浪潮信息云峦服务器操作系统 KeyarchOS

安全加固手册

浪潮电子信息产业股份有限公司

目录

1 概述

1.1 文档简介

本文档给出 KeyarchOS 的加固介绍和加固方法，指导用户进行安全加固。

1.2 适用对象

本文档主要适用于需要对 KeyarchOS 进行安全加固的管理员。管理员需要熟悉操作系统安全架构和安全技术。

更多相关资源，请访问浪潮信息官网或联系浪潮信息技术人员。

1.3 加固目的

操作系统作为信息系统的核心，承担着管理硬件资源和软件资源的重任，是整个信息系统安全的基础。操作系统之上的各种应用，要想获得信息的完整性、机密性、可用性和可控性，必须依赖于操作系统。脱离了对操作系统的安全保护，仅依靠其他层面的防护手段来阻止黑客和病毒等对网络信息系统的攻击，是无法满足安全需求的。

因此，需要对操作系统进行安全加固，构建动态、完整的安全体系，增强产品的安全性，提升产品的竞争力。

2 加固指导

本章主要介绍 KeyarchOS 加固指导方法。

2.1 概述

用户可以通过修改加固策略配置文件进行系统加固。本节介绍各加固项的含义以及 KeyarchOS 是否已默认加固，并给出加固方法，指导用户进行安全加固。

注：为了数据安全，用户在使用 KeyarchOS 过程中，尽量不要使用不安全的服务、协议：如仅支持明文传输、无认证接入的服务，或存在已知漏洞的协议。也不要使用不安全的配置：如启用了不安全的服务、协议，未遵循最小化开放、默认安全原则的配置等。

2.2 帐户安全

2.2.1 设置密码复杂度策略

1、命令行

用户可以通过修改对应配置文件设置口令的复杂度要求，建议用户根据实际情况设置口令复杂度，若不选择配置此项目，可能会导致安全风险。

可以通过修改/etc/pam.d/system-auth 文件，来设置检查密码复杂度策略中的小写字母个数、大写字母个数、数字个数、特殊字符个数和最小长度。例如，口令需至少包含大小写字母、数字、特殊字符、最小长度为 8，可将默认的 password requisite pam_pwquality.so 修改为如下所示(若不存在 password requisite pam_pwquality.so，

则新增）:

password requisite pam_pwquality.so ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 minlen=8 enforce_for_root try_first_pass

注： retry=N：重试多少次后返回密码修改错误；difok=N：新密码必需与旧密码不同的位数；dcredit=N：数字的个数；lcredit=N：小写字母的个数；ucredit=N：大写字母的个数；credit=N：特殊字母的个数；minclass=N：密码组成(大/小字母，数字，特殊字符)；minlen=N：新密码最短长度。

2、GUI

可以通过修改/etc/security/pwquality.conf 文件，来设置检查密码复杂度策略中的小写字母个数、大写字母个数、数字个数、特殊字符个数和最小长度。例如，口令需至少包含大小写字母、数字、特殊字符、最小长度为 8，将对应选项去掉注释后修改为如下所示（若不存在 try_first_pass，则新增）:

ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 minlen=8 enforce_for_root try_first_pass

注：dcredit=N：数字的个数；lcredit=N：小写字母的个数；ucredit=N：大写字母的个数；credit=N：特殊字母的个数；minclass=N：密码组成(大/小字母，数字，特殊字符)；minlen=N：新密码最短长度。

