Linux 用户管理

李 明

E-mail/QQ： samlee@lampbrother.net

课程大纲

- 用户管理配置文件
- 用户管理命令
- 用户组管理命令
- 批量添加用户
- 用户授权

配置文件

- 用户信息文件：/etc/passwd
- 密码文件：/etc/shadow
- 用户组文件：/etc/group
- 用户组密码文件：/etc/gshadow
- 用户配置文件：
  - /etc/login.defs
  - /etc/default/useradd
- 新用户信息文件：/etc/ske1
- 登录信息：/etc/motd /etc/issue

/etc/passwd文件格式

字　段	含 义
用户名	用户登录系统时使用的用户名
密码	密码位
UID	用户标识号
GID	缺省组标识号
注释性描述	例如存放用户全名等信息
宿主目录	用户登录系统后的缺省目录
命令解释器	用户使用的Shell，默认为bash

用户类型

Linux用户分为三种：

- 超级用户（root，UID=0）
- 普通用户（UID 500-60000）
- 伪用户（UID 1-499）

伪用户

1、伪用户与系统和程序服务相关

- bin、daemon、shutdown、halt等，任何Linux系统默认都有这些伪用户
- mail、news、games、apache、ftp、mysql及sshd等，与Linux 系统的进程相关

2、伪用户通常不需要或无法登录系统

3、可以没有宿主目录

用户组

- 每个用户都至少属于一个用户组
- 每个用户组可以包括多个用户
- 同一用户组的用户享有该组共有的权限

/etc/shadow文件格式

字　段	含　义
用户名	用户登录系统时使用的用户名
密码	加密密码
最后一次修改时间	用户最后一次修改密码的天数
最小时间间隔	两次修改密码之间的最小天数
最大时间间隔	密码保持有效的最多天数
警告时间	从系统开始警告到密码失效的天数
帐号闲置时间	帐号闲置时间
失效时间	密码失效的绝对天数
标志	一般不使用

/etc/group文件格式

字　段	含　义
组名	用户登录时所在的组
组密码	一般不使用
GID	组标识号
组内用户列表	属于该组的所有用户列表

手工添加用户

- 分别在/etc/passwd、/etc/group和/etc/shadow文件中添加一笔记录
- 创建用户宿主目录
- 在用户宿主目录中设置默认的配置文件
- 设置用户初始密码

SetUID

思考：为什么普通用户可以更改密码？

SetUID的定义：当一个可执行程序具有SetUID权限，用户执行这个程序时，将以这个程序所有者的身份执行。

范例：1、将touch命令授予SetUID权限

2、当vi命令被授予SetUID权限

3、查找SetUID程序：

find / -perm -4000 -o -perm -2000

添加用户

- useradd 设置选项 用户名 -D 查看缺省参数
  - u：UID
  - g：缺省所属用户组GID
  - G：指定用户所属多个组
  - d：宿主目录
  - s：命令解释器Shell
  - c：描述信息
  - e：指定用户失效时间
- passwd sam
- 手工添加用户

用户组管理命令

- 添加用户组 groupadd

  groupadd -g 888 webadmin

  创建用户组webadmin，其GID为888

- 删除用户组： groupdel 组名

- 修改用户组信息 groupmod

  groupmod -n apache webadmin

  修改webadmin组名为apache

用户组管理命令

- gpasswd 设置组密码及管理组内成员
  - -a 添加用户到用户组
  - -d 从用户组中删除用户
  - -A 设置用户组管理员
  - -r 删除用户组密码
  - -R 禁止用户切换为该组

修改用户信息

- usermod
  - usermod -G softgroup samlee

    将用户samlee添加到softgroup用户组中
  - usermod -l samlee -d /home/samlee -g lampbrother liming

    将用户liming的登录名改为samlee，加入到lampbrother组中，用户目录改为/home/samlee

用户管理命令

- pwck　检测/etc/passwd文件（锁定文件）
- vipw　编辑/etc/passwd文件
- id　　查看用户id和组信息
- finger　查看用户详细信息
- su　　切换用户（su - 环境变量切换）
- passwd -S　查看用户密码状态
- who、w　　查看当前登录用户信息

用户组管理命令

- groups　查看用户隶属于哪些用户组
- newgrp　切换用户组
- grpck　用户组配置文件检测
- chgrp　修改文件所属组
- vigr　编辑/etc/group文件（锁定文件）

用户组权限示例

授权用户jack和mary对目录/software有写权限

```
# groupadd softadm
# usermod -G softadm jack
# gpasswd -a mary softadm
# chgrp softadm /software
# chmod g+w /software
```

```
# ls -ld /software
drwxrwxr-x   2 root     softadm      512 Jul 14 06:17 /software
# grep softadm /etc/group
softadm::100:jack,mary
```

禁用和恢复用户

- 禁用

  # usermod -L username

  # passwd -l username

- 恢复

  # usermod -U username

  # passwd -u username

删除用户

userdel -r 用户名

-r：删除用户目录

手工删除：

使用find命令查找属于某个用户或用户组的文件

find选项-user、-uid、-group、-gid

1、对需要保留的文件进行移动和备份

2、对不需要的文件进行删除

3、清除用户文件中的相关表项

4、清除用户宿主目录

用户管理命令

- chage 设定密码
  - -l 查看用户密码设置
  - -m 密码修改最小天数
  - -M 密码修改最大天数
  - -d 密码最后修改的日期
  - -I 密码过期后，锁定账户的天数
  - -E 设置密码的过期日期，如果为0，代表密码立即过期；如果为-1，代表密码永不过期
  - -W 设置密码过期前，开始警告的天数

用户管理命令

- 启动或停用shadow功能

  pwconv/pwunconv

  grpconv/grpunconv
- system-config-users
- authconfig 、/etc/sysconfig/authconfig

批量添加用户

newusers命令 导入用户信息文件

pwunconv命令 取消shadow password功能

chpasswd 命令 导入密码文件

（格式 用户名:密码）

pwconv命令 将密码写入shadow文件

实例：一次批量添加10个用户

限制用户su为root：

```
# groupadd sugroup
# chmod 4550 /bin/su
# chgrp sugroup /bin/su
# ls -l /bin/su
-r-sr-x--- 1 root sugroup 18360 Jan 15 2010 /bin/su
```

设定后，只有sugroup组中的用户可以使用su切换为root

```
# useradd helen
# passwd helen
# usermod -G sugroup helen
```

用sudo代替su：

- 一在执行sudo命令时，临时成为root
- 一不会泄漏root口令
- 一仅向用户提供有限的命令使用权限

配置文件：/etc/sudoers，编辑配置文件命令visudo，普通用户使用命令sudo。

格式： 用户名（组名） 主机地址=命令（绝对路径）

John the ripper 应用：

```
# tar -xzvf john-1.7.6.tar.gz
# cd john-1.7.6/run
# make
```

破解用户liming密码

```
# grep liming /etc/passwd > /test/liming.passwd
# grep liming /etc/shadow > /test/liming.shadow
# /test/john-1.6.6/run/unshadow /test/liming.passwd
    /test/liming.shadow > /test/liming.john
# /test/john-1.6.6/run/john /test/liming.john
```

下载地址 http://www.openwall.com/john/


Thanks
技术交流 http://www.lampbrother.net/linux.php
视频下载 http://www.lampbrother.net/video.html