sudo 提权

su命令切换用户的时候，需要输入对方账户的密码，导致密码安全性不够

sudo：

某个用户能够以另外一个用户的身份通过某主机执行某命令，而不用输入对方账户密码

sudo 的配置文件 /etc/sudoers

每一行就定义了一个sudo的条目：

who which——hosts=（runas) TAG: command

基本配置格式

<user list> <host list> = <operator list> <tag list> <command list>

user list 用户/组，或者已经设置的用户的别名列表, 用户名直接 username，用户组加上%，比如%admin,

host list 主机名或别名列表

operator list runas用户，即可以以哪个用户、组的权限来执行

command list 可以执行的命令或列表

tag list 这个经常用到的是 NOPASSWD:，添加这个参数之后可以不用输入密码

别名机制：类似定义了一个组

4类别名：

用户别名： User_Alias

主机别名： Hosts_Alias

参照用户： Runas_Alias

命令别名： Cmnd_Alias

别名的名字只能使用大写的英文字母组合

别名：可使用！取反

User_Alias USERADMIN = 系统用户名 或 %组名 或用户别名

Hosts_Alias 主机名 IP 网络地址 其它主机名 可以嵌套

Runas_Alias 用户名 #UID 别名

Cmnd_Alias 命令绝对路径 目录（下面所有命令） 其它定义的命令别名

例子：定义hadoop用户可以以root用户的身份执行useradd 命令

/usr/sbin/useradd hadoop

sudo /usr/sbin/useradd hadoop

visudo

hadoop ALL=(root) /usr/sbin/useradd ,/usr/sbin/usermod

在第一次输入后，密码会被记录，5分钟内是有效的

sudo -k 取消密码记忆，必须再重新进行验证

sudo -l 列出当前用户所有可以使用的sudo类的命令

例子：

hadoop ALL=(root) NOPASSWD: /usr/sbin/useradd

, PASSWD: /usr/sbin/usermod

例子：

User_Alias USERADMIN = hadoop , %hadoop

Cdm_Alias USERADMINCMD = /usr/sbin/useradd,

/user/sbin/usermod,/usr/sbin/userdel,

/usr/bin/passwd [A-Za-z]*,! /usr/bin/passwd root

记录sudo日志到指定的文件：

编辑/etc/sudoers文件，添加如下行：

Defaults logfile=/var/log/sudo.log

Defaults !syslog

visudo -c 可以检查配置文件语法

课后综合练习题：

1、配置允许 juliet 用户可以通过 sudo 命令添加删除帐号，修改用户信息，但不能修改 root 用户的信息。

2、配置允许 romeo 用户通过 sudo 方式执行/sbin 和/user/sbin 目录下的所有命令，并且 不需要密码。

3、所有用户通过 sudo 执行的每一条命令，均以日志记录的形式写到文件/var/log/sudo 中。

4、将/etc 目录复制到/tmp 目录，并将/tmp/etc 目录及其子目录的权限修改为属主属组可读、可写、可执行，其他用户没有任何权限。

5、创建用户 zhukov 和组 ussr，并将 zhukov 用户加入到 ussr 组。将 /tmp/etc 目录及其子目录的属主修改为 zhukov，属组修改为 ussr。

6、 建立/share 目录，并设置该目录下新建的目录或文件只有属主才能删除。

7、创建/home/stooges 目录，创建 stooges 组，并将/home/stooges 的属组设置为 stooges 组。

8、为/home/stooges 目录添加一个 set GID 位，并设置权限为属主属组可读可写可执行， 其他用户没有任何权限。

9、 查看/home/stooges 目录的权限

10、创建目录/abc,将/abc 权限设置为 660。

11、设置 romeo 用户对/abc 有安全控制权限。

12、在不更/abc 目录现有归属的情况下，使 artists 组对该目录下现有文件和未来新建文件拥有完全控制权限