一. 账户安全

1.1 锁定系统中多余的自建帐号

检查方法:

执行命令

#cat /etc/passwd

#cat /etc/shadow

查看账户、口令文件，与系统管理员确认不必要的账号。对于一些保留的系统伪帐户如：bin, sys，adm，uucp，lp, nuucp，hpdb, www, daemon 等可根据需要锁定登陆。

备份方法:

#cp -p /etc/passwd /etc/passwd_bak

#cp -p /etc/shadow /etc/shadow_bak

加固方法:

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>解锁需要恢复的账号。

1.2 设置系统口令策略

检查方法:

使用命令

#cat /etc/login.defs|grep PASS 查看密码策略设置

备份方法:

cp -p /etc/login.defs /etc/login.defs_bak

加固方法:

#vi /etc/login.defs 修改配置文件

PASS_MAX_DAYS 90 #新建用户的密码最长使用天数

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

PASS_MIN_LEN 9 #最小密码长度 9

1.3 禁用 root 之外的超级用户

检查方法：

#cat /etc/passwd 查看口令文件，口令文件格式如下：

login_name：password：user_ID：group_ID：comment：home_dir：command

login_name：用户名

password：加密后的用户密码

user_ID：用户 ID，(1 ~ 6000) 若用户 ID=0，则该用户拥有超级用户的权限。查看此处是否有多个 ID=0。

group_ID：用户组 ID

comment：用户全名或其它注释信息

home_dir：用户根目录

command：用户登录后的执行命令

备份方法：

#cp -p /etc/passwd /etc/passwd_bak

加固方法：

使用命令 passwd -l <用户名>锁定不必要的超级账户。

使用命令 passwd -u <用户名>解锁需要恢复的超级账户。

风险：需要与管理员确认此超级用户的用途。

1.4 限制能够 su 为 root 的用户

检查方法：

#cat /etc/pam.d/su,查看是否有 auth required /lib/security/pam_wheel.so 这样的配置条目

备份方法：#cp -p /etc/pam.d /etc/pam.d_bak

加固方法：

#vi /etc/pam.d/su

在头部添加：

auth required /lib/security/pam_wheel.so group=wheel

这样，只有 wheel 组的用户可以 su 到 root

#usermod -G10 test 将 test 用户加入到 wheel 组

当系统验证出现问题时，首先应当检查 /var/log/messages 或者 /var/log/secure 中的输出信息，根据这些信息判断用户账号的有效

性。如果是因为 PAM 验证故障，而引起 root 也无法登录，只能使用 single user 或者 rescue 模式进行排错。

1.5 检查 shadow 中空口令帐号

检查方法：

#awk -F: '(== "") { print }' /etc/shadow

备份方法：cp -p /etc/shadow /etc/shadow_bak

加固方法：对空口令账号进行锁定，或要求增加密码

二、最小化服务

2.1 停止或禁用与承载业务无关的服务

检查方法：

#who –r 或 runlevel 查看当前 init 级别

#chkconfig --list 查看所有服务的状态

备份方法：记录需要关闭服务的名称

加固方法：

#chkconfig --level <服务名> on|off|reset 设置服务在个 init 级别下开机是否启动

三、数据访问控制

3.1 设置合理的初始文件权限

检查方法：

#cat /etc/profile 查看 umask 的值

备份方法：

#cp -p /etc/profile /etc/profile_bak

加固方法：

#vi /etc/profile

umask=027

风险：会修改新建文件的默认权限，如果该服务器是 WEB 应用，则此项谨慎修改。

四、网络访问控制

4.1 使用 SSH 进行管理

检查方法：

#ps –aef | grep sshd 查看有无此服务

备份方法：

加固方法：

使用命令开启 ssh 服务

#service sshd start

风险：改变管理员的使用习惯

4.2 设置访问控制策略限制能够管理本机的 IP 地址

检查方法：

#cat /etc/ssh/sshd_config 查看有无 AllowUsers 的语句

备份方法：

#cp -p /etc/ssh/sshd_config /etc/ssh/sshd_config_bak

加固方法：

#vi /etc/ssh/sshd_config，添加以下语句

AllowUsers *@10.138.*.* 此句意为：仅允许 10.138.0.0/16 网段所有用户通过 ssh 访问

保存后重启 ssh 服务

#service sshd restart

风险：需要和管理员确认能够管理的 IP 段

4.3 禁止 root 用户远程登陆

检查方法：

#cat /etc/ssh/sshd_config 查看 PermitRootLogin 是否为 no

备份方法：

#cp -p /etc/ssh/sshd_config /etc/ssh/sshd_config_bak

加固方法：

#vi /etc/ssh/sshd_config

PermitRootLogin no

保存后重启 ssh 服务

service sshd restart

4.4 限定信任主机

检查方法：

#cat /etc/hosts.equiv 查看其中的主机

#cat /$HOME/.rhosts 查看其中的主机

备份方法：

#cp -p /etc/hosts.equiv /etc/hosts.equiv_bak

#cp -p /$HOME/.rhosts /$HOME/.rhosts_bak

