加一个用户名为 yujian5 的虚拟用户;需要注意的是,与例 3-5 至例 3-8 不同,本例创建的是虚拟用户,其 UID 的取值范围是 1～999;通过 id 命令查看到该用户的 UID、GID 和组编号均为 998,UID 属于虚拟用户取值范围;使用超级用户权限和 cat 命令查看/etc/shadow 文件发现,该虚拟用户的最后一次修改时间与前面创建的普通用户一样,

但与普通用户不同的是：最小时间间隔、最大时间间隔和警告时间都没有设置。

```
(base) ubuntu@ubuntu:~$ id yujian5
用户id=998(yujian5) 组id=998(yujian5) 组=998(yujian5)
(base) ubuntu@ubuntu:~$ cat  /etc/passwd| grep yujian5
yujian5:x:998:998::/home/yujian5:/bin/sh
(base) ubuntu@ubuntu:~$ sudo  cat  /etc/shadow| grep yujian5
yujian5:!:19004:::::
```

图 3-9　添加“你的姓名 5”虚拟用户

【例 3-10】 添加“你的姓名 6”普通用户，并指定 UID。

在日常工作中，为了方便管理，企事业单位通常使用员工的工号作为员工 ID，而学校通常使用学号作为学号 ID。本例使用“你的姓名 6”作为用户名，使用超级用户权限和 useradd -u 命令将你的学号（本书中以 2019119101 为例）设置为用户 UID，这样，当用户登录 Linux 系统时，可以很方便地通过其学号和姓名进行识别和管理。最后，查看用户账户信息文件和用户密码影子文件。输入以下命令：

```
sudo  useradd  -u  你的学号  你的姓名 6
id  你的姓名 6
cat  /etc/passwd|grep  你的姓名 6
sudo  cat  /etc/shadow|grep  你的姓名 6
```

以上命令的执行效果如图 3-10 所示，添加了用户名为 yujian6 的普通用户。需要注意的是，与例 3-5 至例 3-9 不同，本例中用户的 UID 直接通过命令指定，而不是由系统自动分配。

```
(base) ubuntu@ubuntu:~$ sudo useradd -u 2019119101 yujian6
(base) ubuntu@ubuntu:~$ id yujian6
用户id=2019119101(yujian6) 组id=1005(yujian6) 组=1005(yujian6)
(base) ubuntu@ubuntu:~$ cat  /etc/passwd | grep yujian6
yujian6:x:2019119101:1005::/home/yujian6:/bin/sh
(base) ubuntu@ubuntu:~$ sudo  cat  /etc/shadow| grep yujian6
yujian6:!:19005:0:99999:7:::
```

图 3-10　添加“你的姓名 6”普通用户，并指定 UID

3.2.3　passwd 设置用户密码命令

命令功能：设置指定用户账户名密码。

命令语法：passwd　用户账户名。

常用参数：passwd 命令的常用参数及其含义如表 3-6 所示。

表 3-6　passwd 命令参数含义

参　数	含　义
-d	即 delete，删除指定用户的密码
-e	即 expire，强制指定用户的密码过期
-l	即 lock，锁定指定用户账户
-u	即 unlock，解锁指定用户账户

【例 3-11】 passwd 命令设置用户密码。

本例使用超级用户权限和 passwd 命令设置用户密码。为了配合例 3-26 破解系统用户密码,本例将“你的姓名 1”用户的密码设置为弱口令:654321,将“你的姓名 2”用户的密码设置为弱口令:a12345。输入以下命令:

```
sudo  passwd  你的姓名 1
sudo  passwd  你的姓名 2
su  你的姓名 2
sudo  cat  /etc/shadow|grep  你的姓名 2
exit
```

以上命令的执行效果如图 3-11 所示。从图 3-11 中可以看出,使用超级用户权限和 passwd 命令分别设置了 yujian1 和 yujian2 的弱口令密码,并使用 su 命令切换到 yujian2 用户,由于该用户属于 sudo 超级用户组,因此,该用户能够使用超级用户权限查看/etc/shadow 文件的信息。

```
(base) ubuntu@ubuntu:~$ sudo passwd yujian1
[sudo] ubuntu 的密码:
新的 密码:
重新输入新的 密码:
passwd:已成功更新密码
(base) ubuntu@ubuntu:~$ sudo passwd yujian2
新的 密码:
重新输入新的 密码:
passwd:已成功更新密码
(base) ubuntu@ubuntu:~$ su yujian2
密码:
$ sudo  cat  /etc/shadow |grep yujian2
[sudo] yujian2 的密码:
yujian2:$6$Z.BH/OFZOXOC4zEg$144uDQWkW3YPazb5lcf2wws5.GX/lVfGdpkivU9t/SPKsURynBTBrbU8
kymYVs./FcbvqeBPYpLMZrlgqc33.:19004:0:99999:7:::
$ exit
(base) ubuntu@ubuntu:~$
```

图 3-11　设置用户密码

【例 3-12】 passwd 命令删除用户密码。

本例为删除“你的姓名 3”和“你的姓名 6”两个用户的密码。输入以下命令:

```
sudo  cat  /etc/shadow|grep 你的姓名 3
sudo  passwd  -d 你的姓名 3
sudo  cat  /etc/shadow|grep 你的姓名 3
sudo  passwd  -d 你的姓名 6
```

