窗体底端

用户及文件权限管理

实验介绍

1、Linux 中创建、删除用户，及用户组等操作。 2、Linux 中的文件权限设置。

一、Linux 用户管理

通过第一节课程的学习，你应该已经知道，Linux 是一个可以实现多用户登陆的操作系统，比如“李雷”和“韩梅梅”都可以同时登陆同一台主机，他们共享一些主机的资源，但他们也分别有自己的用户空间，用于存放各自的文件。但实际上他们的文件都是放在同一个物理磁盘上的甚至同一个逻辑分区或者目录里，但是由于 Linux 的 **用户管理** 和 **权限机制** ，不同用户不可以轻易地查看、修改彼此的文件。

下面我们就来学习一下 Linux 下的账户管理的基础知识。

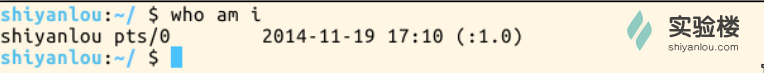
1.查看用户

请打开终端，输入命令：

$ who am i

或者

$ who mom likes



输入的第一列表示打开当前伪终端的用户的用户名（要查看当前登录用户的用户名，去掉空格直接使用 whoami 即可），第二列的pts/0 中 pts 表示伪终端，所谓伪是相对于 /dev/tty 设备而言的，还记得上一节讲终端时的那七个使用 [Ctrl]+[Alt]+[F1]～[F7] 进行切换的 /dev/tty 设备么,这是“真终端”，伪终端就是当你在图形用户界面使用 /dev/tty7 时每打开一个终端就会产生一个伪终端， pts/0 后面那个数字就表示打开的伪终端序号，你可以尝试再打开一个终端，然后在里面输入 who am i ，看第二列是不是就变成 pts/1 了，第三列则表示当前伪终端的启动时间。

who 命令其它常用参数

| **参数** |  | **说明** |
| --- | --- | --- |
| -a |  | 打印能打印的全部 |
| -d |  | 打印死掉的进程 |
| -m |  | 同am i,mom likes |
| -q |  | 打印当前登录用户数及用户名 |
| -u |  | 打印当前登录用户登录信息 |
| -r |  | 打印运行等级 |

2.创建用户

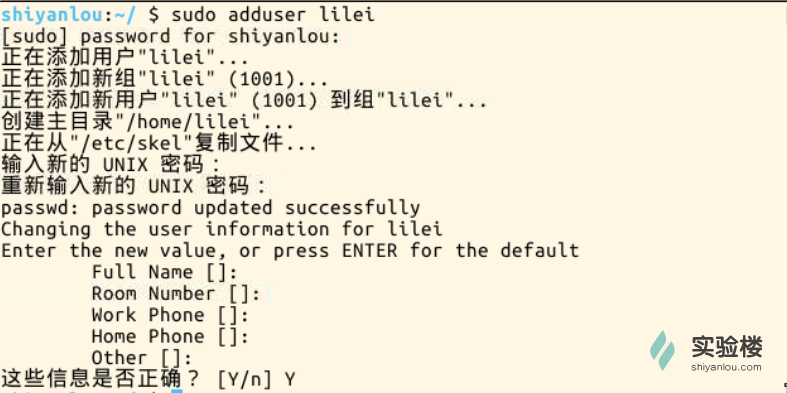
在 Linux 系统里， root 账户拥有整个系统至高无上的权利，比如 新建/添加 用户。

root 权限，系统权限的一种，与 SYSTEM 权限可以理解成一个概念，但高于 Administrator 权限，root 是 Linux 和 UNIX 系统中的超级管理员用户帐户，该帐户拥有整个系统至高无上的权力，所有对象他都可以操作，所以很多黑客在入侵系统的时候，都要把权限提升到 root 权限，用 Windows 的方法理解也就是将自己的非法帐户添加到 Administrators 用户组。更比如安卓操作系统中（基于 Linux 内核）获得 root 权限之后就意味着已经获得了手机的最高权限，这时候你可以对手机中的任何文件（包括系统文件）执行所有增、删、改、查的操作。

我们一般登录系统时都是以普通账户的身份登录的，要创建用户需要 root 权限，这里就要用到 sudo 这个命令了。不过使用这个命令有两个大前提，一是你要知道当前登录用户的密码，二是当前用户必须在 sudo 用户组。shiyanlou 用户的密码就是 “shiyanlou” ，它同时也属于 sudo 用户组（稍后会介绍如何查看和添加用户组）。现在我们新建一个叫 lilei 的用户：

