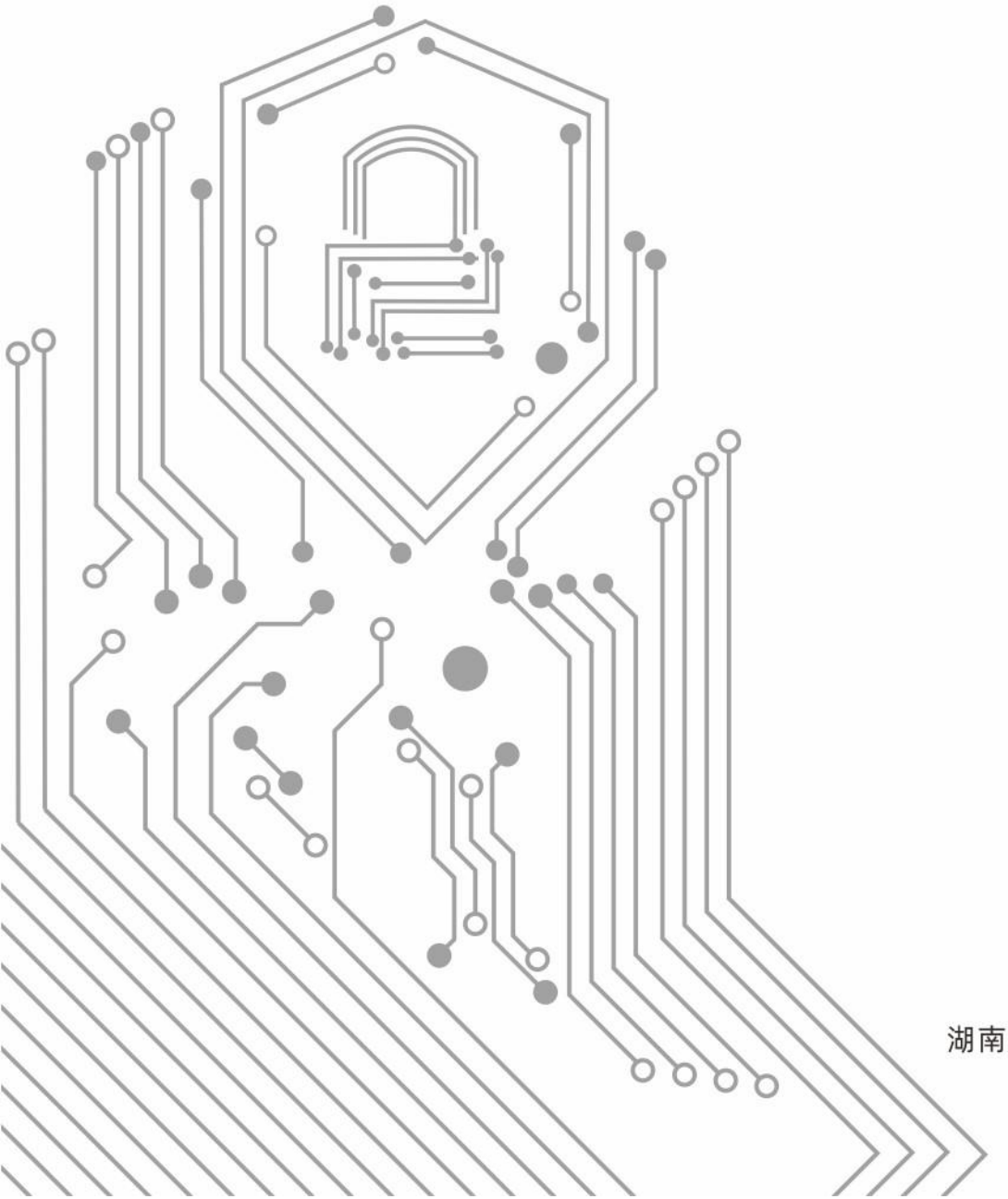
麒麟信安
KYLINSEC

麒麟信安-主机安全加固软件 V1.0 用户手册

文档版本：KYJS-KS-SSR-1.1-SUM-V1.0

发布日期：2023 年 02 月 10 日



湖南麒麟信安科技股份有限公司
www.kylinsec.com.cn
400-012-6606

变更记录

版本	修订时间	修订人	修订类型	修订章节	修订内容
V1.0	2023.02.10	胡新良	ADD	ALL	生成全文

注 1：修订类型分为 A-ADDED，M-MODIFIED，D–DELETED

注 2：对该文件内容增加、删除或修改均需填写此记录，详细记载变更信息，以保证其可追溯性

目　录

1 范围

1.1 标识

文档标识号：KYJS-KS-SSR-1.1-SUM-V1.0；
标题：麒麟信安-主机安全加固软件 V1.1 用户手册；

软件软著名称：麒麟信安主机安全加固软件 V1.1；

软件发布版本：ks-ssr-1.1-xxx.run；

软件缩写：SSR；

软件版本号：V1.1；

本文档适用的系统和计算机软件配置项 CSCI：麒麟信安操作系统。

1.2 软件概述

电网等重要领域行业对于操作系统安全非常重视，大部分业务在入网前需要做入网安全加固、或者是等保测评，厂商对于系统的安全加固很重视。操作系统安全性和易用性是个矛盾体，麒麟信安操作系统通过强制访问控制、完整性控制、多因子验证、关键系统部件加固等技术手段增强了系统安全性，但也增加了管理员和用户的维护难度。为了在提高安全性的同时，提升麒麟信安操作系统的易用性，提高产品粘性，研发麒麟信安-主机安全加固软件，为用户提供易操作、高效率和可定制的系统安全加固方案。

在兼容性方面，安全加固软件充分适配麒麟信安操作系统各发行版本；在稳定性上，保障软件长期无故障运行；在性能方面，作为应用程序提供高效的操作平台；在易用性方面，安全加固软件为图形用户界面，为用户提供良好的用户体验。