以上命令的执行效果如图 3-12 所示。从图 3-12 中可以看出,首先使用超级用户权限和 cat 命令查看 yujian3 用户没有设置密码之前,在/etc/shadow 密码影子文件中的信息。可以发现,其加密后的密码是“!”,表示还没有设置密码;当使用 sudo passwd -d 删除该用户密码后,其加密后的密码显示为空。

```
(base) ubuntu@ubuntu:~$ sudo  cat  /etc/shadow| grep yujian3
[sudo] ubuntu 的密码：
yujian3:!:19004:0:99999:7:::
(base) ubuntu@ubuntu:~$ sudo  passwd  -d yujian3
passwd：密码过期信息已更改。
(base) ubuntu@ubuntu:~$ sudo  cat  /etc/shadow| grep yujian3
yujian3::19004:0:99999:7:::
```

图 3-12　删除用户密码

3.2.4　usermod 修改用户命令

命令功能：修改用户属性信息，包括锁定和解锁用户、添加到附加组和修改 UID。

命令语法：usermod ［选项］ 用户名。

常用参数：usermod 命令的常用参数及其含义如表 3-7 所示。

表 3-7　usermod 命令参数含义

参　数	含　义
-l	即 lock，锁定用户
-U	即 unlock，解锁用户
-G	附加组名称
-a	即 append，也就是将用户附加到附加组中，而不必离开基本组；需要与-G 参数一起配合使用
-u	修改指定用户 UID
-d	修改用户登录的主目录
-l	修改用户名，注意语法为：usermod　-l 新用户名原用户名

【例 3-13】 usermod 命令锁定和解锁用户。

本例使用超级用户权限和 usermod 命令锁定和解锁用户，并使用 su 切换用户命令进行验证，成功切换到该用户账户后，尝试使用超级用户权限显示密码影子文件的内容。输入以下命令：

```
sudo  usermod  -L 你的姓名 1
su  你的姓名 1
sudo  usermod  -U 你的姓名 1
su  你的姓名 1
sudo  cat  /etc/shadow | grep 你的姓名 1
exit
```

以上命令的执行效果如图 3-13 所示。从图 3-13 中可以看出，使用超级用户权限和 usermod -L 锁定 yujian1 用户后，使用 su 命令切换到该用户，显示“su:认证失败”；在使用 usermod -U 解锁后，再次切换，提示符变成“$”，切换成功。切换到该用户后，尝试使用 sudo 命令显示密码影子文件，提示“yujian1 不在 sudoers 文件中。此事将被报告。”，意思是提示 yujian1 用户不在 sudo 超级用户组中，无法使用 sudo 命令。这个问题将在下一个例子中解决。

```
(base) ubuntu@ubuntu:~$ sudo  usermod  -L yujian1
[sudo] ubuntu 的密码：
(base) ubuntu@ubuntu:~$ su yujian1
密码：
su: 认证失败
(base) ubuntu@ubuntu:~$ sudo usermod -U yujian1
(base) ubuntu@ubuntu:~$ su yujian1
密码：
$ sudo  cat  /etc/shadow |grep yujian1
[sudo] yujian1 的密码：
yujian1 不在 sudoers 文件中。此事将被报告。
$ exit
(base) ubuntu@ubuntu:~$
```

图 3-13　usermod 命令锁定和解锁用户

【例 3-14】 usermod 命令将已有用户附加到 sudo 组，并修改 UID。

例 3-13 中，由于 yujian1 用户不属于超级用户组，因此无法使用超级用户权限。本例解决了这一问题：使用 usermod 命令将该用户加入 sudo 组。这需要使用-a 参数将用户附加到某个附加组和-G 参数指定组名。需要注意的是，-aG 参数通常是配合使用的。最后使用-u 参数修改该用户的 UID。输入以下命令：

```
sudo  usermod  -aG  sudo  你的姓名 1
su  你的姓名 1
sudo  cat  /etc/shadow | grep  你的姓名 1
exit
id  你的姓名 1
sudo  usermod  -u  9999  你的姓名 1
id  你的姓名 1
```

以上命令的执行效果如图 3-14 所示。从图 3-14 中可以看出，使用 usermod -aG 命令将 yujian1 添加到 sudo 超级用户组后，yujian1 用户能够使用超级用户权限查看密码影子文件了。因为，不能在已经登录的 yujian1 用户上直接修改其 UID，因此，使用 exit 命令回到原 ubuntu 用户后，使用 id 命令查看 yujian1 用户的 UID 为 1001，接着使用 usermod -u 命令将其改为 9999，再次使用 id 命令查看，验证了 UID 已经修改成功。

```
(base) ubuntu@ubuntu:~$ sudo  usermod  -aG  sudo yujian1
[sudo] ubuntu 的密码：
(base) ubuntu@ubuntu:~$ su yujian1
密码：
$ sudo cat /etc/shadow | grep yujian1
[sudo] yujian1 的密码：
yujian1:$6$TISo2InQGyO.F/yKSyA/.YEmSdb3tltaAd5cRjWMad3eAgs1AdmPWOKCyFBjWFYNvivQnG7YpmpY6eOOf6L4vs68hCthhh
aUFSrhVj/:19004:0:99999:7:::
$ exit
(base) ubuntu@ubuntu:~$ id yujian1
用户id=1001(yujian1) 组id=1001(yujian1) 组=1001(yujian1),27(sudo)
(base) ubuntu@ubuntu:~$ sudo  usermod  -u  9999 yujian1
(base) ubuntu@ubuntu:~$ id yujian1
用户id=9999(yujian1) 组id=1001(yujian1) 组=1001(yujian1),27(sudo)
```

