# 一.账号和口令

## 1.禁用或删除无用账号

减少系统无用账号，降低安全风险。

**操作步骤**

* 使用命令“userdel <用户名>” 删除不必要的账号
* 使用命令“passwd -l <用户名>”锁定不必要的账号
* 使用命令“passwd -u <用户名>”解锁不必要的账号

## 2.检查特殊账号

检查是否存在空口令和root权限的账号。

**操作步骤**

查看空口令和root权限账号，确认是否存在异常账号：

使用命令“awk -F: ‘($2==””)’ /etc/shadow”查看空口令账号使用命令“awk -F: ‘($3==0)’ /etc/passwd”查看UID为零的账号

加固：

* 使用命令“passwd <用户名>”为空口令账号设定密码
* UID为零的账号应该只有root

## 3.添加口令策略

加强口令的复杂度等，降低被猜解的可能性

**操作步骤：**

1. 1.使用命令“vi /etc/login.defs”修改配置文件
2. PASS\_MAX\_DAYS 90 #新建用户的密码最长使用天数
3. PASS\_MIN\_DAYS 0 #新建用户的密码最短使用天数PASS\_WARN\_AGE 7 #新建用户的密码到期提前提醒天数
4. 使用chage命令修改用户设置，例如：
5. chage -m 0 -M 30 -E 2000-01-01 -W 7 <用户名>
6. 表示：将此用户的密码最长使用天数设为30，最短使用天数设为0，密码2000年1月1日过期，过期前7天里警告用户
7. 2.设置连续输错3次密码，账号锁定5分钟，
8. 使用命令“vi /etc/pam.d/common-auth”修改配置文件，添加
9. auth required pam\_tally.so onerr=fail deny=3 unlock\_time=300

## 4.限制用户su

限制能su到root的用户

**操作步骤**

1. 使用命令“vi /etc/pam.d/su”修改配置文件，添加行
2. 例如：只允许test组用户su到root
3. auth required pam\_wheel.so group=test

# 二.服务

## 1.关闭不必要的服务

关闭不必要的服务（普通服务和xinetd服务），降低风险。

**操作步骤**

使用命令“chkconfig —level <服务名> on|off|reset”设置服务在个init级别下开机是否启动

## 2.SSH服务安全

对SSH服务进行安全加固，防止暴力破解成功。

**操作步骤**

使用命令“vim /etc/ssh/sshd\_config”编辑配置文件

* （1）不允许root账号直接登录系统

设置“PermitRootLogin ”的值为no

* （2）修改SSH使用的协议版本

设置“Protocol”的版本为2

* （3）修改允许密码错误次数（默认6次）

设置“MaxAuthTries”的值为3

修改完毕后重启sshd服务生效。

# 三.文件系统

## 1.设置umask值

设置默认的umask值，增强安全性

**操作步骤**

使用命令“vi /etc/profile”修改配置文件，添加行“umask 027”， 即新创建的文件属主读写执行权限，同组用户读和执行权限，其他用户无权限，使用命令“umask 027”应用设置

## 2.设置登录超时

设置系统登录后，连接超时时间，增强安全性.

**操作步骤**

使用命令“vi /etc/profile”修改配置文件，添加“TMOUT=”行开头的注释，设置为“TMOUT=180”，即超时时间为3分钟

# 四.日志日志

## 1.syslogd日志

启用日志功能，并配置日志记录。

**操作步骤**

Linux系统默认启用以下类型日志：

* 系统日志（默认）/var/log/messages
* cron日志（默认）/var/log/cron
* 安全日志（默认）/var/log/secure

注：部分系统可能使用syslog-ng，配置文件：/etc/syslog-ng/syslog-ng.conf

用户可以根据需求配置详细日志。

## 2.记录所有用户的登录和操作日志

通过脚本代码来实现记录所以用户的登录操作日志，防止出现安全事件后无据可查。

**操作步骤**

1. [root@xxx /]# vim /etc/profile
2. history
3. USER=`whoami`
4. USER\_IP=`who -u am i 2>/dev/null| awk '{print $NF}'|sed -e 's/[()]//g'`
5. if [ "$USER\_IP" = "" ]; then
6. USER\_IP=`hostname`
7. fi
8. if [ ! -d /var/log/history ]; then
9. mkdir /var/log/history
10. chmod 777 /var/log/history
11. fi
12. if [ ! -d /var/log/history/${LOGNAME} ]; then
13. mkdir /var/log/history/${LOGNAME}
14. chmod 300 /var/log/history/${LOGNAME}
15. fi
16. export HISTSIZE=4096
17. DT=`date +"%Y%m%d\_%H:%M:%S"`
18. export HISTFILE="/var/log/history/${LOGNAME}/${USER}@${USER\_IP}\_$DT"
19. chmod 600 /var/log/history/${LOGNAME}/\*history\* 2>/dev/null
20. [root@xxx /]# source /etc/profile 加载配置生效
21. 注释： /var/log/history这是记录日志的存放位置，可以自定义。

通过以上方式就可以在/var/log/history下会以每个用户为名新建一个文件夹，每次用户退出后都会产生以用户名、登录IP、时间的文件，里面包含此用户本次的所以操作（root用户除外）。

同时建议您使用OSS服务收集存储日志。