

实验 9 Linux账户和登录安全运维实验

1 实验目的

掌握加固 Linux 账户安全的的基本方法

2 实验内容

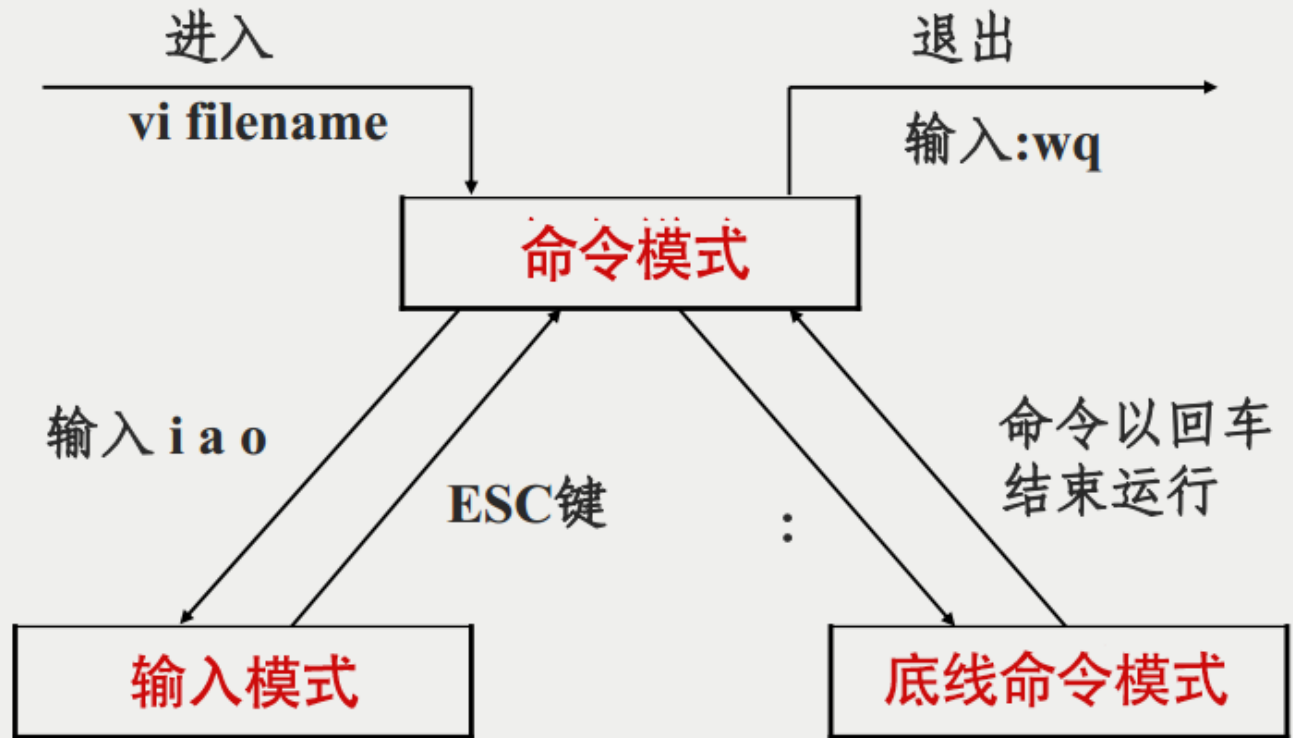
- 删除特殊的用户和用户组
- 关闭系统不需要的服务
- 密码安全策略
- 合理使用su，sudo命令
- 删减系统登录欢迎信息
- 禁止 Control-Alt-Delete 键盘关闭命令

3 实验前提

- 准备好 ubuntu server 1604 虚拟机的克隆版本
- 编辑系统文件可以使用nano或vi工具

如果对vi/vim编辑器不熟悉，可以参考下图：

Vim/Vi 工作模式



vi / vim 键盘图

Esc

命令
模式

~ 转换 大小写	! 外部 过滤器	@ 运行 宏	# prev ident	\$ 行尾	% 括号 匹配	^ "软" 行首	& 重复 :s	* next ident	(句首) 下一 句首	"soft" bol down	+ 后一行 行首
. 跳转到 标注	1	2	3	4	5	6	7	8	9	0 "硬" 行首	- 前一行 行首	= 自动 ³ 格式化
Q 切换至 ex模式	W 下一 单词	E 词尾	R 替换 模式	T back 'till	Y 拷贝 行	U 撤消 行内命令	I 到行首 插入	O 分段 (前)	P 粘贴 (前)	{ 段首	}	段尾
q 录制 宏	w 下一 单词	e 词尾	r 替换 字符	t 'till	y 拷贝 ^{1,3}	u 撤消 命令	i 插入 模式	o 分段 (后)	p 粘贴 ¹ (后)	[杂项]	杂项
A 在行尾 附加	S 删除行 并插入	D 删除 至行尾	F 行内字符 反向查找	G 文尾/ 行号	H 屏幕 顶行	J 合并 两行	K 帮助	L 屏幕 底行	:	ex 命令	" 寄存器 ¹ 标识	行首/ 列
a 附加	s 删除字符 并插入	d 删除 ^{1,3}	f 行内字符 查找	g 附加 ⁶ 命令	h ←	j ↓	k ↑	l →	;	重复 u/T/f/F	' 跳转到标 注的行首	\ 未用!
Z 退出 ⁴	X 退格	C 修改 至行末	V 可视 行模式	B 前一 单词	N 查找 上一处	M 屏幕 中间行	< 反缩进 ³	> 缩进 ³	?	向前 搜索		
Z 附加 命令 ⁵	x 删除 (字符)	c 修改 ^{1,3}	v 可视 模式	b 前一 单词	n 查找 下一处	m 设置 标注	, 反向 u/T/f/F	.	重复 命令	/	向后 搜索	