图 3-14　usermod 命令将用户附加到 sudo 组，并修改 UID

3.2.5　chage 更改用户密码有效期命令

命令功能：更改用户密码有效期信息。

命令语法：chage ［选项］ 用户名。

常用参数：chage 命令的常用参数及其含义如表 3-8 所示。

表 3-8　chage 命令参数含义

参　数	含　义
-l	列出密码的有效期
-m	两次修改密码相距的最小天数，如果为 0，则表示随时可以修改
-M	密码有效的最大天数
-E	指定密码过期时间，0 表示立刻过期，－1 表示永不过期

【例 3-15】 chage 命令直接修改用户密码的有效期。

本例使用 chage 命令和-m、-M 参数直接将用户账户的有效期修改为两次修改密码相距的最小天数为 7 天，密码有效的最大天数为 30 天。输入以下命令：

```
sudo  chage  -l  你的姓名 3
sudo  chage  -m  7  -M  30 你的姓名 3
sudo  chage  -l  你的姓名 3
```

以上命令的执行效果如图 3-15 所示。使用 chage 命令修改 yujian3 用户密码有效期：两次修改密码相距的最小天数从 0 天修改为 7 天，密码有效的最大天数从 99999 天修改为 30 天。

```
(base) ubuntu@ubuntu:~$ sudo chage -l yujian3
[sudo] ubuntu 的密码：
最近一次密码修改时间                                    ：1月 12, 2022
密码过期时间                                          ：从不
密码失效时间                                          ：从不
帐户过期时间                                          ：从不
两次改变密码之间相距的最小天数                        ：0
两次改变密码之间相距的最大天数                        ：99999
在密码过期之前警告的天数                              ：7
(base) ubuntu@ubuntu:~$ sudo  chage  -m  7  -M  30 yujian3
(base) ubuntu@ubuntu:~$ sudo chage -l yujian3
最近一次密码修改时间                                    ：1月 12, 2022
密码过期时间                                          ：2月 11, 2022
密码失效时间                                          ：从不
帐户过期时间                                          ：从不
两次改变密码之间相距的最小天数                        ：7
两次改变密码之间相距的最大天数                        ：30
在密码过期之前警告的天数                              ：7
```

图 3-15　chage 命令直接修改用户密码的有效期

【例 3-16】 chage 命令交互式修改用户账户的有效期。

本例使用 chage 命令交互式修改用户账户的有效期，不需要任何参数。对不需要修改的选项，直接输入后按 Enter 键跳过即可。输入以下命令：

```
sudo  chage  -l  你的姓名 4
sudo  chage  你的姓名 4
sudo  chage  -l  你的姓名 4
```

以上命令的执行效果如图 3-16 所示。从图 3-16 中可以看出,使用 chage 命令交互式修改 yujian4 用户密码有效期:两次修改密码相距的最小天数从 0 天修改为 7 天,密码有效的最大天数从 99 999 天修改为 30 天。需要注意的是,在交互式选项中,最小密码年龄表示两次修改密码相距的最小天数,最大密码年龄密码有效的最大天数。

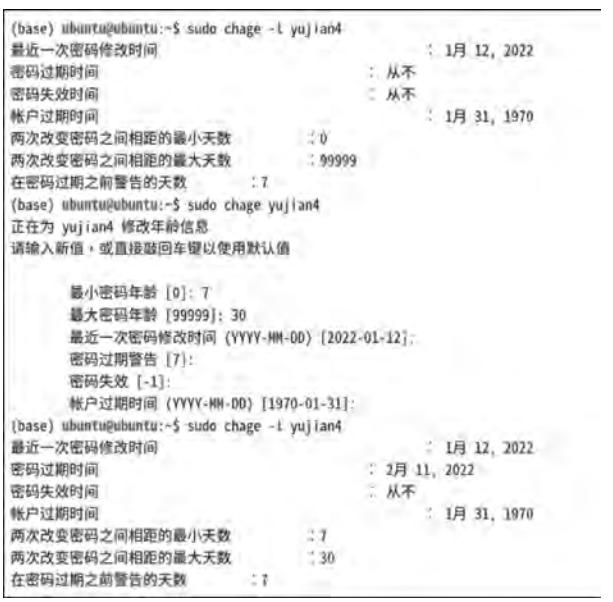

图 3-16　chage 命令交互式修改用户账户的有效期

3.2.6　userdel 删除用户命令

命令功能:删除指定用户。

命令语法:userdel ［选项］ 用户名。

常用参数:userdel 命令的常用参数及其含义如表 3-9 所示。

表 3-9　userdel 命令参数含义

参　数	含　义
-r	删除指定用户,并递归删除其主目录下的所有文件和文件夹
-f	强制删除用户,即使该用户已经登录系统

【例 3-17】 userdel 命令删除用户及其主目录。

本例使用 userdel 命令分别删除三个用户及其主目录。输入以下命令:

```
sudo  userdel  你的姓名 5
sudo  userdel  -r  你的姓名 4
ls  /home
```

