sudo 提权

一.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

useradd admin

sudo 的配置文件 /etc/sudoers

visudo

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：

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