LINUX 加固手册

一、修改密码策略

1、cp /etc/login.defs /etc/login.defs.bak

2、vi /etc/login.defs

```
PASS_MAX_DAYS   90  （用户的密码不过期最多的天数）
PASS_MIN_DAYS   0  （密码修改之间最小的天数）
PASS_MIN_LEN    8  （密码最小长度）
PASS_WARN_AGE   7  （口令失效前多少天开始通知用户更改密码）
```

按要求修改这几个密码选项，修改完之后保存（：wq!）退出即可。

二、查看系统是否已设定了正确UMASK值（022）

1、用命令umask查看umask值是否是 022，

如果不是用下面命令进行修改：

cp /etc/profile /etc/profile.bak

vi /etc/profile

找到 umask 022，修改这个数值即可。

三、锁定系统中不必要的系统用户和组

1、cp /etc/passwd /etc/passwd.bak

cp /etc/shadow /etc/shadow.bak

锁定下列用户

```
2、for i in adm lp sync news uucp games ftp rpc rpcuser nfsnobody mailnull gdm
do
usermod -L $i
done
```

3、检查是否锁定成功

more /etc/shadow 如 ：lp:!*:13943:0:99999:7::: lp帐户后面有! 号为已锁定。

4、禁用无关的组：

备份：

cp /etc/group /etc/group.bak

5、编辑： vi /etc/group

在组前面 加#进行注释 参考下面

#lp:x:7:daemon,lp
#uucp:x:14:uucp
#games:x:20:
#ftp:x:50:
#rpc:x:32:
#rpcuser:x:29:
#nfsnobody:x:65534:
#mailnull:x:47:
#gdm:x:42:

6、禁止root用户远程登录

cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
vi /etc/ssh/sshd_config文件，将其中的PermitRootLogin改成no，然后重新启动ssh服务
/etc/init.d/sshd restart

四、linux中预防SYN flood

1、备份 cp /etc/sysctl.conf /etc/sysctl.conf.bak
2、编辑vi /etc/sysctl.conf

3、添加 net.ipv4.tcp_syncookies = 1

4、保存退出
5、/sbin/sysctl -p 命令使变更生效

五、ARP捆绑IP

1、确认网关IP 和 mac 地址是正确的

2.查看 arp -a

3. echo '210.75.211.254 00:17:0E:5A:AE:C6' > /etc/ethers
4.捆绑 arp -f
5、对比
例子：（请参考系统运行的实际情况）
捆绑前root@beijing238 etc]# arp -a
? (210.75.211.254) at 00:17:0E:5A:AE:C6 [ether] on eth0

捆绑后

? (210.75.211.254) at 00:17:0E:5A:AE:C6 [ether] PERM on eth0

6、设置开机捆绑MAC
备份 开机自启动服务文件cp /etc/rc.d/rc.local /etc/rc.d/rc.local.bak

编辑vi /etc/rc.d/rc.local 添加 arp -f

六、停止无用服务

注意：需要根据系统的实际情况和询问管理员那些服务跟业务无关方可停用。

```
for i in  autofs chargen chargen-udp gpm ip6tables isdn kudzu xinetd nfs nfslock pcmcia
rhnsd
do
```

```
chkconfig --level 2345 $i off
service $i stop
done
```

启动审计服务

```
for i in  audit
do
```

```
chkconfig --level 2345 $i on
service $i start
done
```

七、系统禁用X-Window系统

1、编辑 ：
cp /etc/inittab /etc/inittab.bak
vi /etc/inittab
id:5:initdefault：将数值5改为3即可。

八、残留信息保护（使.bash_history值保存30个命令，用户退出是自动删除.bash_history文件）

1、 备份：cp /etc/profile /etc/profile.bak
2、 编辑 vi /etc/profile
HISTFILESIZE=30 （如果没有请自行添加） 修改保存值为30
HISTSIZE=30 修改保存值为30
3、 退出后自动删除个用户的".bash_history"文件