打开一个新终端，输入以下命令：

```
su  你的姓名3
sudo  userdel  -r  你的姓名3
sudo  userdel  -rf  你的姓名3
```

以上命令的执行效果如图 3-17 所示。从图 3-17 中可以看出，使用 userdel 命令删除 yujian5 用户，由于该用户是虚拟用户，没有创建主目录，因此不需要使用任何参数直接删除即可。对于 yujian4 普通用户，在例 3-1 中已经创建了主目录，需要使用-r 参数删除其对应的主目录。对于 yujian3 普通用户，特意打开一个新终端，切换到该用户上，使该用户登录系统，再使用-r 参数删除时，显示 userdel：user yujian3 is currently used by process 6441，意思是 yujian3 用户正在由进程 6441 使用。因此，需要使用-rf 参数强制删除。

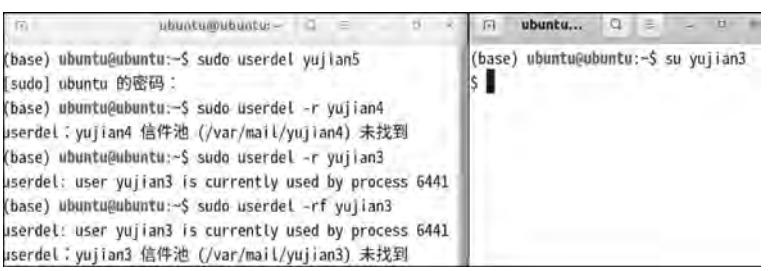

图 3-17　userdel 命令删除用户及其主目录

3.3　用户组管理命令

3.3.1　groupadd 添加用户组命令

命令功能：添加用户组。

命令语法：groupadd　用户组名。

常用参数：groupadd 命令的常用参数及其含义如表 3-10 所示。

表 3-10　groupadd 命令参数含义

参　数	含　义
-g	指定新建用户组的 GID
-f	如果组已存在，则此参数失效；如果 GID 已被使用，则取消
-r	创建系统组账户，GID 小于 1000

【例 3-18】 groupadd 命令添加用户组。

本例使用 groupadd 命令分别添加两个用户组，并指定 GID。输入以下命令：

```
sudo  groupadd  -g  6666  student
cat  /etc/group | grep student
sudo  groupadd  -g  8888  teacher
cat  /etc/group | grep teacher
```

以上命令的执行效果如图 3-18 所示。从图 3-18 中可以看出,使用 groupadd 命令添加了 student 用户组,并指定 GID 为 6666;添加了 teacher 用户组,并指定 GID 为 8888,并使用 cat 命令查看/etc/group 文件中的组信息。

```
(base) ubuntu@ubuntu:~$ sudo  groupadd  -g  6666  student
(base) ubuntu@ubuntu:~$ cat  /etc/group | grep student
student:x:6666:
(base) ubuntu@ubuntu:~$ sudo  groupadd  -g  8888  teacher
(base) ubuntu@ubuntu:~$ cat  /etc/group | grep teacher
teacher:x:8888:
```

图 3-18　groupadd 命令添加用户组

3.3.2　groupmod 修改用户组命令

命令功能:修改用户组属性信息,包括用户组的 GID 和用户组名。

命令语法:groupmod ［选项］ 组名。

常用参数:groupmod 命令的常用参数及其含义如表 3-11 所示。

表 3-11　groupmod 命令参数含义

参　数	含　义
-g	修改用户组的 GID
-n	修改用户组名

【例 3-19】 groupmod 命令修改组名和 GID。

本例使用 groupmod 命令修改用户组名和 GID。输入以下命令:

```
sudo  groupmod -n  stu  student
sudo  groupmod  -g  你的班级号  stu
cat  /etc/group|grep stu
```

以上命令的执行效果如图 3-19 所示。从图 3-19 中可以看出,使用 groupmod 命令修改了 student 用户组名为 stu,并修改了 GID 为你的班级号(本书以 20191191 为例),最后查看/etc/group 文件验证了用户组信息已经成功修改。

```
(base) ubuntu@ubuntu:~$ sudo  groupmod  -n  stu  student
[sudo] ubuntu 的密码:
(base) ubuntu@ubuntu:~$ sudo  groupmod  -g  20191191  stu
(base) ubuntu@ubuntu:~$ cat  /etc/group | grep stu
stu:x:20191191:
```

图 3-19　groupmod 命令修改组名和 GID

3.3.3　gpasswd 管理用户组命令

命令功能:管理用户组,包括添加或删除用户,设置和删除组密码,以及指定管理员。

命令语法:gpasswd ［选项］ 用户组名。

常用参数:gpasswd 命令的常用参数及其含义如表 3-12 所示。

表 3-12　gpasswd 命令参数含义

参　数	含　义
-a	添加用户到组
-d	从组中删除用户
-r	删除组密码
-A	指定组管理员，不一定是组内成员，组管理员可以增删成员，修改组密码等操作
-M	指定组成员

