2023 － 2024 学年 第 1 学期



### 实 验 报 告

课 程 名 C01218

课 程 号 网络安全防护技术

学 生 姓 名 张炳欣

学 生 姓 号 32201241

专 业 班 级 软件工程2204

所 在 学 院 计算机与计算科学学院

指 导 老 师 沈淳

实验报告日期： 2024年 11 月 28 日

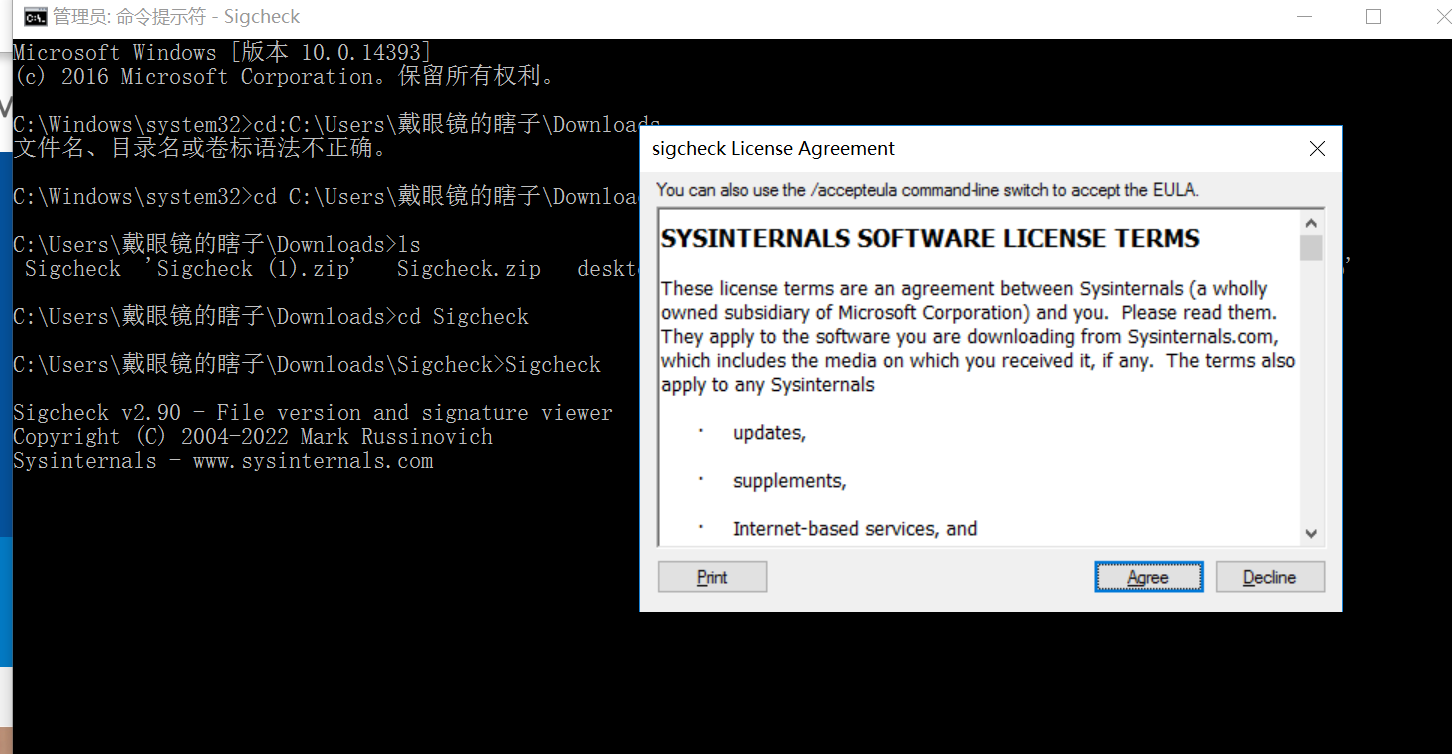
**课程实验报告清单**

|  |
| --- |
| 目录 |
| 1. 使用sigcheck工具生成对某个exe执行文件的6种哈希摘要 |
| 2. 用tripwire检查系统完整性，首先生成密钥，配置策略，初始化数据库，修改需要检查的目录，检验tripwire有没有检测到关键目录发生改变。  另外，尝试使--check --interactive参数更新数据库之后，再使用check检查是否还能发现完整性被破坏。 |
| 3. 使用AIDE进行系统完整性检测，具体实验步骤参考ppt。 |