如果您有任何疑问，都可以通过以下的方式获得帮助：

a) 求助在线帮助：http://www.kylinsec.com.cn；

b) 热线：400-012-6606；0731-88777708 。

c) 麒麟信安技术服务平台：https://support.kylinsec.com.cn

1.3 文档概述

本文档是麒麟信安-主机安全加固软件用户手册，它包含以下内容：

a) 麒麟信安-主机安全加固软件概述；

b) 麒麟信安-主机安全加固软件使用指南。

2 使用指南

这里主要介绍如何使用麒麟信安-主机安全加固软件。

2.1 安装与卸载

本节主要介绍麒麟信安-主机安全加固软件安装与卸载相关内容。

2.1.1 安装软件

.run 文件的安装方法：

第一步：为.run 文件增加可执行属性，输入命令$ chmod +x ks-ssr-xxx(安装包版本).run；

第二步：执行安装，输入命令$ ./ks-ssr-xxx.run ，即可完成安装。

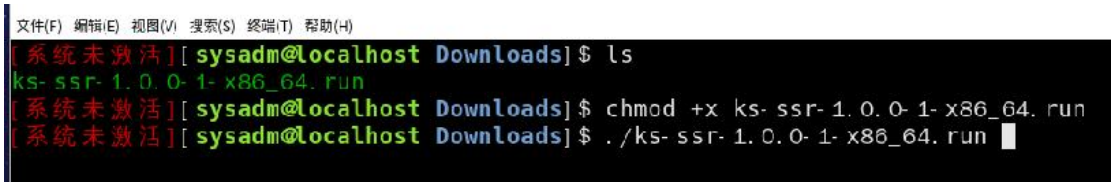


图 2-1 安装软件

2.1.2 卸载软件

卸载软件方法：

输入命令$ ks-ssr-uninstall，稍等片刻即可完成卸载。

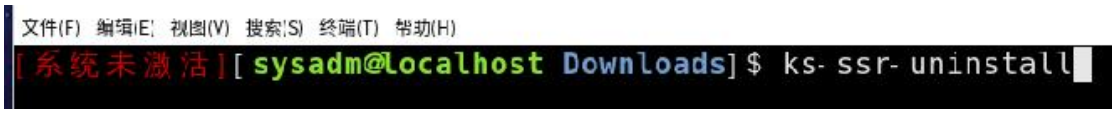


图 2-2 卸载软件

2.1.3 启动软件

有两种方式可以启动软件。

启动软件方式一：双击桌面 " 系统安全加固 " 的图标，弹出麒麟信安-主机安全加固软件的窗口。

图 2-3 桌面图标

启动软件方式二：鼠标左键单击＂开始菜单＂－＞＂系统工具＂－＞＂系统安全加固＂，弹出麒麟信安-主机安全加固软件的窗口。

图 2-4 开始菜单入口

2.2 软件升级

本节主要介绍麒麟信安-主机安全加固软件升级方法。

第一步：下载需要升级的软件包.run 文件；

第二步：关闭软件当前界面，为.run 文件增加可执行属性，输入命令$ chmod +x ks-ssr-xxx(安装包版本).run；

第三步：执行升级，输入命令$ ./ks-ssr-xxx.run ，即可完成升级。

```
[服务未授权][sysadm@localhost Downloads]$ ls
ks-ssr-1.0-20220519-x86_64.run  ks-ssr-1.1-20230202.run
[服务未授权][sysadm@localhost Downloads]$ ./ks-ssr-1.1-20230202.run
KylinSecOS version: KylinSec-PG-3.3-6C-2105-101504-x86_64
kylin license 2.3.5-2 is less than or equal to 2.3.5-2.1
Current arch is x86_64
The rpm path /tmp/ks-run-tmp/ks-ssr/KY3.3/x86_64
准备中...                          ################################## [100%]
正在升级/安装...
   1:ks-ssr-gui-1.1.6-1              ################################## [ 50%]
```