$ sudo adduser lilei

按照提示输入 shiyanlou 密码（Linux 下密码输入通常都是不可见的），然后是给 lilei 用户设置密码，后面的选项的一些内容你可以选择直接回车使用默认值：

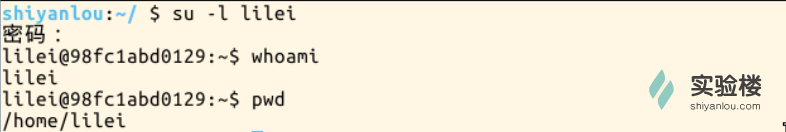


这个命令不但可以添加用户到系统，同时也会默认为新用户创建 home 目录：

$ ls /home

现在你已经创建好一个用户，并且你可以使用你创建的用户登录了，使用如下命令切换登录用户：

$ su -l lilei



退出当前用户跟退出终端一样可以使用 exit 命令或者使用快捷键 Ctrl+d。

3.用户组

在 Linux 里面每个用户都有一个归属（用户组），用户组简单地理解就是一组用户的集合，它们共享一些资源和权限，同时拥有私有资源，就跟家的形式差不多，你的兄弟姐妹（不同的用户）属于同一个家（用户组），你们可以共同拥有这个家（共享资源），爸妈对待你们都一样（共享权限），你偶尔写写日记，其他人未经允许不能查看（私有资源和权限）。当然一个用户是可以属于多个用户组的，正如你既属于家庭，又属于学校或公司。

在 Linux 里面如何知道自己属于哪些用户组呢？

方法一：使用groups命令

$ groups shiyanlou

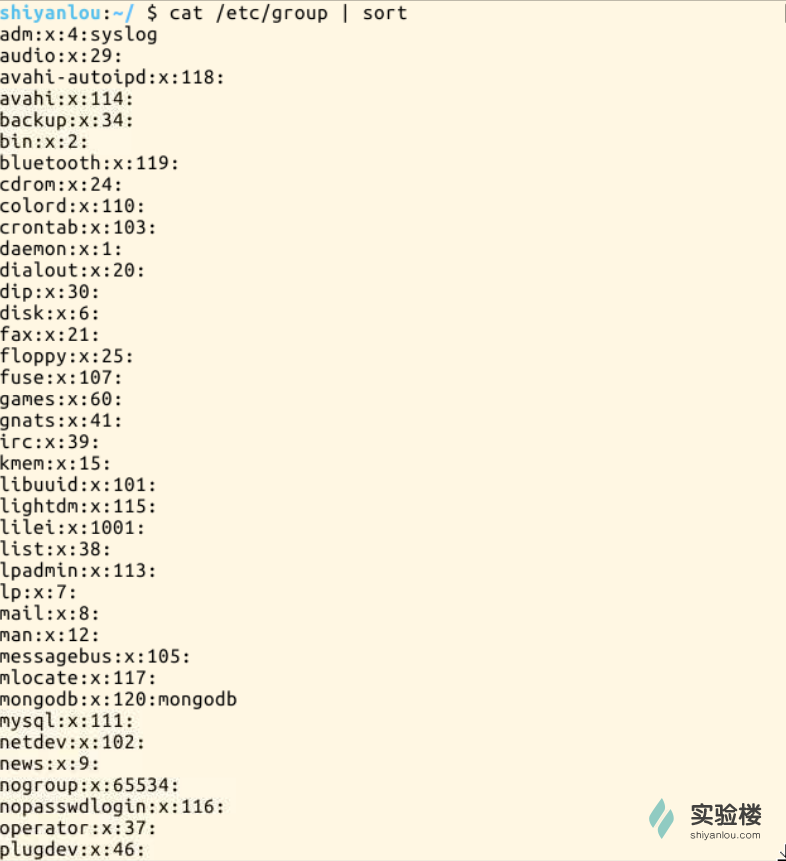
https://dn-anything-about-doc.qbox.me/linux_base/3-4.png/logoblackfont

其中冒号之前表示用户，后面表示该用户所属的用户组。这里可以看到 shiyanlou 用户同时属于 shiyanlou 和 sudo 用户组，每次新建用户如果不指定用户组的话，默认会自动创建一个与用户名相同的用户组（差不多就相当于家长的意思，或者说是老总）。默认情况下在sudo用户组里的可以使用sudo命令获得root权限。