2.2.2 设置密码重复使用次数限制

可在配置文件/etc/pam.d/system-auth 中设置密码重复使用次数显示，修改设置

如下：

password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=5

注：sha512：使用 sha512 算法对口令加密；remember:不能重复几次以前的密码。

创建文件/etc/security/opasswd 用于存储旧密码，并设置权限：

touch /etc/security/opasswd

chown root:root /etc/security/opasswd

chmod 600 /etc/security/opasswd

2.2.3 设置口令有效期

出于系统安全性考虑，建议设置口令有效期限，且口令到期前通知用户更改口令。口令有效期的设置通过修改/etc/login.defs 文件实现。

通过设置 PASS_MAX_DAYS 项的值来设置口令有效期，如果该文件不存在，则创建并按照要求进行编辑；如下所示，设置口令有效期为 99 天：

PASS_MAX_DAYS 99

通过设置 PASS_MIN_DAYS 项的值来设置两次修改口令的最小间隔时间，如下所示，设置口令修改最短间隔时间为 6 天：

PASS_MIN_DAYS 6

通过设置 PASS_WARN_AGE 项的值，来设置口令过期前警告天数；如下所示，

设置口令过期前 7 天开始提示：

PASS_WARN_AGE 7

2.2.4 登录失败超过阈值后锁定

为了保障用户系统的安全，建议用户设置口令出错次数的阈值（建议 3 次），以及由于口令尝试被锁定用户的自动解锁时间（建议 300 秒）；若不选择配置此项目，可能会导致安全风险。

若配置此项目，用户锁定期间，任何输入被判定为无效，锁定时间会因用户的再次输入而重新计时；解锁后，用户的错误输入记录被清空。通过上述设置可以有效防范口令被暴力破解，增强系统的安全性。

可在配置文件/etc/pam.d/system-auth 和/etc/pam.d/password-auth 中设置口令出错次数锁定的阈值和自动解锁时间，增加如下所示的代码：

auth required pam_faillock.so preauth audit deny=3 even_deny_root unlock_time=300 root_unlock_time=300

auth [default=die] pam_faillock.so authfail audit deny=3 unlock_time=300

account required pam_faillock.so

注： auth required pam_faillock.so preauth audit deny=3 even_deny_root unlock_time=300 root_unlock_time=300 必须在最前面，建议按照下图的位置配置/etc/pam.d/system-auth 和/etc/pam.d/password-auth，否则可能会导致配置失败或

者用户无法登录等问题。

```
# Generated by authselect on Thu Jul 27 08:04:06 2023
# Do not modify this file manually.

auth        required                                     pam_env.so
auth        required                                     pam_faillock.so preauth audit deny=5 even_deny_root unlock_time=300 root_unlock_time=300
auth        required                                     pam_faildelay.so delay=2000000
auth        sufficient                                   pam_fprintd.so
auth        [default=1 ignore=ignore success=ok]         pam_usertype.so isregular
auth        [default=1 ignore=ignore success=ok]         pam_localuser.so
auth        sufficient                                   pam_unix.so nullok
auth        [default=1 ignore=ignore success=ok]         pam_usertype.so isregular
auth        sufficient                                   pam_sss.so forward_pass
auth        [default=die]                                pam_faillock.so authfail audit deny=5 unlock_time=300
auth        required                                     pam_deny.so

account     required                                     pam_unix.so
account     sufficient                                   pam_localuser.so
account     sufficient                                   pam_usertype.so issystem
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required                                     pam_permit.so
account     required                                     pam_faillock.so

password    requisite                                    pam_pwquality.so local_users_only
password    sufficient                                   pam_unix.so yescrypt shadow nullok use_authtok
password    sufficient                                   pam_sss.so use_authtok
password    required                                     pam_deny.so

session     optional                                     pam_keyinit.so revoke
session     required                                     pam_limits.so
-session    optional                                     pam_systemd.so
session     [success=1 default=ignore]                   pam_succeed_if.so service in crond quiet use_uid
session     required                                     pam_unix.so
session     optional                                     pam_sss.so
~
~
~
```

注：deny=3：设置用户连续登录失败次数超过 3 次即被锁定；unlock_time：普通用户自动解锁时间为 600 秒；even_deny_root：同样限制 root 帐户。

2.2.5 加固 su 命令

su 命令用于在不同帐户之间切换。为了增强系统安全性，有必要对 su 命令的使用权进行控制，只允许 root 和 wheel 群组的帐户使用 su 命令，限制其他帐户使用。su 命令的使用控制通过修改/etc/pam.d/su 文件实现，可用 PAM 认证模块未禁止 wheel 组之外的用户 su 为 root，编辑 su 文件(vi /etc/pam.d/su)，在开头添加下面两行：

auth sufficient pam_rootok.so

auth required pam_wheel.so group=wheel

这表明只有 wheel 组的成员可以使用 su 命令成为 root 用户。可以把用户添加到 wheel 组，以使它可以使用 su 命令成为 root 用户。添加方法为：

usermod -G wheel username

2.2.6 禁止 root 用户远程登录 SSH

出于系统安全性考虑，建议禁止 root 用户远程登录 SSH，可以通过修改 /etc/ssh/sshd_config 文件来实现。打开 /etc/ssh/sshd_config 文件，配置 PermitRootLogin no。重启服务（systemctl restart sshd）即可。