2.3 主界面

本节主要介绍麒麟信安-主机安全加固软件主界面的菜单项及其对应的功能。

双击桌面＂系统安全加固＂的图标，弹出麒麟信安-主机安全加固软件的窗口。如下图

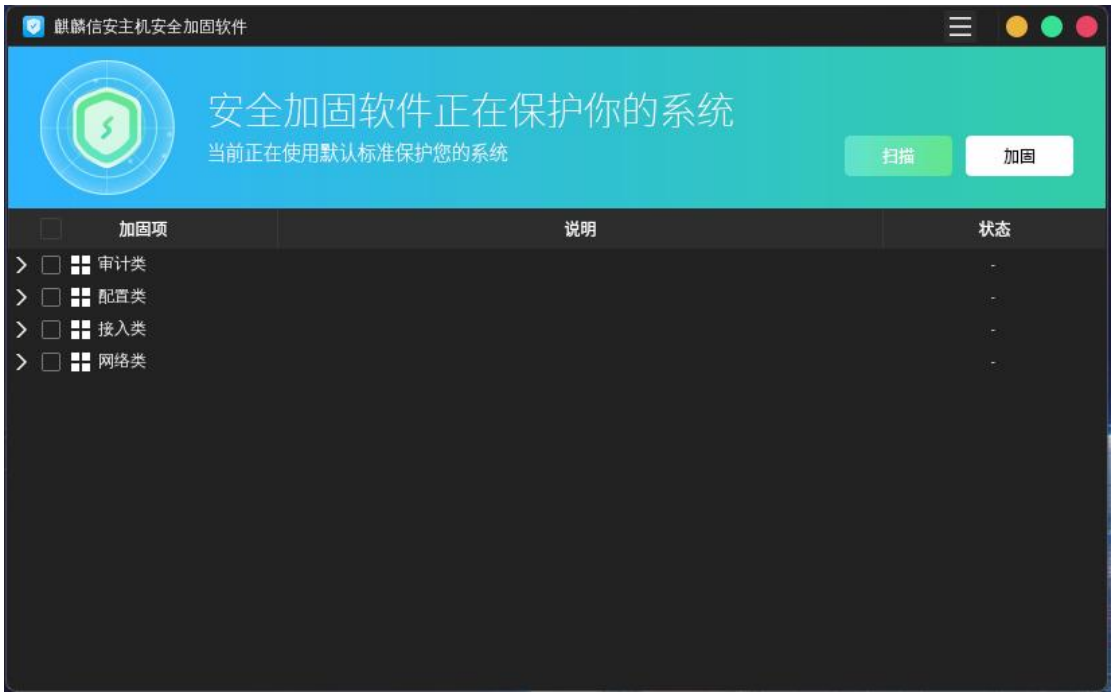


图 2-5 软件窗口

2.3.1 加固

“加固”释义：对加固项按照系统标准进行加固。

点击加固，对选择的加固项进行加固。加固中会有百分比进度条显示加固进度，加固过程中也可以点击＂取消＂停止加固，如下图：

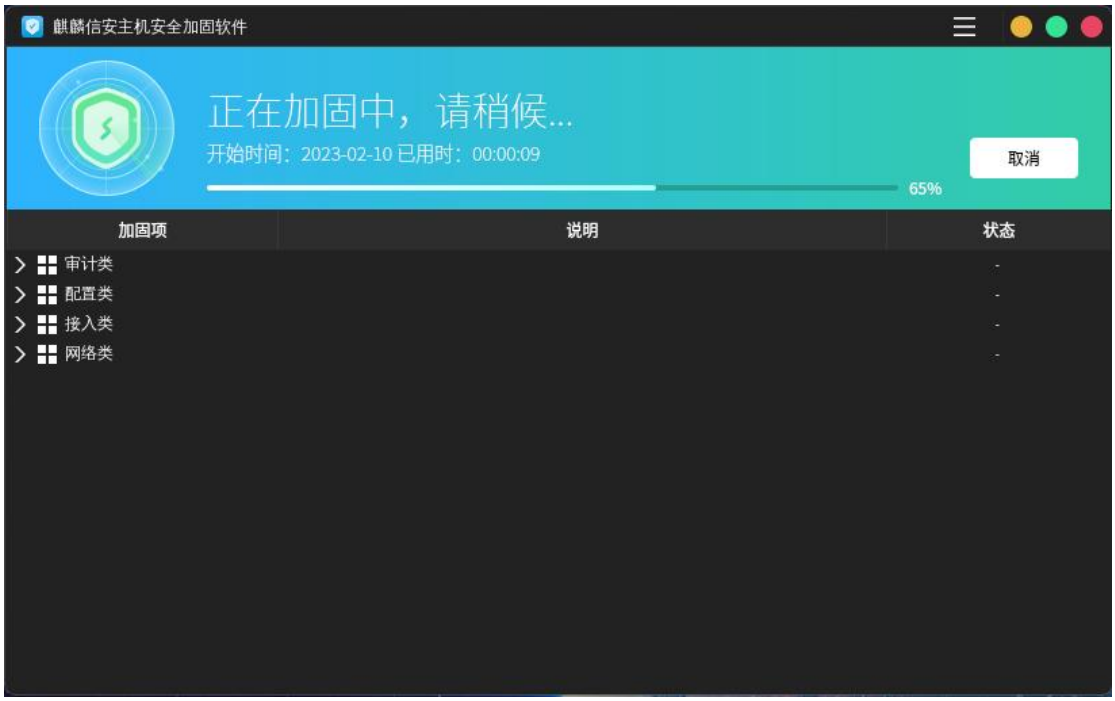


图 2-6 加固

加固完成后会显示：加固完成的总数，成功加固总数，加固失败的总数，加固用时，加固进度。加固成功会在＂状态＂栏显示＂已加固＂，加固失败会在＂状态＂栏显示＂加固失败＂。