方法二：查看/etc/group文件

$ cat /etc/group | sort

这里 cat 命令用于读取指定文件的内容并打印到终端输出，后面会详细讲它的使用。 | sort 表示将读取的文本进行一个字典排序再输出，然后你将看到如下一堆输出，你可以在最下面看到 shiyanlou 的用户组信息：



没找到，没关系，你可以使用命令过滤掉一些你不想看到的结果：

$ cat /etc/group | grep -E "shiyanlou|sudo"

etc/group 文件格式说明

/etc/group 的内容包括用户组（Group）、用户组口令、GID 及该用户组所包含的用户（User），每个用户组一条记录。格式如下：

group\_name:password:GID:user\_list

你看到上面的 password 字段为一个 'x' 并不是说密码就是它，只是表示密码不可见而已。

将其它用户加入 sudo 用户组

默认情况下新创建的用户是不具有 root 权限的，也不在 sudo 用户组，可以让其加入sudo用户组从而获取 root 权限。

$ su -l lilei

$ sudo ls

会提示 lilei 不在 sudoers 文件中，意思就是 lilei 不在 sudo 用户组中，至于 sudoers 文件（/etc/sudoers）你现在最好不要动它，操作不慎会导致比较麻烦的后果。

使用 usermod 命令可以为用户添加用户组，同样使用该命令你必需有 root 权限，你可以直接使用 root 用户为其它用户添加用户组，或者用其它已经在 sudo 用户组的用户使用 sudo 命令获取权限来执行该命令

这里我用 shiyanlou 用户执行 sudo 命令将 lilei 添加到 sudo 用户组，让它也可以使用 sudo 命令获得 root 权限

$ su shiyanlou

$ groups lilei

$ sudo usermod -G sudo lilei

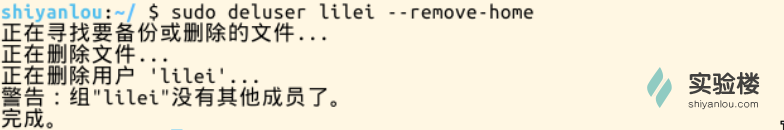
$ groups lilei

然后你再切换会 lilei 用户，现在就可以使用 sudo 获取 root 权限了。

4.删除用户

删除用户是很简单的事：

$ sudo deluser lilei --remove-home



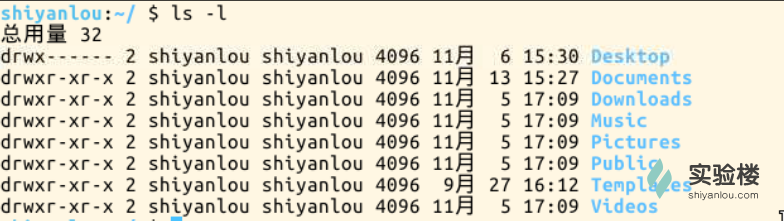
二、Linux 文件权限

1.查看文件权限

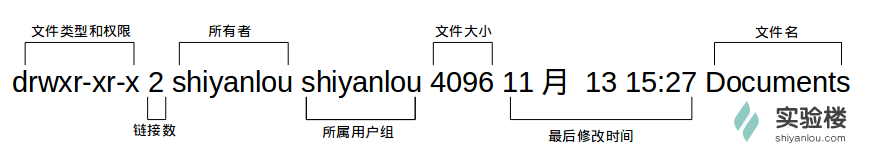
我们之前已经很多次用到 ls 命令了，如你所见，我们用它来列出并显示当前目录下的文件，当然这是在不带任何参数的情况下，它能做的当然不止这么多，现在我们就要用它来查看文件权限。