动作 移动光标, 或者定义操作的范围

命令 直接执行的命令,
红色命令 进入编辑模式

操作 后面跟随表示操作范围的指令

extra 特殊功能,
需要额外的输入

q 后跟字符参数

w,e,b命令

小写(b): quux(foo, bar, baz);
大写(B): quux(foo, bar, baz);

主要ex命令:

:w (保存), :q (退出), :q! (不保存退出)
:e f (打开文件 f),
:%s/x/y/g ('y' 全局替换 'x'),
:h (帮助 in vim), :new (新建文件 in vim),

其它重要命令:

CTRL-R: 重复 (vim),
CTRL-F/-B: 上翻/下翻,
CTRL-E/-Y: 上滚/下滚,
CTRL-V: 块可视模式 (vim only)

可视模式:

漫游后对选中的区域执行操作 (vim only)

备注:

- (1) 在 拷贝/粘贴/删除 命令前使用 "x (x=a..z,*)"
使用命令的寄存器('剪贴板')
(如: "ay\$ 拷贝剩余的行内容至寄存器 'a')"
- (2) 命令前添加数字
多遍重复操作
(e.g.: 2p, d2w, 5i, d4j)
- (3) 重复本字符在光标所在行执行操作
(dd = 删除本行, >> = 行首缩进)
- (4) ZZ 保存退出, ZQ 不保存退出
- (5) zt: 移动光标所在行至屏幕顶端,
zb: 底端, zz: 中间
- (6) gg: 文首 (vim only),
gf: 打开光标处的文件名 (vim only)

原图: www.viemu.com 翻译: fdl (linuxsir)

4 实验步骤

4.1 一.删除特殊的用户和用户组

1.使用下列命令查看当前用户列表

```
sudo less /etc/passwd
```

结果大致如下：

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/
sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/syste
md:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/
netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/b
in/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/fa
lse
syslog:x:104:108:./home/syslog:/bin/false
_apt:x:105:65534:./nonexistent:/bin/false
messagebus:x:106:110:./var/run/dbus:/bin/false
uidd:x:107:111:./run/uidd:/bin/false
leo:x:1000:1000:ubuntu server 1604,,,:/home/leo:/bin/bash
sshd:x:108:65534:./var/run/sshd:/usr/sbin/nologin
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false

```

2.使用下列命令删除不需要的用户

```
sudo userdel -r <用户名>
```

说明：用户名可以从下列列表选取。

不需要的用户大致有：

- adm
- lp
- sync
- shutdown

- halt
- news
- uucp
- operator
- games
- gopher

3.使用下列命令删除不需要的用户组

```
sudo groupdel <用户组名>
```

说明：用户组名可以从下列列表选取。

不需要的用户大致有：

- adm
- lp
- news
- uucp
- games
- dip
- pppusers
- popusers
- slipusers

二.关闭不必要的服务

1.查看当前系统服务列表

- 老版本初始化系统、系统管理器 (System V) 使用下列命令

`sudo service --status-all | more`，显示结果前为+，表示已启动，为-表示未启动。

- 新版本系统管理器 (systemd) 使用下列命令

```
sudo systemctl list-unit-files --type servic
```

使用下列命令查看当前运行的服务：

```
sudo systemctl | grep running
```

使用下列命令查看启动加载服务

```
sudo systemctl list-unit-files | grep enabled
```

2.使用下列命令关闭不必要的某个服务

先安装工具 `sudo apt install sysv-rc-conf`

然后执行：