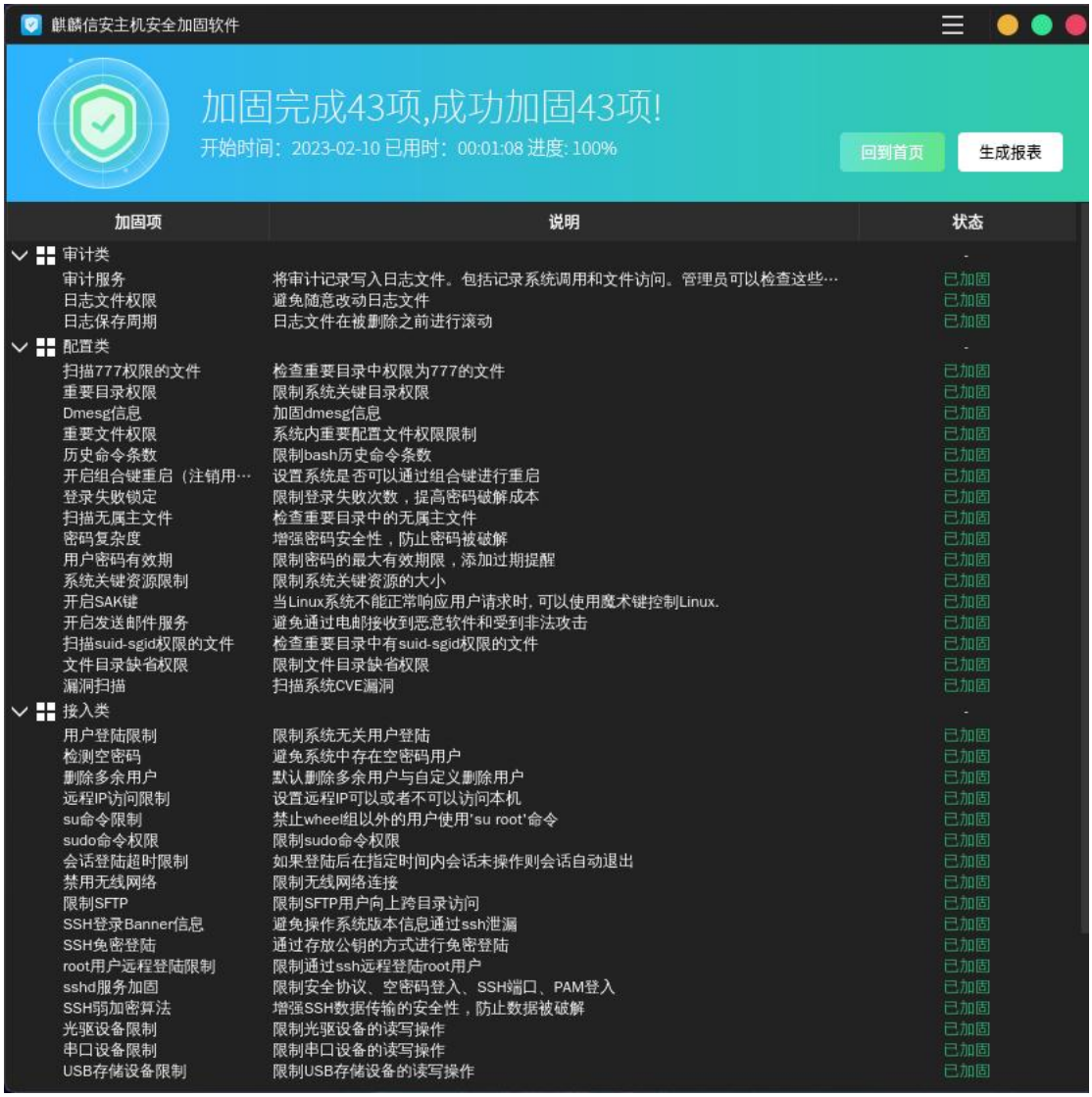


图 2-7 加固完成

加固完成后可以点击＂回到首页＂，也可以点击＂生成报表＂查看详细信息。

2.3.2 扫描

扫描释义：对比加固项配置是否与系统标准一致。加固项配置与系统标准一致时显示为＂符合＂，加固项配置与系统标准不一致时显示为＂不符合＂。

点击扫描，扫描中会有百分比进度条显示扫描进度，扫描过程中也可以点击＂取消＂停止扫描，如下图

图 2-8 扫描

扫描完成后会显示：扫描完成的总数，扫描符合的总数，扫描不符合的总数，加固用时，加固进度。符合系统标准的会在＂状态＂栏显示为＂符合＂，不符合系统标准的会在＂状态＂栏显示为＂不符合＂。如下图

图 2-9 扫描完成

扫描完成后可以点击＂回到首页＂或＂生成报表＂。

“回到首页”释义：回到初始界面。

“生成报表”释义：生成扫描报告。

2.3.3 生成报表

“生成报表”释义：扫描或加固后可点击＂生成报表＂，生成麒麟信安-主机安全加固软件软件报告，查看扫描和加固的详细信息。主要包含设备信息，加固信息饼图，安全加固图标三类信息。

点击＂生成报表＂，选择要保存的文件路径，设置要保存的文件名称，点击右下角＂保存＂按钮，提示导出成功，点击＂确认＂即可。

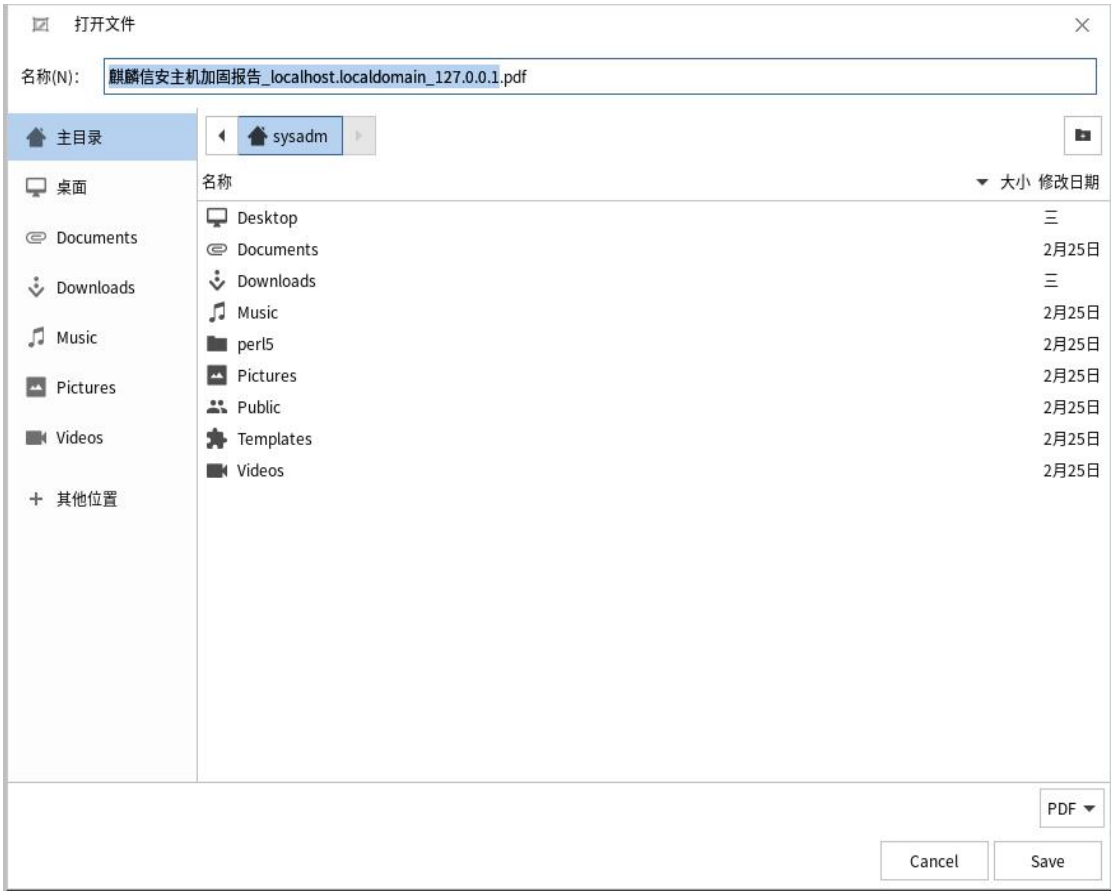


图 2-10 生成报表

图 2-11 报表导出成功

设备信息包含的内容如下图

图 2-12 设备信息

加固信息饼图包含的内容如下图

图 2-13 加固信息饼图

安全加固图表包含的内容如下图

检测项	检测结果	加固结果	备注
审计服务	符合	已加固	-
日志文件权限	符合	已加固	-
日志保存周期	符合	已加固	-
扫描777权限的文件	符合	已加固	-
重要目录权限	符合	已加固	-
Dmesg信息	符合	已加固	-
重要文件权限	符合	已加固	-
历史命令条数	符合	已加固	-
开启组合键重启（注销用户后生效）	符合	已加固	-
登录失败锁定	符合	已加固	-
扫描无属主文件	符合	已加固	-
密码复杂度	符合	已加固	-
用户密码有效期	符合	已加固	-
系统关键资源限制	符合	已加固	-
开启SAK键	符合	已加固	-
开启发送邮件服务	符合	已加固	-
扫描suid-sgid权限的文件	符合	已加固	-
文件目录缺省权限	符合	已加固	-