【例 3-20】 gpasswd 命令添加和删除用户。

本例使用 gpasswd 命令添加两个用户并分别添加到用户组，并从用户组中删除一个用户，最后通过 id 命令查看用户所属的组名是否修改成功。输入以下命令：

```
sudo  gpasswd  -a  你的姓名1  teacher
id  你的姓名1
sudo  gpasswd  -a  你的姓名6  teacher
sudo  gpasswd  -a  你的姓名6  stu
id  你的姓名6
sudo  gpasswd  -d  你的姓名6  teacher
id  你的姓名6
```

以上命令的执行效果如图 3-20 所示。从图 3-20 中可以看出，首先使用 gpasswd -a 命令将 yujian1 添加到了 teacher 组，将 yujian6 添加到了 teacher 组和 stu 组。yujian6 同时属于教师组和学生组，这有些不合理。接着，使用 gpasswd -d 命令将 yujian6 用户从 teacher 组中删除。最后使用 id 命令验证了修改结果是否正确。可以发现，yujian1 用户属于 yujian1 基本组、sudo 附加组和 teacher 附加组，yujian6 用户属于 yujian6 基本组、stu 附加组。

```
(base) ubuntu@ubuntu:~$ sudo  gpasswd  -a  yujian1  teacher
[sudo] ubuntu 的密码：
正在将用户 "yujian1"加入到 "teacher"组中
(base) ubuntu@ubuntu:~$ id yujian1
用户id=9999(yujian1) 组id=1001(yujian1) 组=1001(yujian1),27(sudo),8888(teacher)
(base) ubuntu@ubuntu:~$ sudo  gpasswd  -a  yujian6  teacher
正在将用户 "yujian6"加入到 "teacher"组中
(base) ubuntu@ubuntu:~$ sudo  gpasswd  -a  yujian6  stu
正在将用户 "yujian6"加入到 "stu"组中
(base) ubuntu@ubuntu:~$ id yujian6
用户id=2019119101(yujian6) 组id=1005(yujian6) 组=1005(yujian6),8888(teacher),20191191(stu)
(base) ubuntu@ubuntu:~$ sudo  gpasswd  -d  yujian6  teacher
正在将用户 "yujian6"从 "teacher"组中删除
(base) ubuntu@ubuntu:~$ id yujian6
用户id=2019119101(yujian6) 组id=1005(yujian6) 组=1005(yujian6),20191191(stu)
```

图 3-20　gpasswd 命令添加和删除用户

【例 3-21】 gpasswd 命令设置和删除组密码。

本例设置 stu 组的密码，将 teacher 组密码删除，并通过/etc/gshadow 密码影子文件查看设置情况。输入以下命令：

```
sudo  gpasswd  stu
sudo  cat  /etc/gshadow  |grep stu
sudo  gpasswd  -r  teacher
sudo  cat  /etc/gshadow  |grep teacher
```

以上命令的执行效果如图 3-21 所示。从图 3-21 中可以看出,使用 gpasswd 命令设置了 stu 用户组的密码(可设置为弱口令 123456),目的在于方便课后习题(实操题)使用 john 软件破解;使用 gpasswd -r 命令删除了 teacher 组密码。通过/etc/gshadow 文件,读者可以发现 stu 组记录末尾显示组成员有用户 yujian6,teacher 组记录末尾显示组成员有用户 yujian1,并且 teacher 组密码为空。

```
(base) ubuntu@ubuntu:~$ sudo  gpasswd  stu
[sudo] ubuntu 的密码：
正在修改 stu 组的密码
新密码：
请重新输入新密码：
(base) ubuntu@ubuntu:~$ sudo  cat  /etc/gshadow  | grep stu
stu:$6$uq4Y5/hE4U$byIQkCcU96vVg8atDVZp8feTg8sJ14WJxkOxvQlrDquu83.T2oEOKiEBksM2Xl2ByOiyg94TzZN
SvLOcgrdg21::yujian6
(base) ubuntu@ubuntu:~$ sudo  gpasswd  -r  teacher
(base) ubuntu@ubuntu:~$ sudo  cat  /etc/gshadow  | grep teacher
teacher:::yujian1
```

图 3-21　gpasswd 命令设置和删除组密码

3.3.4　groupdel 删除用户组命令

命令功能：删除用户组。

命令语法：groupdel　用户组名。

【例 3-22】　groupdel 命令删除用户组。

本例首先添加了一个用户组 testgroup,并使用 tail -n1 命令查看/etc/group 文件的最后一行;然后在确认创建了该用户组后,使用 groupdel 命令删除,并查看/etc/group 文件。输入以下命令:

```
sudo  groupadd  testgroup
tail  -n1  /etc/group
sudo  groupdel  testgroup
cat  /etc/group | grep testgroup
```

以上命令的执行效果如图 3-22 所示。删除 testgroup 用户组后,在/etc/group 组账户信息文件中查找 testgroup,显示结果为空,表明该用户组已经成功删除。

```
(base) ubuntu@ubuntu:~$ sudo  groupadd  testgroup
(base) ubuntu@ubuntu:~$ tail -n1 /etc/group
testgroup:x:8889:
(base) ubuntu@ubuntu:~$ sudo  groupdel  testgroup
(base) ubuntu@ubuntu:~$ cat /etc/group | grep testgroup
(base) ubuntu@ubuntu:~$
```