完成要求：必须有详细过程。

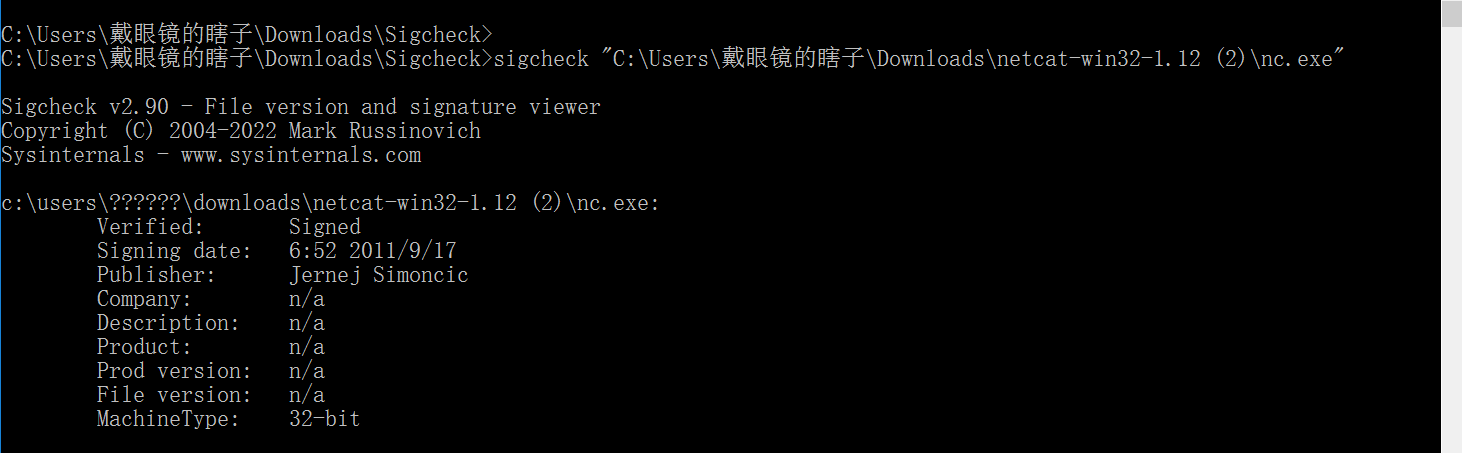
1. 使用sigcheck工具生成对某个exe执行文件的6种哈希摘要

先管理员进入



生成哈希摘要

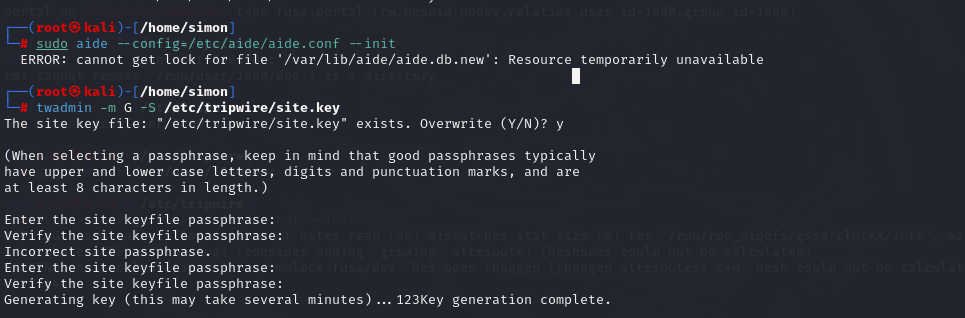
注意路径中带空格 路径要用双引号括起来