图 2-14 安全加固图表

2.3.4 菜单栏

主界面的菜单栏包含如下功能按钮：

- 加固回退
- 重置加固配置
- 设置
- 激活
- 帮助
- 关于

图 2-15 菜单栏

2.3.4.1 加固回退

“加固回退”释义：使用加固回退可以恢复加固项到初始配置或上一次配置。

图 2-16 加固回退

2.3.4.2 重置加固配置

“重置加固配置”释义：把所有的加固项配置恢复为系统标准的默认值。

点击＂重置加固配置＂，所有的加固配置恢复为系统标准的默认参数。

2.3.4.3 设置

“设置”释义：可以选择加固策略，开关定时扫描功能，设置定时扫描时间，开关加固操作通知和资源监控功能。

加固策略：默认为系统策略，不能对加固项参数进行修改，扫描和加固也不能自定义选择单个或多个加固项，只能对所有加固项扫描和加固；

可选择自定义策略，自定义策略可对加固项参数进行自定义修改，且可导出策略保存为自定义策略。扫描和加固可自定义选择单个或多个加固项执行。

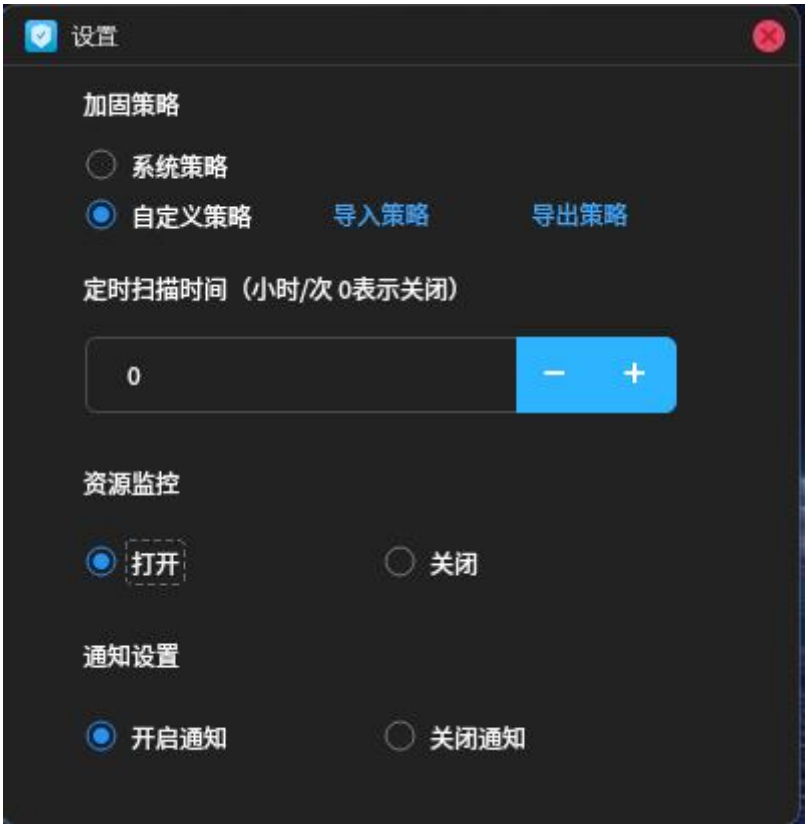


图 2-17 设置

2.3.4.4 激活

“激活”释义：给麒麟信安-主机安全加固软件授权，未激活时不能对加固项进行加固，激活后才能对加固项进行加固操作。

未激活时状态如下

图 2-18 未激活状态

点击＂激活＂，弹出软件激活窗口，如下图

图 2-19 激活

输入正确的激活码，点击 " 激活 " ，提示激活成功。可通过扫描机器码右侧的二维码获取机器码。

激活成功后查看到软件激活窗口信息，如下图

图 2-20 激活成功

2.3.4.5 帮助

“帮助”释义：点击帮助弹出用户指导手册。

2.3.4.6 关于

“关于”释义：显示软件相关的信息。

点击 " 关于 " ，弹出关于的窗口，可查看到软件相关的版本信息。点击右上角的 "

X " 可关闭窗口。如下图

图 2-21 关于

2.4 加固项

本节主要介绍麒麟信安-主机安全加固软件软件加固项内容，包含如下类别的加固项：

- ●审计类
- ●配置类
- ●接入类
- ●网络类

图 2-22 加固项类别

2.4.1 审计类

审计类加固项包含：审计规则，审计服务，日志文件权限，日志保存周期。

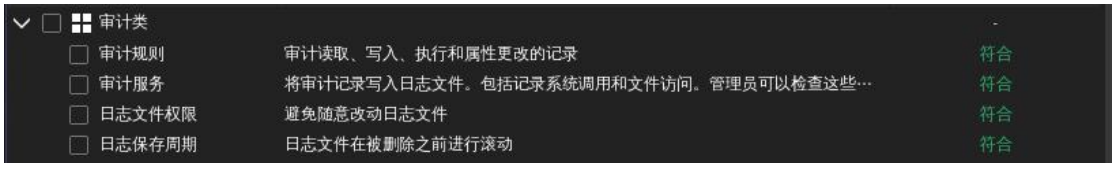


图 2-23 审计类加固项

2.4.1.1 审计规则

支持添加和删除审计规则，默认为空。

2.4.1.2 审计服务

审计服务加固后默认开启。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-24 审计服务加固参数设置

2.4.1.3 日志文件权限

日志文件加固后默认最大权限为 0644，只能被添加不能删除。

可以双击＂说明＂对应的位置打开加固参数设置，用户可进行自定义设置，点击＂重置＂参数恢复为默认标准参数，点击＂确定＂后可进行加固。

图

图 2-25 日志文件权限加固参数设置

2.4.1.4 日志保存周期

日志保存周期加固后默认保存 24 周。

可以双击 " 说明 " 对应的位置打开加固参数设置，用户可进行自定义设置为 " 0~99999 " 的值，点击 " 重置 " 参数恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-26 日志保存周期加固参数设置

2.4.2 配置类

配置类加固项包含：扫描 777 权限的文件，重要目录权限，Dmesg 信息，重要文件权限，历史命令条数，开启组合键重启，登录失败锁定，扫描无属主文件，密码复杂度，账户密码有效期，系统关键资源限制，开启 SAK 键，开启发送邮件服务，扫描 suid-sgid 权限的文件，文件目录缺省权限，漏洞扫描。