图 3-22　groupdel 命令删除用户组

3.4 用户和组的运行维护

3.4.1 chpasswd 批量修改用户密码命令


视频讲解

命令功能：从系统的标准输入读入用户名和密码，对已存在的用户修改密码，达到批量修改用户密码的目的。

命令语法：echo 用户名：密码|chpasswd。

【例 3-23】 chpasswd 命令批量修改用户密码。

本例通过一个 Shell 脚本文件批量添加用户 user01～user10，共 10 个用户，并使用 useradd -g 命令指定用户所属的组为 stu；通过 chpasswd 命令批量修改用户密码为 123456。最后使用 tail 命令查看/etc/passwd 文件信息，观察用户是否批量添加成功。输入以下命令：

```
gedit  adduser.sh
```

打开 gedit 窗口后，输入以下 Shell 脚本内容：

```
#!/bin/bash
for  i  in  {01..10}
do
  useradd  user$i  -g  stu
  echo  user$i:123456 | chpasswd
done
```

保存并关闭窗口。该脚本中，$i 表示获取变量 i 的值，{01..10}表示 01～10 的数字序列。输入以下命令：

```
sudo  bash  adduser.sh
tail  /etc/passwd
id  user01
su  user01
exit
```

以上命令的执行效果如图 3-23 所示。从图 3-23 中可以看出，使用 tail 命令查看到这 10 个用户已经批量添加成功，并加入了 stu 组(GID 为 20191191)。选择第一个用户 user01 进行验证，使用 id 命令查看其用户组，使用 su 命令输入密码 123456，如果密码输入正确，就会跳转到下一行，在提示符 $ 后可以继续输入命令，表示切换成功；否则会提示用户“su：认证失败”。

需要注意的是，本例首先批量添加了用户，如果完成后需要批量删除用户，可以输入以下命令：

```
gedit  deluser.sh
```

```
(base) ubuntu@ubuntu:~$ gedit adduser.sh
(base) ubuntu@ubuntu:~$ sudo bash adduser.sh
(base) ubuntu@ubuntu:~$ tail /etc/passwd
user01:x:10020:20191191::/home/user01:/bin/sh
user02:x:10021:20191191::/home/user02:/bin/sh
user03:x:10022:20191191::/home/user03:/bin/sh
user04:x:10023:20191191::/home/user04:/bin/sh
user05:x:10024:20191191::/home/user05:/bin/sh
user06:x:10025:20191191::/home/user06:/bin/sh
user07:x:10026:20191191::/home/user07:/bin/sh
user08:x:10027:20191191::/home/user08:/bin/sh
user09:x:10028:20191191::/home/user09:/bin/sh
user10:x:10029:20191191::/home/user10:/bin/sh
(base) ubuntu@ubuntu:~$ id user01
用户id=10020(user01) 组id=20191191(stu) 组=20191191(stu)
(base) ubuntu@ubuntu:~$ su user01
密码：
$ exit
```

图 3-23　chpasswd 命令批量修改用户密码

打开 gedit 窗口后，输入以下 Shell 脚本内容：

```
#!/bin/bash
for  i  in  {01..10}
do
  userdel  user$i
done
```

保存并关闭窗口。然后输入以下命令：

```
sudo  bash  deluser.sh
```

此时即可删除以上创建的 10 个用户。

3.4.2　awk 命令列出系统用户

/etc/passwd 文件和/etc/group 文件中，各字段采用冒号作为分隔符。可以使用 awk 命令，并使用-F 参数指定冒号作为分隔符，列出系统中的所有用户名，或者某些用户名。

【例 3-24】 awk 命令列出当前系统的某些用户名。

输入以下命令：

```
awk  -F  ':'  '{print $1}'  /etc/passwd|grep 你的姓名
awk  -F  ':'  '{print $1}'  /etc/group|tail  -n4
```

以上命令的执行效果如图 3-24 所示。使用 awk -F 命令结合 grep 命令显示了包括 yujian 关键字的用户名，结合 tail -n4 命令显示了用户组账户信息文件最后 4 行的内容。

```
(base) ubuntu@ubuntu:~$ awk  -F  ':'  '{print $1}'  /etc/passwd | grep yujian
yujian1
yujian2
yujian6
(base) ubuntu@ubuntu:~$ awk  -F  ':'  '{print $1}'  /etc/group | tail  -n4
yujian1
teacher
stu
yujian6
```

图 3-24　awk 命令列出当前系统的某些用户名

3.4.3　修改用户名和主目录的方法和命令

当不满意安装时设定的用户名时，由于已经在该用户上做了很多配置并安装了很多软件，不希望再新建用户，这时最好在原来的基础上直接修改用户名。一个修改用户名和主目录的简单粗暴的方法是修改三个配置文件：/etc/passwd、/etc/shadow 和/etc/group，将这三个文件中的原用户名修改为现在需要设置的用户名，同时修改/etc/passwd 中的主目录。也可以综合使用多个命令来修改用户名和主目录。

【例 3-25】　修改用户名和主目录之简单粗暴法。

首先切换到 root 用户，然后创建用户 testuser，分别编辑以上三个配置文件，定位到文件内容的最后一行，将用户名 testuser 修改为“你的姓名 7”，其他内容不要修改，保存并关闭窗口。用户配置即可生效。输入以下命令：

```
su  root
useradd  -m  testuser
passwd  testuser
```