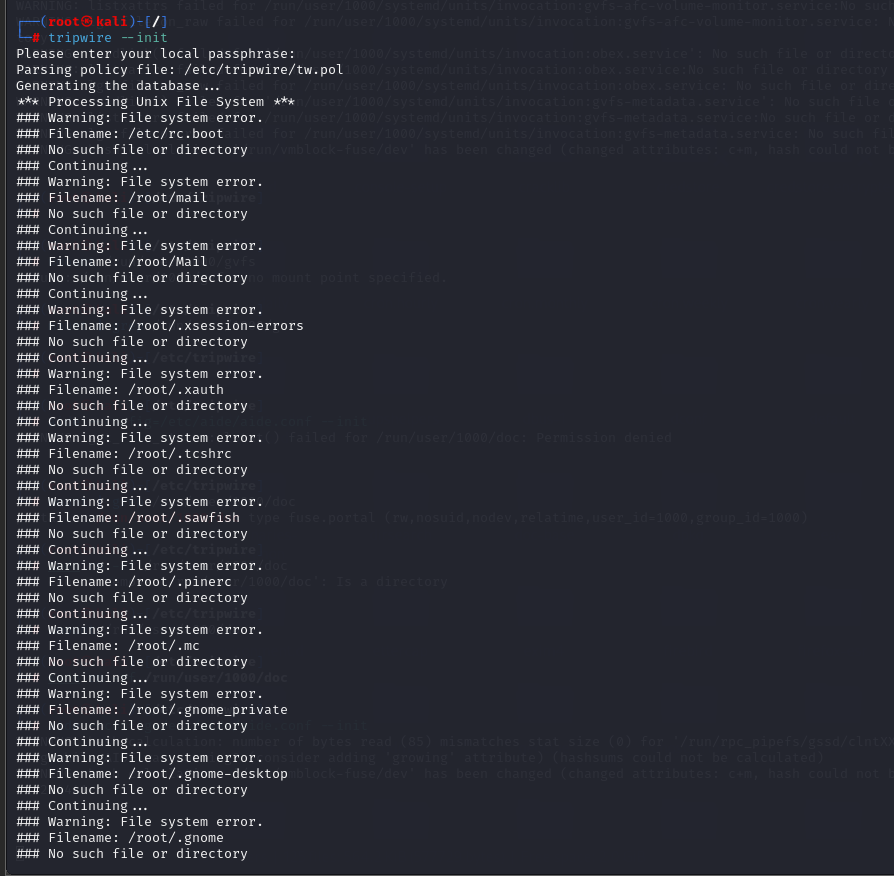


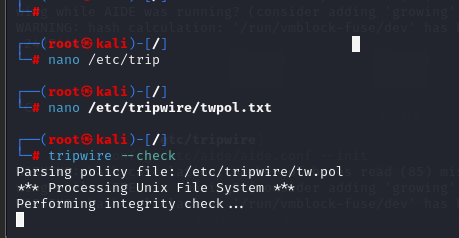


2. 用tripwire检查系统完整性，首先生成密钥，配置策略，初始化数据库，修改需要检查的目录，检验tripwire有没有检测到关键目录发生改变。