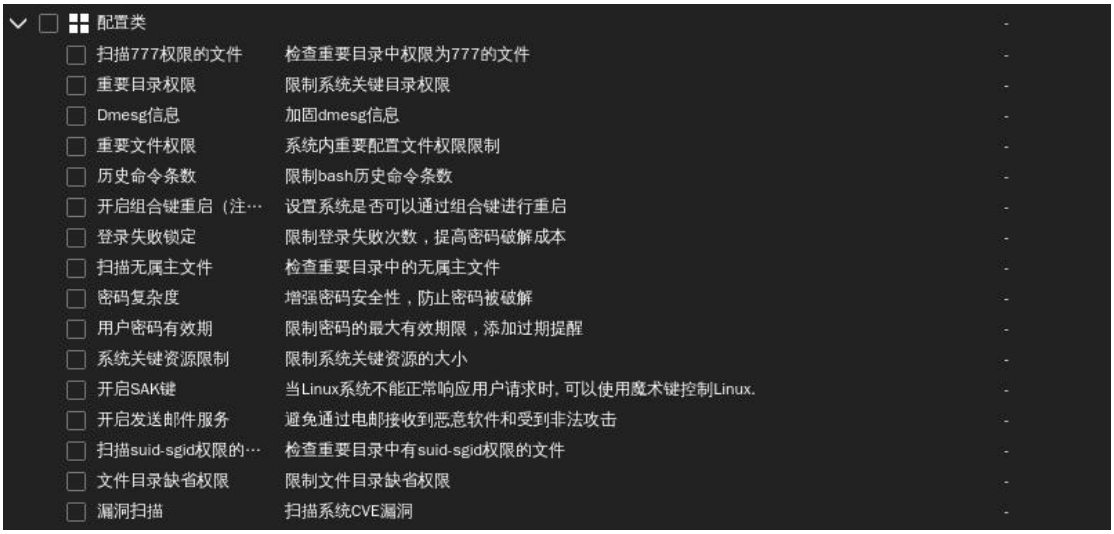


图 2-27 配置类加固项

2.4.2.1 扫描 777 权限的文件

检查重要目录文件中权限为 777 的文件，并在报表中进行展示。

可以双击 " 说明 " 对应的位置打开加固参数设置，用户可进行自定义设置，点击 " 重置 " 参数恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-28 扫描 777 权限的文件加固参数设置

2.4.2.2 重要目录权限

重要目录权限加固后默认最大权限为 0755。

可以双击 " 说明 " 对应的位置打开加固参数设置，用户可进行自定义设置，点击 " 重置 " 参数恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-29 重要目录权限加固参数设置

2.4.2.3 Dmesg 信息

开启后仅管理员可查看 dmesg 信息。

可以双击 " 说明 " 对应的位置打开加固参数设置，用户可进行自定义设置，

点击＂重置＂参数恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-30 Dmesg 信息加固参数设置

2.4.2.4 重要文件权限

重要文件权限加固后默认最大权限为 0644。

可以双击＂说明＂对应的位置打开加固参数设置，用户可进行自定义设置，点击＂重置＂参数恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-31 重要文件权限加固参数设置

2.4.2.5 历史命令条数

历史命令条数加固后默认保存 5 条。

可以双击＂说明＂对应的位置打开加固参数设置，用户可进行自定义设置＂0~99999＂的值，点击＂重置＂参数恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-32 历史命令条数加固参数设置

2.4.2.6 开启组合键重启

开启组合键重启加固后默认关闭，系统不可以通过组合键重启。

可以双击 " 说明 " 对应的位置打开 " 加固参数设置 "，用户可进行自定义设置，点击 " 重置 " 参数会恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-33 开启组合键重启加固参数设置

2.4.2.7 登录失败锁定

登录失败锁定加固后，默认密码错误次数为 3，非 root 用户锁定后自动解锁时间为 300 秒，root 用户登录失败锁定开启。也就是如果连续输入错误的密码 3 次，用户会被锁定 300 秒无法登陆。

可以双击 " 说明 " 对应的位置打开加固参数设置，用户可进行自定义设置，密码错误次数可修改为 " 1~99999 " 的值，非 root 用户锁定后自动解锁时间可修改为 " 0~99999 " 的值，root 用户登录失败锁定可修改为 " 否 "，点击 " 重置 " 参数恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-34 登录失败锁定加固参数设置

2.4.2.8 扫描无属主文件

检查系统中重要目录中的无属主文件，并在报表中展示。

可以双击＂说明＂对应的位置打开加固参数设置，用户可进行自定义设置，点击＂重置＂参数恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-35 扫描无属主文件加固参数设置

2.4.2.9 密码复杂度

密码复杂度加固后，默认最小密码长度为 8，大写字母数为 0，小写字母数

为 0，数字个数为 1，特殊字符个数为 1，包含字符类型数（特殊字符，数字，字母）为 3，最大连续字符个数为 3，允许包含用户名为 " 否 " ，启用字典检查默认为 " 是 " 。

可以双击 " 说明 " 对应的位置打开加固参数设置，用户可进行自定义设置，最小密码长度可修改为 " 6~99999 " 的值，大写字母数可修改为 " 0~99999 " 的值，小写字母数可修改为 " 0~99999 " 的值，数字个数可修改为 " 0~99999 " 的值，特殊字符个数可修改为 " 0~99999 " 的值，包含字符类型数可修改为 " 0~99999 " 的值，最大连续字符个数可修改为 " 0~99999 " 的值，允许包含用户名可修改为 " 是 " ，启用字典检查默认为 " 否 " ，点击 " 重置 " 参数恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-36 密码复杂度加固参数设置

2.4.2.10 用户密码有效期

用户密码有效期加固后，默认新用户可使用密码的最大有效天数为 180，密码更改允许的最小间隔天数为 1 ，密码过期前发出警告的天数为 28。

可以双击 " 说明 " 对应的位置打开加固参数设置，用户可进行自定义设置，

新用户可使用密码的最大有效天数可修改为 " 6~99999 " 的值，密码更改允许的最小间隔天数可修改为 " 0~99999 " 的值，密码过期前发出警告的天数可修改为 " 0~99999 " 的值，点击 " 重置 " 参数恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-37 用户密码有效期加固参数设置