为了方便例 3-26 中的 john 软件破解，设置密码为弱口令：123456。

```
gedit  /etc/passwd
```

定位到最后一行，将 testuser 修改为“你的姓名 7”，保存并关闭窗口。

```
gedit  /etc/shadow
```

定位到最后一行，将 testuser 修改为你的姓名 7，保存并关闭窗口。

```
gedit  /etc/group
```

定位到最后一行，将 testuser 修改为你的姓名 7，保存并关闭窗口。

```
exit
su    你的姓名 7
exit
```

以上命令的执行效果如图 3-25 所示。将以上三个配置文件对应的用户名信息修改后，输入 su 命令切换到 yujian7，输入创建 testuser 用户时设置的密码 123456，即可成功切换。

```
(base) ubuntu@ubuntu:~$ su root
密码：
root@ubuntu:/home/ubuntu# useradd -m testuser
root@ubuntu:/home/ubuntu# passwd testuser
新的 密码：
重新输入新的 密码：
passwd：已成功更新密码
root@ubuntu:/home/ubuntu# gedit   /etc/passwd
root@ubuntu:/home/ubuntu# gedit   /etc/shadow
root@ubuntu:/home/ubuntu# gedit   /etc/group
root@ubuntu:/home/ubuntu# exit
exit
(base) ubuntu@ubuntu:~$ su yujian7
密码：
$
```

图 3-25　修改用户名

【例 3-26】 修改用户名和主目录之命令法。

本例综合使用多个命令修改用户名和主目录。输入以下命令：

```
sudo  useradd  -m  temp
sudo  passwd  temp
sudo  usermod  -l  你的姓名 8  temp
sudo  mv  /home/temp  /home/你的姓名 8
sudo  usermod  -d  /home/你的姓名 8  你的姓名 8
sudo  cat  /etc/passwd|grep 你的姓名 8
```

以上命令的执行效果如图 3-26 所示。从 3-26 中可以看出，首先，创建 temp 用户，使用 -m 参数创建对应的主目录/home/temp，并设置较复杂和难以破解的密码，例如，本书设置为 hstc；然后，使用 usermod－l 命令将 temp 用户名改为 yujian8，将主目录/home/temp 重命名为主目录/home/yujian8，使用 usermod -d 命令将 yujian8 用户的主目录设为/home/yujian8；最后，通过查看/etc/passwd 文件，可以发现 yujian8 的用户名和主目录都已经修改成功了。

```
(base) ubuntu@ubuntu:~$ sudo  useradd  -m  temp
[sudo] ubuntu 的密码：
(base) ubuntu@ubuntu:~$ sudo  passwd  temp
新的 密码：
重新输入新的 密码：
passwd：已成功更新密码
(base) ubuntu@ubuntu:~$ sudo  usermod  -l  yujian8  temp
(base) ubuntu@ubuntu:~$ sudo  mv  /home/temp  /home/yujian8
(base) ubuntu@ubuntu:~$ sudo  usermod  -d  /home/yujian8  yujian8
(base) ubuntu@ubuntu:~$ sudo  cat  /etc/passwd | grep yujian8
yujian8:x:10002:10002::/home/yujian8:/bin/sh
```

图 3-26　修改用户名和主目录

3.5　综合实例：使用 john 软件破解系统用户密码

/etc/passwd 存放的是用户账户信息，而/etc/shadow 存放的是用户的加密后密码信息。Linux 操作系统采用安全哈希算法(MD5、SHA1)等加密用户密码，使加密后的用户密

码不可逆向破解，即黑客无法从密文直接推导出明文。那么，如果想要破解 Linux 操作系统用户密码，只能采用字典攻击等蛮力破解方式了。

本综合实例中，首先编译 john 破解软件，生成其可执行文件，然后将用户名信息和用户密码信息重定向为一个新的文件，最后 john 软件通过字典模式破解。需要注意的是，编译 john 软件，需要安装 GCC 和 make。如果系统没有安装，可以输入以下命令进行安装：

```
sudo apt update
sudo apt install gcc
sudo apt install make
```

读者可以从本书的配套资源中下载 john -1.9.0.tar.gz，并复制至 Ubuntu 操作系统的 Downloads 目录下，然后输入以下命令：

```
cd  Downloads
tar  -xzvf  john-1.9.0.tar.gz
cd  john-1.9.0/src
make  clean  linux-x86-64
cd..
cd  run
sudo  ./unshadow  /etc/passwd  /etc/shadow > myshadow
```

以上命令的执行效果如图 3-27 所示。从图 3-27 中可以看出，将 john 软件使用 make 命令编译成功后，在其 run 目录下，使用超级用户权限和./执行 unshadow 程序，将/etc/passwd 和/etc/shadow 合成文件 myshadow。

```
(base) ubuntu@ubuntu:~$ cd Downloads/
(base) ubuntu@ubuntu:~/Downloads$ tar  -xzvf   john-1.9.0.tar.gz
(base) ubuntu@ubuntu:~/Downloads$ cd john-1.9.0/
(base) ubuntu@ubuntu:~/Downloads/john-1.9.0$ cd ..
(base) ubuntu@ubuntu:~/Downloads$ cd john-1.9.0/src
(base) ubuntu@ubuntu:~/Downloads/john-1.9.0/src$ make  clean  linux-x86-64
rm -f ../run/john ../run/unshadow ../run/unafs ../run/unique ../run/john.bin ../run/john.com ../run/unshadow.cc
m ../run/unafs.com ../run/unique.com ../run/john.exe ../run/unshadow.exe ../run/unafs.exe ../run/unique.exe
make[1]: 离开目录 "/home/ubuntu/Downloads/john-1.9.0/src"
(base) ubuntu@ubuntu:~/Downloads/john-1.9.0/src$ cd ..
(base) ubuntu@ubuntu:~/Downloads/john-1.9.0$ cd run
(base) ubuntu@ubuntu:~/Downloads/john-1.9.0/run$ sudo  ./unshadow  /etc/passwd  /etc/shadow > myshadow
```