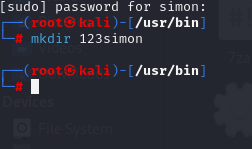
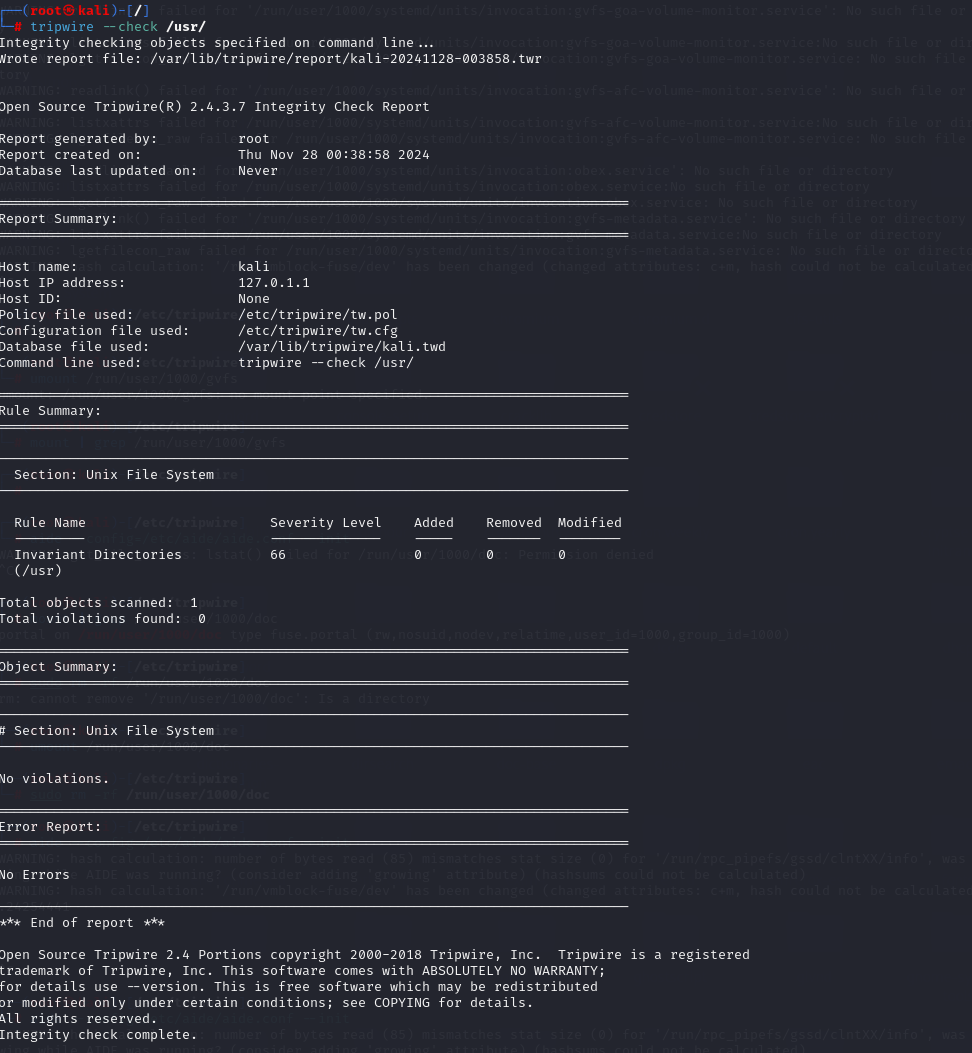
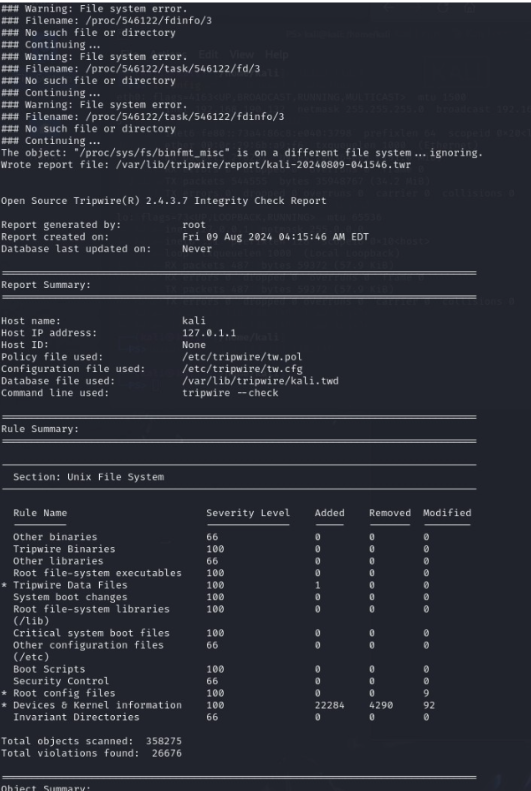
另外，尝试使--check --interactive参数更新数据库之后，再使用check检查是否还能发现完整性被破坏。