2.4.2.11 系统关键资源限制

系统关键资源加固后默认开启。Stack 和 Rss 默认值为 10240。

可以双击 " 说明 " 对应的位置打开 " 加固参数设置 "，用户可进行自定义设置，参数 " 否 " 表示 Stack 和 Rss 为 ulimited，点击 " 重置 " 参数会恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-38 系统关键资源限制加固参数设置

2.4.2.12 开启 SAK 键

开启 SAK 键加固后默认开启，可使用组合按键 alt + sysrq 控制 Linux。

可以双击 " 说明 " 对应的位置打开 " 加固参数设置 "，用户可进行自定义设置，参数 " 否 " 表示关闭 SAK 键，点击 " 重置 " 参数会恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-39 开启 SAK 键加固参数设置

2.4.2.13 开启发送邮件服务

开启发送邮件服务加固后默认关闭。

可以双击 " 说明 " 对应的位置打开 " 加固参数设置 "，用户可进行自定义设置，参数 " 否 " 表示开启邮件服务，点击 " 重置 " 参数会恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-40 开启发送邮件服务加固参数设置

2.4.2.14 扫描 suid-sgid 权限的文件

检查系统中重要目录中有 suid-sgid 权限的文件，并在报表中展示。

可以双击＂说明＂对应的位置打开加固参数设置，用户可进行自定义设置，点击＂重置＂参数恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-41 扫描 suid-sgid 权限文件的加固参数设置

2.4.2.15 文件目录缺省权限

文件目录缺省权限加固后默认为 027。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-42 文件目录缺省权限加固参数设置

2.4.2.16 漏洞扫描

检查系统中的 CVE 漏洞，并在报表中展示。

可以双击＂说明＂对应的位置打开加固参数设置，用户可进行自定义设置，点击＂重置＂参数恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-43 漏洞扫描加固参数设置

2.4.3 接入类

接入类加固项包含：用户登陆限制，检测空密码，删除多余用户，远程 IP 访问限制，su 命令限制，sudo 命令权限，会话登陆超时限制，禁用无线网络，限制 SFTP，SSH 登录 Banner 信息，SSH 免密登陆，root 用户远程登陆限制，sshd 服务加固，SSH 弱加密算法，光驱设备限制，串口设备限制，USB 存储设备限制。

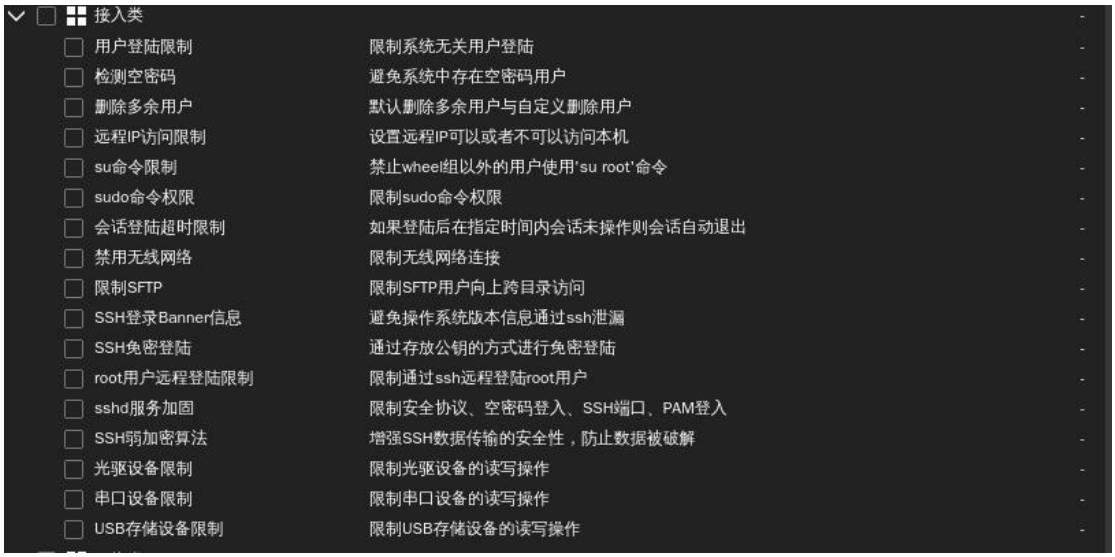


图 2-44 接入类加固项

2.4.3.1 用户登陆限制

用户登录限制加固后默认限制 root，三权用户（sysadm，secadm，audadm）和普通用户以外的用户进行登陆。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，可在允许登录账号输入允许登陆的账号。点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-45 用户登陆限制加固参数设置

2.4.3.2 检测空密码

检测空密码加固后默认开启。加固时会清除空密码账户。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，参数＂否＂表示允许空密码账户存在，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-46 检测空密码加固参数设置

2.4.3.3 删除多余用户

删除多余用户加固后默认开启。加固时会清除 lp，games，operator，adm。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-47 删除多余用户加固参数设置

2.4.3.4 远程 IP 访问限制

远程 IP 访问限制加固后默认列表为空。表示所有 IP 均可进行远程访问。

可以双击 " 说明 " 对应的位置打开加固参数设置，用户可进行自定义设置，根据输入框示例语法进行添加， " 允许远程访问的 IP 列表 " 表示可进行远程访问的 IP，" 禁止远程访问的 IP 列表 " 表示不能进行远程访问的 IP，点击 " 重置 " 参数恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-48 远程 IP 访问限制加固参数设置

2.4.3.5 su 命令限制

su 命令限制加固后默认开启。禁止 wheel 组以外的用户进行 su root。

可以双击 " 说明 " 对应的位置打开 " 加固参数设置 "，用户可进行自定义设置，参数 " 否 " 表示 wheel 组以外的用户可以进行 su root，点击 " 重置 " 参数会恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-49 su 命令限制加固参数设置

2.4.3.6 Sudo 命令权限

限制用户使用 sudo 命令权限加固后默认开启。开启 selinux 时会失效。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-50 sudo 命令权限加固参数设置

2.4.3.7 会话登陆超时限制

会话登陆超时限制加固后默认超时退出时间为 300 秒，只针对 ssh 远程登录退出。

可以双击＂说明＂对应的位置打开加固参数设置，用户可进行自定义设置为＂0~99999＂的值，点击＂重置＂参数恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-51 会话登陆超时限制加固参数设置