2.2.7 设置用户登录显示

可以通过修改/etc/motd 文件来设置用户登录显示，配置完成后，每次登录系统时，通过终端展示一些消息给登录用户，如向用户提示欢迎信息，或提示使用系统的注意事项等等信息。编辑文件/etc/motd 的内容，如没有该文件，则创建它，执行如下所示的命令修改（可根据实际需要修改该文件的内容）:

echo " Authorized users only. All activity may be monitored and reported " > /etc/motd

ssh 登录时,可能会自动显示系统版本信息之类的敏感信息，有些版本会存在一些固有的安全问题 ,很容易被黑客利用。可以通过修改/etc/sshbanner 隐藏敏感信息：

1、执行如下命令创建 sshbanner 信息文件：

touch /etc/sshbanner

chown bin:bin /etc/sshbanner

chmod 644 /etc/sshbanner

echo " Authorized users only. All activity may be monitored and reported " >/etc/sshbanner

可根据实际需要修改该文件的内容。

2、修改/etc/ssh/sshd_config 文件，添加如下行：

Banner /etc/sshbanner

3、重启 sshd 服务：

systemctl restart sshd

2.3 授权认证

2.3.1 设置终端的自动退出时间

无人看管的终端容易被侦听或被攻击，可能会危及系统安全。因此建议设置终端在停止运行一段时间后能够自动退出。

自动退出时间由/etc/profile 文件的 TMOUT 字段(单位为秒)控制，在/etc/profile 的尾部添加如下配置：

export TMOUT=300

2.3.2 设置用户的默认 umask 值

umask 值用于为用户新创建的文件和目录设置缺省权限。如果 umask 的值设置过小，会使群组用户或其他用户的权限过大，给系统带来安全威胁。因此设置所有用户默认的 umask 值为 0077，即用户创建的目录默认权限为 700，文件的默认权限为

600。配置方法如下：

1、在文件/etc/csh.cshrc 中设置 umask 077 或 UMASK 077

2、检查文件/etc/bashrc（或/etc/bash.bashrc）中设置 umask 077 或 UMASK 077

3、在文件/etc/profile 中设置 umask 077 或 UMASK 077

2.4 文件权限

Linux 将所有对象都当作文件来处理，即使一个目录也被看作是包含有多个其他文件的大文件。因此，Linux 中最重要的就是文件和目录的安全性。文件和目录的安全性主要通过权限和属主来保证。

配置重要文件属性方法如下：

1、配置/etc/passwd 文件属性，执行 chattr +i /etc/passwd；如果不支持 chattr，编辑/etc/fstab，在相应的 reiserfs 系统的选项中添加"user_xattr,attrs"这两个选项，然后重启主机。

2、配置/etc/shadow 文件属性，执行 chattr +i /etc/shadow；如果不支持 chattr，编辑/etc/fstab，在相应的 reiserfs 系统的选项中添加"user_xattr,attrs"这两个选项，然后重启主机。

3、配置/etc/group 文件属性，执行 chattr +i /etc/group；如果不支持 chattr,编辑/etc/fstab，在相应的 reiserfs 系统的选项中添加"user_xattr,attrs"这两个选项，然后重启主机。

4、配置/etc/gshadow 文件属性 ,执行 chattr +i /etc/gshadow ;如果不支持 chattr, 编辑/etc/fstab，在相应的 reiserfs 系统的选项中添加"user_xattr,attrs"这两个选项，然后重启主机。