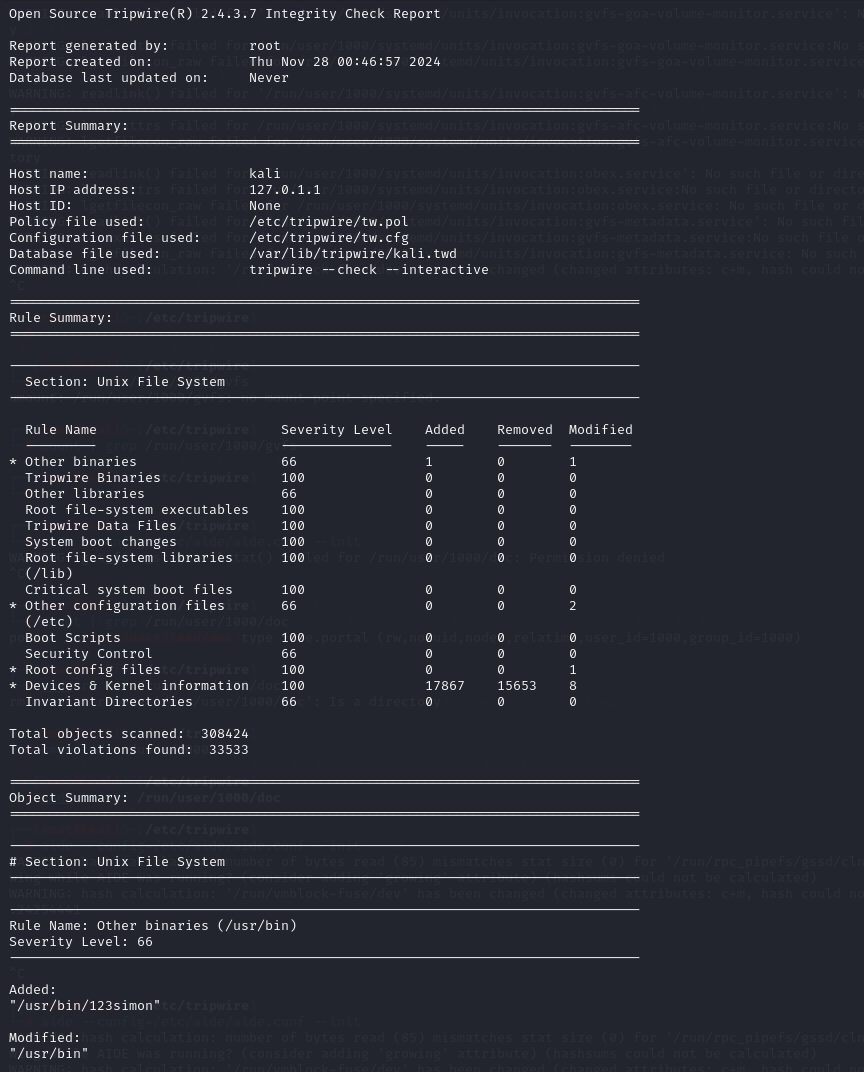
长时间后得到