2.4.3.8 禁用无线网络

禁用无线网络加固后默认开启，无线网络不可用。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，参数＂否＂表示启用无线网络，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-52 禁用无线网络加固参数设置

2.4.3.9 限制 SFTP

限制 SFTP 用户向上跨目录访问，加固后默认开启。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-53 检测空密码加固参数设置

2.4.3.10 SSH 登录 Banner 信息

SSH 登录 Banner 信息加固后默认为 none。表示登陆时隐藏操作系统版本信息。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-54 SSH 登录 Banner 信息加固参数设置

2.4.3.11 root 用户远程登陆限制

root 用户远程登陆限制加固后默认禁止，表示不允许 ssh 登陆 root 用户。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，参数＂否＂表示可以通过 ssh 登陆 root 用户，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-56 root 用户远程登陆限制加固参数设置

2.4.3.12 Sshd 服务加固

Sshd 服务加固限制安全协议，空密码登入，加固后默认开启。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-57 sshd 服务加固参数设置

2.4.3.13 SSH 弱加密算法

SSH 弱加密算法默认关闭，表示不允许使用弱加密算法。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，参数＂是＂表示允许使用弱加密算法，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-58 SSH 弱加密算法加固参数设置

2.4.3.14 SSH 免密登陆

SSH 免密登陆加固后默认关闭。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，参数＂是＂表示允许 SSH 免密登陆，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

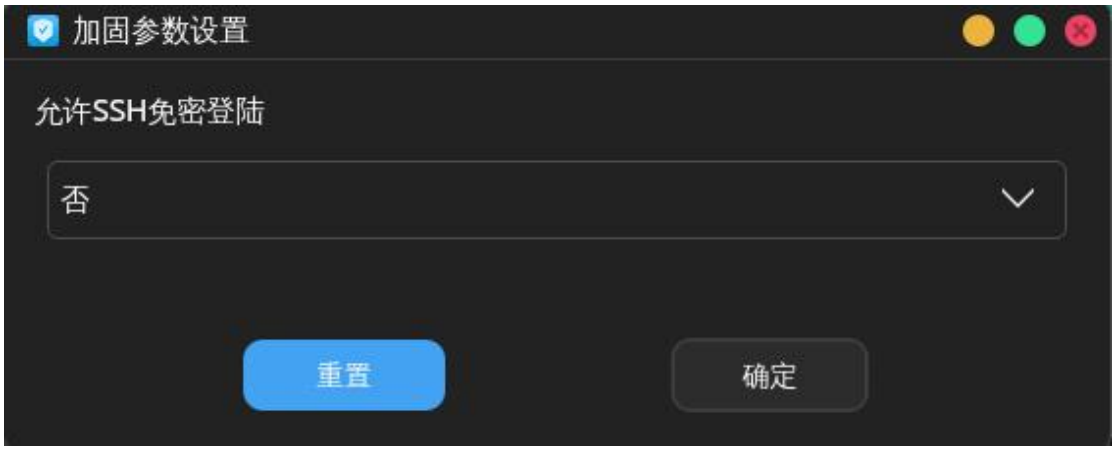


图 2-55 SSH 免密登陆加固参数设置

2.4.3.15 光驱设备限制

光驱设备限制加固后默认关闭，表示不能使用光驱设备。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，参数＂是＂表示能使用光驱设备，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-59 光驱设备限制加固参数设置

2.4.3.16 串口设备限制

串口设备限制加固后默认关闭，表示不能使用串口设备。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，参数＂是＂表示能使用串口设备，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-60 串口设备限制加固参数设置

2.4.3.17 USB 存储设备限制

USB 设备限制加固后默认关闭，表示不能使用 USB 设备。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，参数＂是＂表示能使用 USB 设备，点击＂重置＂参数会恢复为默认标准参

数，点击＂确定＂后可进行加固。

图 2-61 USB 存储设备限制加固参数设置

2.4.4 网络类

网络类加固项包含：防火墙配置，ICMP 时间戳请求，Traceroute 探测，禁止高危漏洞服务，ICMP 重定向，IP 源路由，Syn flood 攻击。

图 2-62 网络类加固项

2.4.4.1 防火墙配置

防火墙配置可配置系统防火墙规则。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

加固时会将 firewall 服务关闭，该加固项生效的前提是 firewall 关闭

图 2-63 防火墙配置加固参数设置

2.4.4.2 ICMP 时间戳请求

ICMP 时间戳请求加固后默认关闭。

可以双击 " 说明 " 对应的位置打开 " 加固参数设置 "，用户可进行自定义设置，参数 " 是 " 表示允许 ICMP 时间戳请求，点击 " 重置 " 参数会恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-64 ICMP 时间戳请求加固参数设置

2.4.4.3 Traceroute 探测

Traceroute 探测加固后默认开启，防止主机被 Traceroute 探测的威胁。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，参数＂否＂表示允许 Traceroute 探测，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-65 Traceroute 探测加固参数设置

2.4.4.4 禁止高危漏洞服务

禁止高危漏洞服务加固后默认关闭。包含蓝牙服务，打印服务，avahi-daemon 服务，RPC 端口映射服务，smb 服务。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，参数＂是＂表示开启对应服务，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-66 禁止高危漏洞服务加固参数设置

2.4.4.5 ICMP 重定向

ICMP 重定向加固后默认关闭。

可以双击 " 说明 " 对应的位置打开 " 加固参数设置 "，用户可进行自定义设置，参数 " 是 " 表示开启 ICMP 重定向，点击 " 重置 " 参数会恢复为默认标准参数，点击 " 确定 " 后可进行加固。

图 2-67 ICMP 重定向加固参数设置

2.4.4.6 IP 源路由

IP 源路由加固后默认关闭。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，参数＂是＂表示开启 IP 源路由，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-68 IP 源路由加固参数设置

2.4.4.7 Syn flood 攻击

Syn flood 加固后默认开启，表示防止 Syn flood 攻击。

可以双击＂说明＂对应的位置打开＂加固参数设置＂，用户可进行自定义设置，点击＂重置＂参数会恢复为默认标准参数，点击＂确定＂后可进行加固。

图 2-69 Syn flood 攻击加固参数设置

3 免责声明

我们尊重版权，也致力于保护版权，如果您在使用我们的安全加固软件，请

尽快激活。由于用户未及时激活，导致软件问题，造成的一切后果，本公司概不负责。

4 注释

无

5 附录

无