加固方法：

#vi /etc/hosts.equiv 删除其中不必要的主机

#vi /$HOME/.rhosts 删除其中不必要的主机

风险：在多机互备的环境中，需要保留其他主机的 IP 可信任。

4.5 屏蔽登录 banner 信息

检查方法：

#cat /etc/ssh/sshd_config 查看文件中是否存在 Banner 字段，或 banner 字段为 NONE

#cat /etc/motd 查看文件内容，该处内容将作为 banner 信息显示给登录用户。

备份方法：

#cp -p /etc/ssh/sshd_config /etc/ssh/sshd_config_bak

#cp -p /etc/motd /etc/motd_bak

加固方法：

#vi /etc/ssh/sshd_config

banner NONE

#vi /etc/motd

删除全部内容或更新成自己想要添加的内容

风险：无可见风险

4.6 防止误使用 Ctrl+Alt+Del 重启系统

检查方法：

#cat /etc/inittab|grep ctrlaltdel 查看输入行是否被注释

备份方法：

#cp -p /etc/inittab /etc/inittab_bak

加固方法：

#vi /etc/inittab

在行开头添加注释符号“#”

#ca::ctrlaltdel:/sbin/shutdown -t3 -r now

五、用户鉴别

5.1 设置帐户锁定登录失败锁定次数、锁定时间

检查方法：

#cat /etc/pam.d/system-auth 查看有无 auth required pam_tally.so 条目的设置

备份方法：

#cp -p /etc/pam.d/system-auth /etc/pam.d/system-auth_bak

加固方法：

#vi /etc/pam.d/system-auth

auth required pam_tally.so onerr=fail deny=6 unlock_time=300 设置为密码连续错误 6 次锁定，锁定时间 300 秒

解锁用户 faillog -u <用户名> -r

风险：需要 PAM 包的支持;对 pam 文件的修改应仔细检查，一旦出现错误会导致无法登陆;

当系统验证出现问题时，首先应当检查 /var/log/messages 或者 /var/log/secure 中的输出信息，根据这些信息判断用户账号的有效性。

5.2 修改帐户 TMOUT 值，设置自动注销时间

检查方法：

#cat /etc/profile 查看有无 TMOUT 的设置

备份方法：

#cp -p /etc/profile /etc/profile_bak

加固方法：

#vi /etc/profile

增加

TMOUT=600 无操作 600 秒后自动退出

风险：无可见风险

5.3 Grub/Lilo 密码

检查方法：

#cat /etc/grub.conf|grep password 查看 grub 是否设置密码

#cat /etc/lilo.conf|grep password 查看 lilo 是否设置密码

备份方法：

#cp -p /etc/grub.conf /etc/grub.conf_bak

#cp -p /etc/lilo.conf /etc/lilo.conf_bak

加固方法：为 grub 或 lilo 设置密码

风险：etc/grub.conf 通常会链接到/boot/grub/grub.conf

5.4 限制 FTP 登录

检查方法：

#cat /etc/ftpusers 确认是否包含用户名，这些用户名不允许登录 FTP 服务

备份方法：

#cp -p /etc/ftpusers /etc/ftpusers_bak

加固方法：

#vi /etc/ftpusers 添加行，每行包含一个用户名，添加的用户将被禁止登录 FTP 服务

风险：无可见风险

5.5 设置 Bash 保留历史命令的条数

检查方法：

#cat /etc/profile|grep HISTSIZE=

#cat /etc/profile|grep HISTFILESIZE= 查看保留历史命令的条数

备份方法：

#cp -p /etc/profile /etc/profile_bak

加固方法：

#vi /etc/profile

修改 HISTSIZE=5 和 HISTFILESIZE=5 即保留最新执行的 5 条命令

六、审计策略

6.1 配置系统日志策略配置文件

检查方法：

#ps –aef | grep syslog 确认 syslog 是否启用

#cat /etc/syslog.conf 查看 syslogd 的配置，并确认日志文件是否存在

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

备份方法：

#cp -p /etc/syslog.conf

6.2 为审计产生的数据分配合理的存储空间和存储时间

检查方法：

#cat /etc/logrotate.conf 查看系统轮询配置，有无

rotate log files weekly

weekly

keep 4 weeks worth of backlogs

rotate 4 的配置

备份方法：

#cp -p /etc/logrotate.conf /etc/logrotate.conf_bak

加固方法：

#vi /etc/logrotate.d/syslog

增加

rotate 4 日志文件保存个数为 4，当第 5 个产生后，删除最早的日志

size 100k 每个日志的大小

加固后应类似如下内容：

/var/log/syslog/*_log {

missingok

notifempty

size 100k # log files will be rotated when they grow bigger that 100k.

rotate 5 # will keep the logs for 5 weeks.

compress # log files will be compressed.

sharedscripts

postrotate

/etc/init.d/syslog condrestart >/dev/null 2>1 || true

endscript

```
}
```