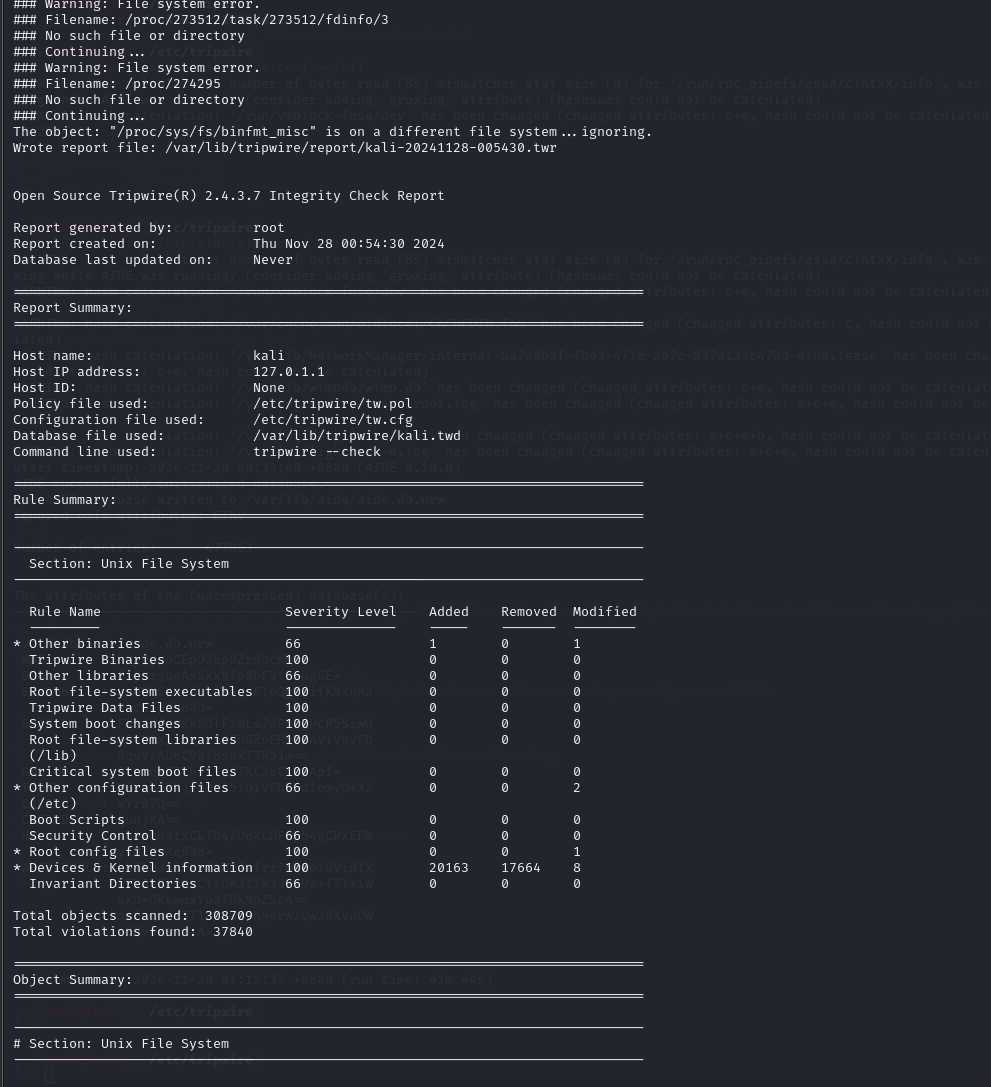
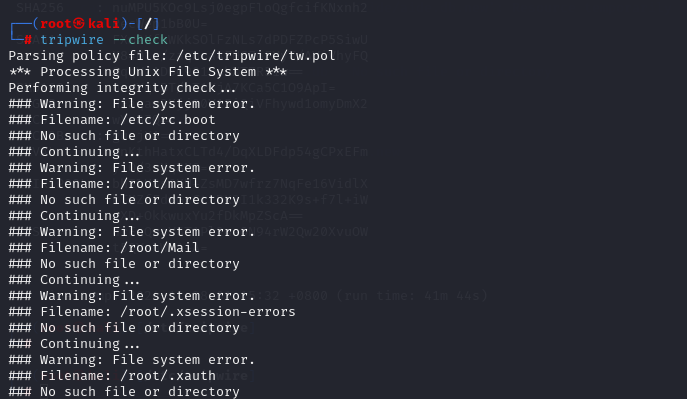
创建文件夹