```
sudo cp /usr/sbin/sysv-rc-conf /usr/sbin/chkconfig
```

```
sudo chkconfig --level 345 <服务名> off
```

服务名可从下列表中任选一个。

- **anacron**
 - 用来保证在系统关机时错过的定时任务可以在系统开机之后在执行
- **auditd**
 - 审计工具，常用来对文件修改进行监听
- **autofs**
 - 实现光驱，软盘等的动态自动挂载
- **avahi-daemon**
 - 运行在客户机上实施查找基于网络的Zeroconf service的服务守护进程。
 - 该服务可以为Zeroconf网络实现DNS服务发现及DNS组播规范。
- **avahi-dnssconfd**
 - 在没有 DNS 服务的局域网里发现基于 zeroconf 协议的设备和服务，与Bonjour类似
- **bluetooth**
- **cpuspeed**
- **firstboot**
 - Fedora系统的特有的调度任务
 - Fedora系统第一次启动时，执行一次特定任务
- **gpm**
 - 终端鼠标指针支持（无图形界面）
- **haldaemon**
 - 维护连接到系统的设备的数据库
- **hidd**
 - 管理所有可见的蓝牙设备
 - 维护键盘/鼠标等蓝牙输入设备
- **ip6tables**
 - IPv6软件防火墙
- **ipsec**
 - IPSec虚拟专用网络
- **isdn**

- 专用数字线路，一种互联网的接入方式
- lpd
 - 打印机管理程序
- mcstrans
 - SELinux内核安全套件
- messagebus
 - 进程间通讯服务，与 DBUS 交互
- netfs
 - 自动挂载网络中的共享文件空间
- nfs
 - 标准文件共享方式
- nfslock
- nscd
 - 用户/用户组/DNS解析缓存服务
- pcscd portmap
 - 提供智能卡读卡器支持
- readahead_early
 - 预先加载特定的应用到内存中以提供性能
- restorecond
 - 给 SELinux 监测和重新加载正确的文件上下文
- rpcgssd
 - NFS v4
- rpcidmapd
 - NFS v4
- rstatd
 - 系统内核性能统计
- sendmail
 - IMAP/POP3邮件工具
- setroubleshoot
 - 服务器安全审计工具，从CentOS 6.x开始合并入auditd
- yppasswdd ypserv
 - 用于NIS用户修改服务器端的密码

3.重启系统

三.密码安全策略

1.使用下列命令查看系统账户登录安全策略。

```
less /etc/login.defs
```

2.使用下列命令编辑上述文件，增加下列内容。

```
vi /etc/login.defs
```

```
#在文件中找到 PASS_MAX_DAYS 所在行，修改为30天：
```

```
PASS_MAX_DAYS 30
```

```
#在文件中找到 PASS_MIN_DAYS 所在行，修改为7天：
```

```
PASS_MIN_DAYS 7
```

```
#在文件中找到 PASS_MIN_LEN 所在行，修改为10字符：
```

```
PASS_MIN_LEN 10
```

```
#在文件中找到 PASS_WARN_AGE 所在行，修改为7天：
```

```
PASS_WARN_AGE 7
```

3.使用下列命令设置账户规则，注销长期不活动(以60天为例)的账户。

```
sudo useradd -D -f 60
```

4.使用下列查看当前pam下有的配置文件

```
ls /etc/pam.d/
```

5.使用下列命令编辑密码策略文件

```
#Debian、Ubuntu 或 Linux Mint 系统上
```

```
sudo vi /etc/pam.d/common-password
```

```
#打开密码策略文件后，找到或添加内容：
```

```
#表示禁止使用最近用过的5个密码（已用密码保存在 /etc/security/opasswd）
```

```
password [success=1 default=ignore] pam_unix.so obscure sha512 remember=5
```

此外，如果你的系统是其它版本linux，可用下列命令：

```
#CentOS、Fedora、RHEL 系统上
```

```
sudo vi /etc/pam.d/system-auth
```

```
#打开密码策略文件后，找到或添加内容：
```

```
password sufficient pamunix.so sha512 shadow nullok tryfirstpass useauthtok remember=5
```

4.2 五.合理使用su， sudo命令

1.使用下列命令打开/etc/sudoers文件

```
sudo vi /etc/sudoers
```


然后，在文件中键入如下内容：

```
leo ALL = (ALL) NOPASSWD : ALL
```

4.3 六.删减系统登录欢迎信息

1.使用xshell连接ubuntu server

2.打开或新建/etc/motd文件

```
sudo vi /etc/motd
```

3.在打开的文件中复制以下内容

```
Welcome
```

```
.,="",.
 / _ _ \
 | d b |
 \ / \ /
 ,/'-=-\/'-'\,
 / /      \ \
 | /        \ |
 \ \      / \
  '.      .'
  _|`~~`|_
  /\    /\
```

4.重启服务器，验证是否有开机欢迎词及ASCII图。

4.4 七.禁止 Control-Alt-Delete 键盘关闭命令

1.由于ubuntu 1604采用了systemd系统管理，所以需要在命令行下执行下列操作：

```
sudo systemctl mask ctrl-alt-del.target
```

2.重启系统后台管理进程

```
sudo systemctl daemon-reload
```

如果你的系统是老的系统管理器system v，使用下列方法:

1.打开/etc/init/control-alt-delete.conf文件

```
sudo vi etc/init/control-alt-delete.conf
```

2.注释掉文件中的下列内容：`exec /sbin/shutdown -r now Control-Alt-Delete pressed"`