使用较长格式列出文件：

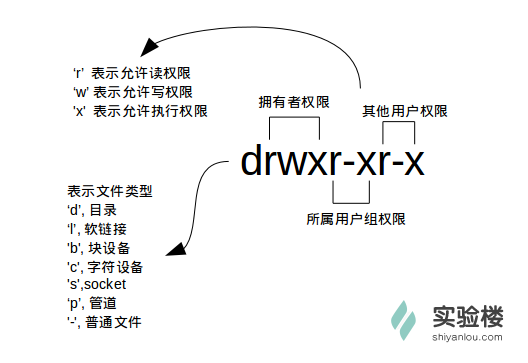
$ ls -l



你可能除了知道最后面那一项是文件名之外，其它项就不太清楚了，那么到底是什么意思呢：



可能你还是不太明白，比如第一项文件类型和权限那一堆东西具体指什么，链接又是什么，何为最后修改时间，下面一一道来：



* 文件类型

关于文件类型，这里有一点你必需时刻牢记**Linux 里面一切皆文件**，正因为这一点才有了设备文件（ /dev 目录下有各种设备文件，大都跟具体的硬件设备相关）这一说，还有 socket（网络套接字，具体是什么，感兴趣的用户可以自己去了解或期待实验楼的后续相关课程），和 pipe (管道，这个东西很重要，我们以后将会讨论到，这里你先知道有它的存在即可)。软链接文件，链接文件是分为两种的，另一种当然是“硬链接”(硬链接不常用，具体内容不作为本课程讨论重点，而软链接等同于 Windows 上的快捷方式,你记住这一点就够了）

* 文件权限

读权限，表示你可以使用 cat <file name> 之类的命令来读取某个文件的内容;写权限，表示你可以编辑和修改某个文件； 执行权限，通常指可以运行的二进制程序文件或者脚本文件，如同 Windows 上的 'exe' 后缀的文件，不过 Linux 上不是通过文件后缀名来区分文件的类型。你需要注意的一点是，**一个目录要同时具有读权限和执行权限才可以打开，而一个目录要有写权限才允许在其中创建其它文件**，这是因为目录文件实际保存着该目录里面的文件的列表等信息

所有者权限，这一点相信你应该明白了，至于所属用户组权限，是指你所在的用户组中的所有其它用户对于该文件的权限，比如，你有一个艾派德,那么这个用户组权限就决定了你的兄弟姐妹有没有权限使用它破坏它和占有它。

* 链接数

链接到该文件所在的 inode 结点的文件名数目（关于这个概念涉及到 Linux 文件系统的相关概念知识，不在本课程的讨论范围，感兴趣的用户可以自己去了解）。

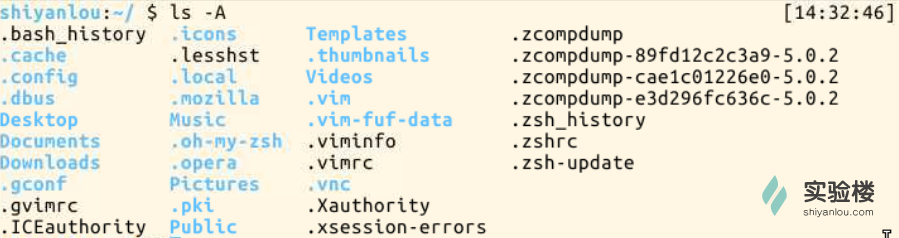
* 文件大小

以 inode 结点大小为单位来表示的文件大小，你可以给 ls 加上 -lh 参数来更直观的查看文件的大小。

明白了文件权限的一些概念，我们顺带补充一下关于 ls 命令的一些其它常用的用法：

* 显示除了 '.'(当前目录)，'..' 上一级目录之外的所有包含隐藏文件（Linux 下以 '.' 开头的文件为隐藏文件）

$ ls -A



当然，你可以同时使用 '-A' 和 '-l' 参数：

$ ls -Al

查看某一个目录的完整属性，而不是显示目录里面的文件属性：

$ ls -dl <目录名>

* 显示所有文件大小，并以普通人类能看懂的方式呈现：

$ ls -AsSh

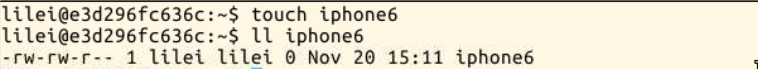
其中小 s 为显示文件大小，大 S 为按文件大小排序，若需要知道如何按其它方式排序，请使用“man”命令查询。