检测到修改

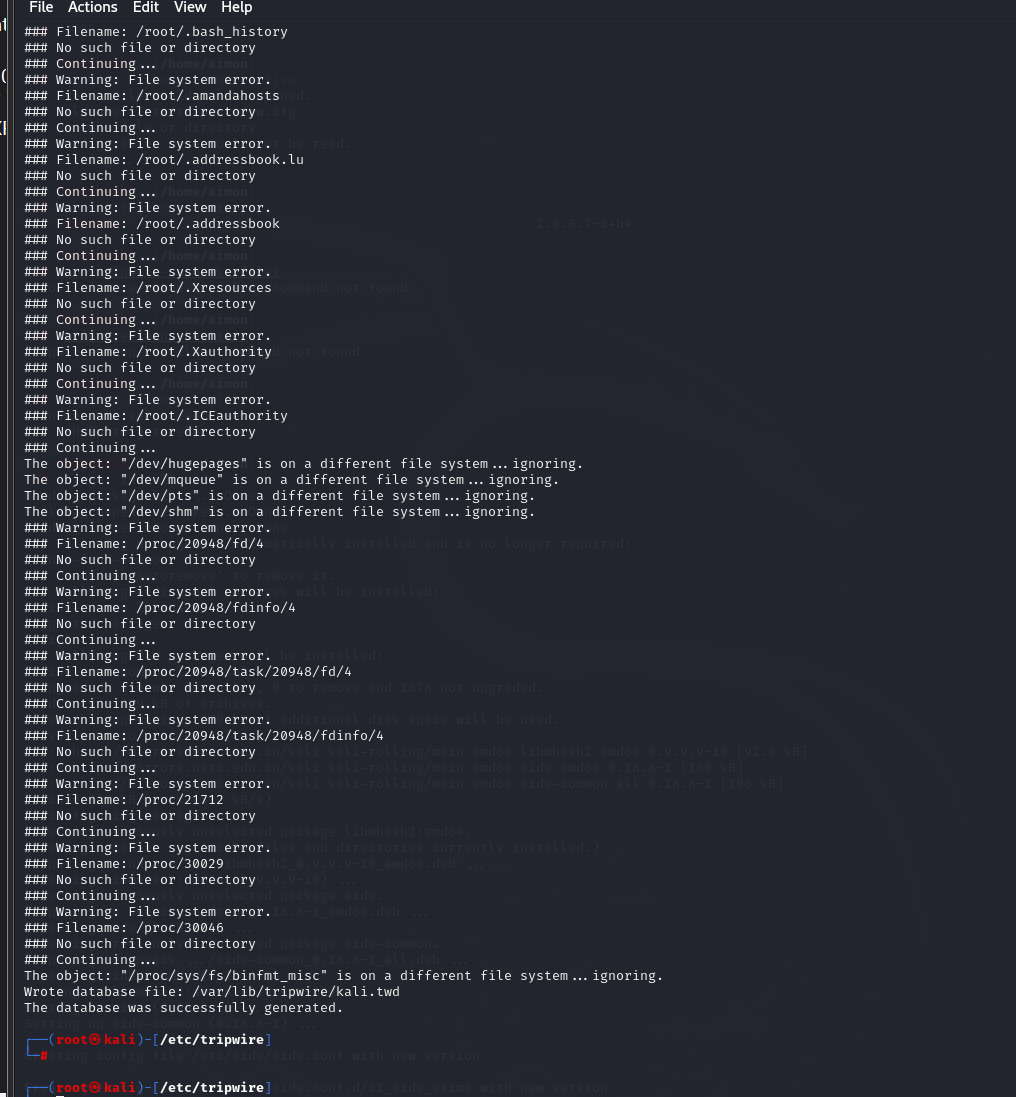


更新数据库



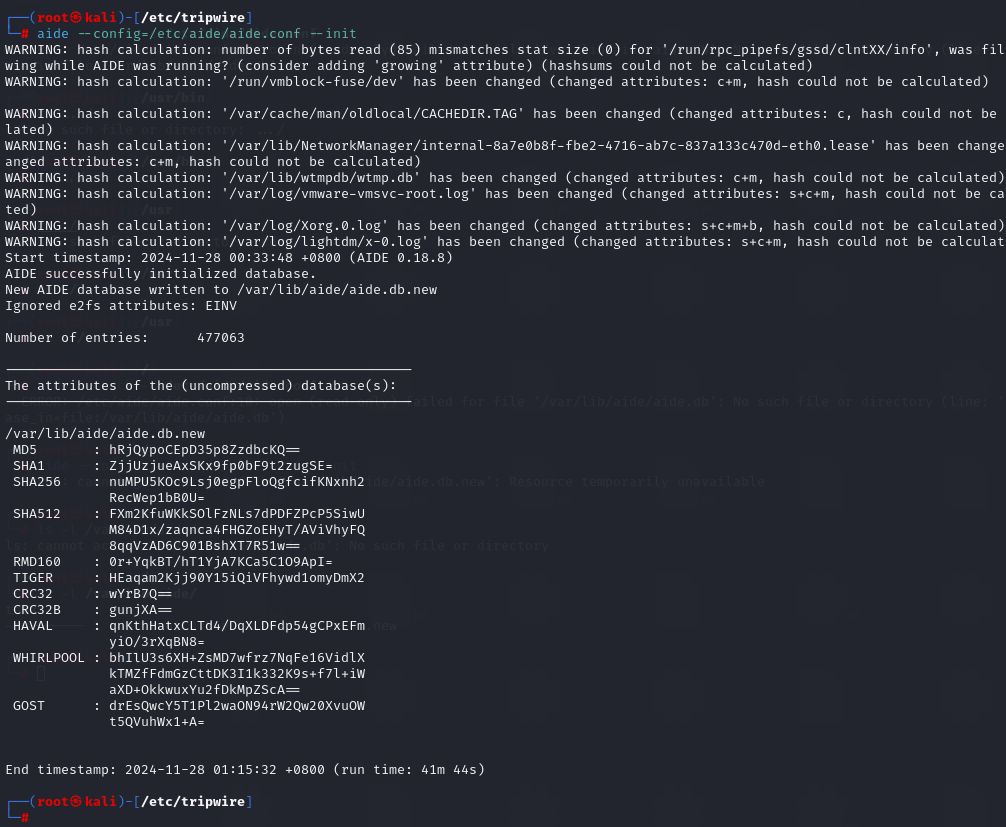
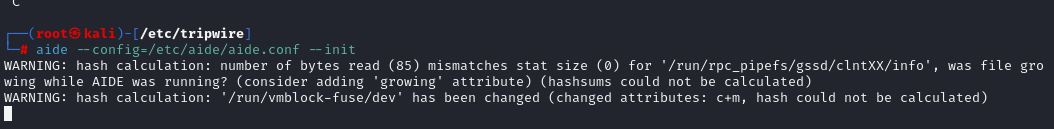