备份：cp /etc/skel/ .bash_logout /etc/skel/ .bash_logout.bak
编辑： vi /etc/skel/ .bash_logout
在后面添加 rm -f $HOME/.bash_history

more /etc/sysctl.conf

九、查看/tmp和/var/tmp目录具有粘滞位

1、查看，例如： ls -al / | grep tmp
drwxrwxrwt 7 root
2、修改：chmod +t /tmp
chmod +t /var/tmp

十、加固TCP/IP协议栈

1、系统当前状态
more /etc/sysctl.conf
检查/etc/sysctl.conf 是否存在以下内容：
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0

2、Vi /etc/sysctl.conf 文件添加或修改下列值。
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0

```
chown root:root /etc/sysctl.conf
chmod 0600 /etc/sysctl.conf
sysctl -p /etc/sysctl.conf
```

注意：修改前请备份/etc/sysctl.conf文件，如果对上面参数不清楚的请找相关资料了解。这些参数应依据实际业务的需要来微调，具体请咨询厂商与业务开发商。

十一、 系统重要文件访问权限是否为644或600

一般检查/etc/passwd 、/etc/shadow 文件

默认配置如下（可参照此）：

ls -al /etc/passwd /etc/shadow

修改方法：chmod 644 /etc/shadow

Chmod 600 /etc/passwd

十二、系统是否启用安全审计

用命令查看chkconfig --list | grep auditd

例如：

[root@linux ~]# chkconfig --list | grep auditd

auditd 0:off 1:off 2:on 3:off 4:on 5:off 6:off

root@linux ~]# service auditd status

auditd is stopped

[root@linux ~]# service auditd restart

Starting auditd: [OK]

[root@linux ~]# service auditd status

auditd (pid 32217) is running...

chkconfig --list | grep auditd

auditd 0:off 1:off 2:on 3:on 4:on 5:on 6:off

十三、安全审计

启用计策略，一般对系统的登陆、退出、创建/删除目录、修改密码、添加组、计划任务，添加完策略后需重启这个服务：service auditd restart

范例：

```
more /etc/audit/audit.rules
# Enable auditing
-e 1
## login configuration and information
-w /etc/login.defs -p wa -k CFG_login.defs
-w /etc/securetty -p wa -k CFG_securetty
-w /var/log/faillog -p wa -k LOG_faillog
-w /var/log/lastlog -p wa -k LOG_lastlog
-w /var/log/tallylog -p wa -k LOG_tallylog

## directory operations
#-a entry,always -S mkdir -S mkdirat -S rmdir


## cron configuration & scheduled jobs
-w /etc/cron.allow -p wa -k CFG_cron.allow
-w /etc/cron.deny -p wa -k CFG_cron.deny
-w /etc/cron.d/ -p wa -k CFG_cron.d
```

```
-w /etc/cron.daily/ -p wa -k CFG_cron.daily
-w /etc/cron.hourly/ -p wa -k CFG_cron.hourly
-w /etc/cron.monthly/ -p wa -k CFG_cron.monthly
-w /etc/cron.weekly/ -p wa -k CFG_cron.weekly
-w /etc/crontab -p wa -k CFG_crontab
-w /var/spool/cron/root -k CFG_crontab_root


## user, group, password databases
-w /etc/group -p wa -k CFG_group
-w /etc/passwd -p wa -k CFG_passwd
-w /etc/gshadow -k CFG_gshadow
-w /etc/shadow -k CFG_shadow
-w /etc/security/opasswd -k CFG_opasswd


# ----- File System audit rules -----
# Add a watch on "passwd" with the arbitrary filterkey "fk_passwd" that
# generates records for "reads, writes, executes, and appends" on "passwd"
-w /etc/passwd -k fk_passwd -p rwxa

# Add a watch "shadow" with a NULL filterkey that has permissions
# filtering turned off
-w /etc/shadow
```

警告：

如果在运行守护进程时添加规则/etc/audit/audit.rules，则一定要以根用户身份用 service auditd restart 命令启用修改。