2.变更文件所有者

假设目前是 lilei 用户登录，新建一个文件，命名为 “iphone6”：

$ touch iphone6

可见文件所有者是 lilei ：



现在，使用以下命令变更文件所有者为 shiyanlou ：

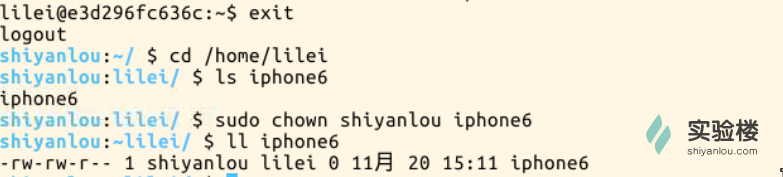
$ cd /home/lilei

$ ls iphone6

$ sudo chown shiyanlou iphone6

$ cp iphone6 /home/shiyanlou

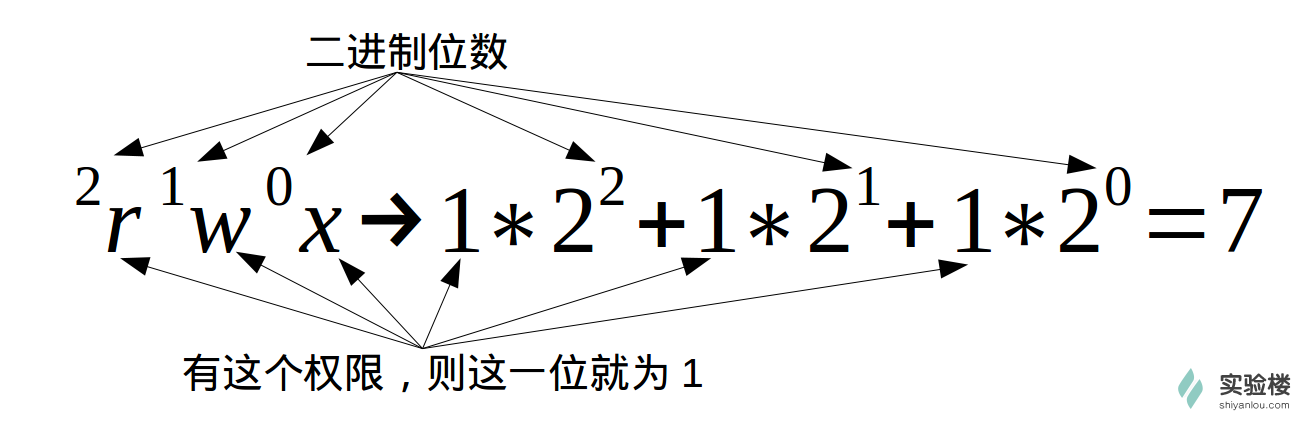
现在查看，发现 文件所有者成功修改为 shiyanlou ：



3.修改文件权限

如果你有一个自己的文件不想被其他用户读、写、执行，那么就需要对文件的权限做修改，这里有两种方式：

* 方式一：二进制数字表示



每个文件的三组权限（拥有者，所属用户组，其他用户,**记住这个顺序是一定的**）就对应这一个 "rwx"，也就是一个 '7' ,所以如果我要将文件“iphone6”的权限改为只有我自己可以用那么就这样:

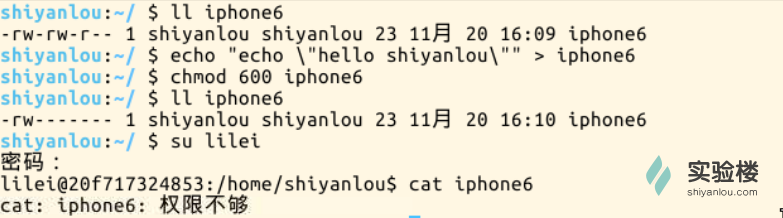
为了演示，我先在文件里加点内容：

$ echo "echo \"hello shiyanlou\"" > iphone6

然后修改权限：

$ chmod 700 iphone6

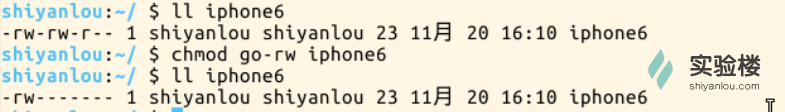
现在，其他用户已经不能读这个“iphone6”文件了：



* 方式二：加减赋值操作

完成上述相同的效果，你可以：

$ chmod go-rw Iphone



'g''o'还有'u'，分别表示group，others，user，'+'，'-' 就分别表示增加和去掉相应的权限。

三、更多

Linux 还有一些关于隐藏权限和特殊权限的内容，想全面了解 Linux 权限管理这部分内容的用户可以通过其他方式学习。

作业

添加一个用户loutest，使用sudo创建文件/opt/forloutest，设置成用户loutest可以读写。截图并把操作过程写入实验报告。