图 3-27　编译 john 破解软件

接着，可以使用./执行 john 破解程序，采用字典模式去破解 myshadow 文件，最后显示破解结果。输入以下命令：

```
sudo  ./john  -w: password.lst  myshadow
sudo  ./john  -show  myshadow
```

以上命令的执行效果如图 3-28 所示。从图 3-28 中可以发现，由于在前面章节中是将各用户密码设置为弱口令，因此，使用 john 软件能够在比较短的时间内破解出大部分用户

的密码：yujian1 用户的密码为 654321，yujian2 用户的密码为 a12345，yujian6 用户没有密码(密码被删除)，yujian7 用户和 user01～user10 用户的密码为 123456。这个实例说明，如果将用户的密码设置为弱口令，是很容易被破解的。在日常工作中，设置密码最好包含字母、数字和特殊字符，这样安全性比较高，难以被破解。

```
(base) ubuntu@ubuntu:~/Downloads/john-1.9.0/run$ sudo  ./john  -w:password.lst  myshadow
Loaded 15 password hashes with 15 different salts (crypt, generic crypt(3) [?/64])
Remaining 2 password hashes with 2 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 100% 0g/s 636.6p/s 1273c/s 1273C/s !@#$%..sss
Session completed
(base) ubuntu@ubuntu:~/Downloads/john-1.9.0/run$ sudo  ./john  -show  myshadow
yujian1:654321:9999:1001::/home/yujian1:/bin/sh
yujian2:a12345:1002:27::/home/yujian2:/bin/sh
yujian6:NO PASSWORD:2019119101:1005::/home/yujian6:/bin/sh
user01:123456:10020:20191191::/home/user01:/bin/sh
user02:123456:10021:20191191::/home/user02:/bin/sh
user03:123456:10022:20191191::/home/user03:/bin/sh
user04:123456:10023:20191191::/home/user04:/bin/sh
user05:123456:10024:20191191::/home/user05:/bin/sh
user06:123456:10025:20191191::/home/user06:/bin/sh
user07:123456:10026:20191191::/home/user07:/bin/sh
user08:123456:10027:20191191::/home/user08:/bin/sh
user09:123456:10028:20191191::/home/user09:/bin/sh
user10:123456:10029:20191191::/home/user10:/bin/sh
yujian7:123456:10030:10030::/home/yujian7:/bin/sh

14 password hashes cracked, 2 left
```

图 3-28　破解用户密码结果

3.6　课后习题

一、填空题

1. 使用超级用户权限，添加一个名为 testuser 的用户，并为该用户创建用户主目录和登录 bash shell 的命令是_____。

2. 使用超级用户权限，设置用户 yy 的密码的命令是_____。

3. 使用超级用户权限，锁定用户 yy 的命令是_____。

4. 使用超级用户权限，解锁用户 yy 的命令是_____。

5. 使用超级用户权限，强制删除用户 yy，并且删除该用户文件夹的命令是_____。

6. 使用超级用户权限，添加用户 yy，并将其加入 sudo 超级用户组的命令是_____。

7. 使用超级用户权限，将已有用户 yy 附加到 sudo 组的命令是_____。

8. 使用超级用户权限，修改 teach 用户组名为 teacher 的命令是_____。

9. 使用超级用户权限，将 8888 作为用户组 ID，创建用户组 teach 的命令是_____。

10. 使用超级用户权限，修改 teacher 用户组 ID 为 6666 的命令是_____。

11. 使用超级用户权限，设定 teach 用户组的密码的命令是_____。

12. 使用超级用户权限，删除 teach 用户组的密码的命令是_____。

13. 使用超级用户权限，删除用户组名为 teacher 的命令是_____。

14. 在主目录上，分析并只提取出所有系统用户名的命令是_____。

15. 使用超级用户权限，直接修改用户 yy 的密码有效期为两次密码修改最小天数为 7 天，密码有效的最大天数为 30 天的命令是_____。

16. 用 cat 命令查看用户组名信息的命令是_____。

17. 使用超级用户权限和 cat 命令查看用户组影子文件的命令是_____。

18. 使用超级用户权限、john 软件和字典模式破解系统用户密码的命令是_____。提示：已经合成了用户信息和密码信息文件 xx，字典文件为 password.lst。

19. 修改已经创建用户的用户名，需要修改的三个配置文件分别是_____、_____和_____。

20. 使用超级用户权限，将用户名 xx 改为 yy 的命令是_____。

二、实操题

1. 批量删除例 3-23 所创建的 user01～user10 用户后，再批量添加 stu01～stu10 用户，同样指定所属的用户组为 stu。

2. 借鉴例 3-26 中的方法，使用 john 软件破解用户组密码。