配置重要目录或文件权限：

1、配置/etc/security 目录权限：

```
chmod 600 /etc/security
```

2、配置/etc/rc6.d 文件权限：

```
chmod 750 /etc/rc6.d
```

3、配置/tmp 文件权限：

```
chmod 750 /tmp
```

4、配置/etc/rc0.d 文件权限：

```
chmod 750 /etc/rc0.d
```

5、配置/etc/rc1.d/文件权限：

```
chmod 750 /etc/rc1.d
```

6、配置/etc/rc2.d 文件权限：

```
chmod 750 /etc/rc2.d
```

7、配置/etc/rc3.d 文件权限：

```
chmod 750 /etc/rc3.d
```

8、配置/etc/rc4.d 文件权限：

```
chmod 750 /etc/rc4.d
```

9、配置/etc/rc5.d 文件权限：

```
chmod 750 /etc/rc5.d
```

10、配置/etc/rc.d/init.d/文件权限：

```
chmod 750 /etc/rc.d/init.d/
```

11、配置系统引导器配置文件权限：

如果/etc/grub.conf 文件存在，且非链接文件，则执行 chmod 600 /etc/grub.conf;

如果/boot/grub/grub.conf 文件存在，则执行 chmod 600 /boot/grub/grub.conf;

如果/etc/lilo.conf 文件存在，则执行 chmod 600 /etc/lilo.conf;

如果/etc/grub2.cfg 文件存在，且非链接文件，则执行 chmod 600 /etc/grub2.cfg;

如果/boot/grub2/grub.cfg 件存在，则执行 chmod 600 /boot/grub2/grub.cfg。

2.5 内核参数

内核参数决定配置和应用特权的状态。内核提供用户可配置的系统控制，这一系

统控制可微调或配置，该功能特性可通过控制各种可配置的内核参数，来提高操作系统的安全特性。比如：通过微调或配置网络选项，可有效提高系统的安全性。

配置系统内核参数方法如下：

1、禁止发送 icmp 重定向报文，执行命令：

```
sysctl -w net.ipv4.conf.all.accept_redirects="0"
```

修改后可查看文件

```
cat /proc/sys/net/ipv4/conf/all/accept_redirects 的值为 0
```

注：修改只能当次生效，重启系统需重新修改

2、检查 send_redirects 配置是否为 0，执行命令

```
sysctl -w net.ipv4.conf.all.send_redirects="0"
```

修改后可查看文件

```
cat /proc/sys/net/ipv4/conf/all/send_redirects 的值为 0
```

注：修改只能当次生效，重启系统需重新修改

2.6 禁止内核 core dump

出于系统安全性考虑，内核崩溃时不建议产生 core dump；可以进行如下所示的配置来禁止内核产生 dump 文件：

1、在/etc/security/limits.conf 文件底部增加配置 * hard core 0

```
echo "* hard core 0" >> /etc/security/limits.conf
```

2、在/etc/security/limits.conf 文件底部增加配置 * soft core 0

```
echo "* soft core 0"   >> /etc/security/limits.conf
```

2.7 SELinux 配置

自主访问控制 DAC（Discretionary Access Control）基于用户、组和其他权限，决定一个资源是否能被访问的因素是某个资源是否拥有对应用户的权限，它不能使系统管理员创建全面和细粒度的安全策略。SELinux（Security-Enhanced Linux）是 Linux 内核的一个模块，也是 Linux 的一个安全子系统。SELinux 实现了强制访问控制 MAC（Mandatory Access Control），每个进程和系统资源都有一个特殊的安全标签，资源能否被访问除了 DAC 规定的原则外，还需要判断每一类进程是否拥有对某一类资源的访问权限。

KeyarchOS 默认使用 SELinux 提升系统安全性。SELinux 分为三种模式：

- ✧ permissive：SELinux 仅打印告警而不强制执行。
- ✧ enforcing：SELinux 安全策略被强制执行。
- ✧ disabled：不加载 SELinux 安全策略。

可以通过修改 SELinux 的配置文件/etc/selinux/config 来配置 SELinux。

3 术语表

无

4 FAQ

559 对外服务可配置：第三方的口令可修改即可

560 响应包：验证 ssh 支持的安全协议算法安全（v2）即可

561 密码找回：没有找回则安全

562 用户权限（第三方非开源）linux 本身机制即可

564 终端访问限制 防火墙限制 ip 范围即可

572 日志存储控制 调小阈值