Linux 加固方案

1 加固目标

1. 用户账号
2. 权限分配
3. 系统配置

1.1 用户账号加固

1.1.1 锁定系统中多余的自建帐号

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。

使用 cat /etc/passwd cat /etc/shadow 查看

加固：

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。

1.1.2 设置口令策略

使用 cat /etc/login.defs|grep PASS 查看当前密码策略设置

口令应该具有一定复杂度，定期更换口令，输入错误一定数量后锁定

加固：

#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

#vi /etc/pam.d/system-auth 修改配置文件

auth required pam_env.so

auth required pam_tally2.so deny=3 unlock_time=300

连续输入错误 3 次，账户锁定 5 分钟。

1.1.3 禁用 root之外的超级用户

#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

加固：

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。

1.1.4 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

加固：

#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

1.1.5 检查 shadow中空口令帐号

检查方法：

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

加固：

对空口令账号进行锁定，或要求增加密码

1.1.6 服务账号创建

检查方法：

#cat /etc/passwd

加固：

对应的服务应该创建对应的账户。

#useradd 选项 用户名

选项：

-c comment 指定一段注释性描述。

-d 目录 指定用户主目录，如果此目录不存在，则同时使用 -m 选项，可以创建主目录。

-g 用户组 指定用户所属的用户组。

-G 用户组，用户组 指定用户所属的附加组。

-s Shell 文件 指定用户的登录 Shell 。

-u 用户号 指定用户的用户号，如果同时有 -o 选项，则可以重复使用其他用户的标识号。

1.2 权限分配

总体思路就是权限最低原则。

1.web 文件夹

一般只给读 rx 的权限，不给 w 权限，只有特殊目录比如 /upload 、/data 等才给予 w 的权限。如果某些目录要有 w 权限，但不必需要 x 权限，则要取消 x 权限。

检查方法：

使用 ls -l 目录名查看用户权限

加固：

#chmod 755 目录名 设置权限为 rx

#chmod +w　　目录名　增加 w 的权限

#chmod　–x　目录名　　去除 x 权限

注意：

Web 文件权限分配是针对的　web 服务器用户。

2.系统文件夹及文件

加固：

系统一般的文件夹都只需要给　rx 权限, 不需要给 w 权限, 特殊文件夹除外。

1.3　系统配置

1.3.1 网络访问控制

1.使用 SSH 进行管理

检查方法：

#ps –aef | grep sshd　　查看有无此服务

加固：

使用命令开启 ssh 服务

#service sshd start

开机启动 ssh

#vi /etc/rc.local　　加入 service sshd start

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

加固：

#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

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

加固：

#vi /etc/ssh/sshd_config

PermitRootLogin no

保存后重启 ssh 服务

service sshd restart

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

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

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。

加固：

#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

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

加固：

#vi /etc/inittab

在行开头添加注释符号“ # ”

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

7.减少来自网络自动化脚本攻击压力

加固：

修改端口号，修改成 5 位数非常用的端口号数字

#vi /etc/ssh/sshd_config

Port 22 修改数字后保存退出

#service sshd restart 重启 ssh 服务

iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport

刚才修改的端口号数字 -j ACCEPT 修改端口号后对应防火墙也要开放

#iptables –save

8.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

加固：

#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

1.3.2 审计策略配置

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

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

加固：

#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 that100k.

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

}

1.3.3 其他

1 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

加固：

#vi /etc/profile

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

2.定期更新系统，保持系统版本最新

加固：

#yum -y update

#yum -u upgrade

Redhat 和 Centos 系列

#apt-get update

#apt-get upgrade

Debian 系列