用户管理

• chage --help

–选项：

-d, --lastday 最近日期 将最近一次密码设置时间设为“最近日期”

-E, --expiredate 过期日期 将帐户过期时间设为“过期日期”

-l , --list 查看用户信息

-h, --help 显示此帮助信息并推出

#密码: SHA512加密算法

• passwd

选项: -l, --lock 锁定指名帐户的密码(仅限 root 用户)

-u, --unlock 解锁指名账户的密码(仅限 root 用户)

-S, --status 查看用户密码状态(只有根用户才能进行此操作)

shadow中: 密码为”!!”是不能登录

• 用户默认信息:

/etc/login.defs

• 版本信息

/etc/issue

–\S: 获取操作系统版本

#隐藏版本号: 把内容改成不相关的东西(随便改)

##################################################################

锁定/解锁保护文件

–对管理员也有效

????????

• 查看特殊属性

–lsattr 文件

• 添加特殊属性

–chattr 选项 文件

选项:

控制方式: +, -,=

a: 仅可追加(echo ??? >> file)

I : 不可变(不可删,改,什么都不能做)

RHEL6/7的区别

RHEL6 chkconfig httpd on|off #开机自启(6里没有systemctl)

service httpd start|stop......

RHEL7 systemctl enable|disable httpd

systemctl start|stop..... httpd

########################################################################

**su命令**

• su [-] [用户]

• su [-] -c “命令” [用户]

–”-c”: 切换到用户后执行的命令

–带”-”: 切换用户同时切换系统环境

–不带”-”: 仅切换用户

]$su #不指定用户默认为root

]#

• 安全日志文件: /var/log/secure

–记录了su - ,或su - root等

**提权(sudo)**

–系统的root用户,配置系统的普通用户,有执行自身命令的权限

• 普通用户执行提权命令

sudo 提权命令

• 普通用户查看可以执行提权命令

sudo -l (必须输入自己登录系统的密码才能查看)

• 主配置文件: /etc/sudoers

打开方式:

visudo(无颜色) 或 vim

提权格式:

普通用户 主机名列表=命令列表 (**必须写命令的绝对路径**)

%用户组 ALL=(ALL) ALL ??????

“\*”: 所有

“!”: 取反

强制保存: wq**!**

#注释掉改行,bug

99 %wheel ALL=(ALL) ALL #在wheel组的成员有所有权限

NOPASSWD ?????????????

**启用日志文件,记录用户的提权操作**

#写在文件末尾

Defaults logfile="/var/log/sudo"

写完后不会立即生成文件,需切换用户,sudo -l 一下

]#tail -f /var/log/sudo

**sudo别名设置**

#配置文件里写

User\_Alias 名字=用户名

Host\_Alias 名字=内容

Cmnd\_Alias 名字=命令绝对路径

################################################################################

**SSH访问控制**

–默认允许使用本机所有用户登录本机

• 服务名: sshd

• 配置文件: /etc/ssh/sshd\_config

基本安全设置

/etc/ssh/sshd\_config

–Port 3389 #改用非标准端口号

–Protocol 2 #启用SSH V2版协议

–ListenAddress IP #

–PermitRootLogin no #禁止root登录

–UseDNS no #不解析客户机地址

–LoginGraceTime 1m #登录时限(超出最多认证次数后,所长时间才能再认证)

–MaxAuthTries #每连接最多认证次数(经常与登录时限连用)

重启

sshd黑白名单

白名单: **只允许**使用**白名单**列表里的本地用户连接ssh服务

黑名单: 仅仅不允许黑名单列表里的用户连接ssh服务

黑白名单不能同时用,会冲突

/etc/ssh/sshd\_config

*写在末尾行*

白: ALLowUsers 用户名 用户名@Host #仅仅允许Host使用”用户名”连接本机

黑: DenyUsers 用户名 用户名@Host

DenyGroups 组 组

ALLowGroups 组 组

重启

口令(密码),密钥验证

65 PasswordAuthentication yes #口令

43 PubkeyAuthentication yes #打开注释

47 AuthorizedKeysFile .ssh/authorized\_keys

id\_rsa: 私钥

id\_sa.pub: 公钥

ssh-keygen

可以手动指定算法: -t rsa

-t dsa

###################################################################################

SElinux

• 配置文件: /etc/selinux/conf

sestatus 查看SElinux状态

touch /.autorelabel

/sys/fs/selinux/

安全上下文

–为目录/文件/设备标记访问控制属性

• 查看: -Z

]#ls -ldZ /etc

]#ps aux -Z

• 属性构成:

–用户:角色:访问类型:选项.....

–system\_u:object\_r:etc\_t:s0

• 一般操作

–移动的文件,原有的上下文属性不变

–复制,创建的文件,自动继承目标位置的上下文