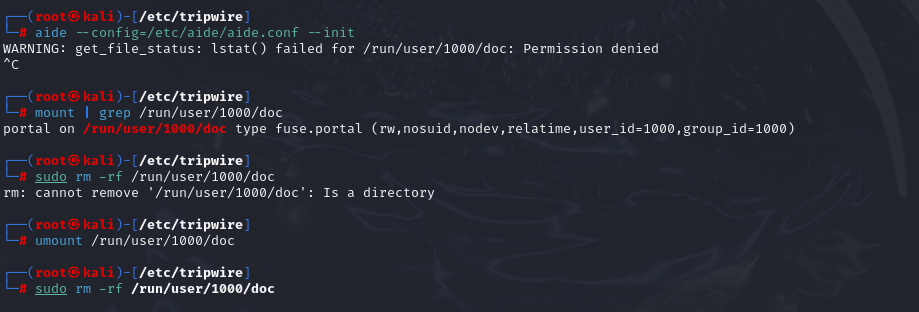
3. 使用AIDE进行系统完整性检测，具体实验步骤参考ppt。

安装aide：

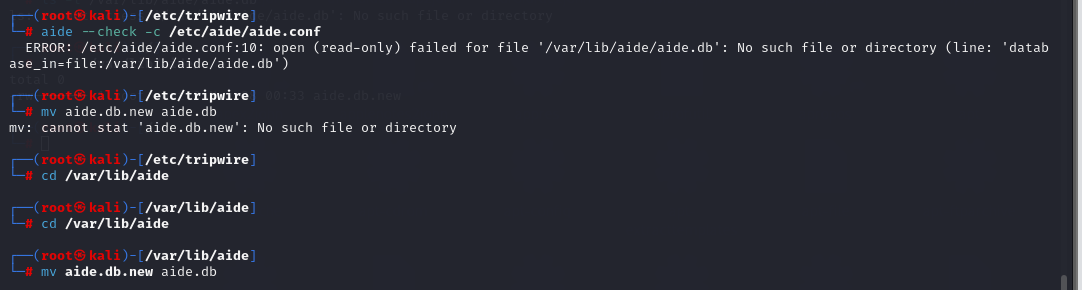


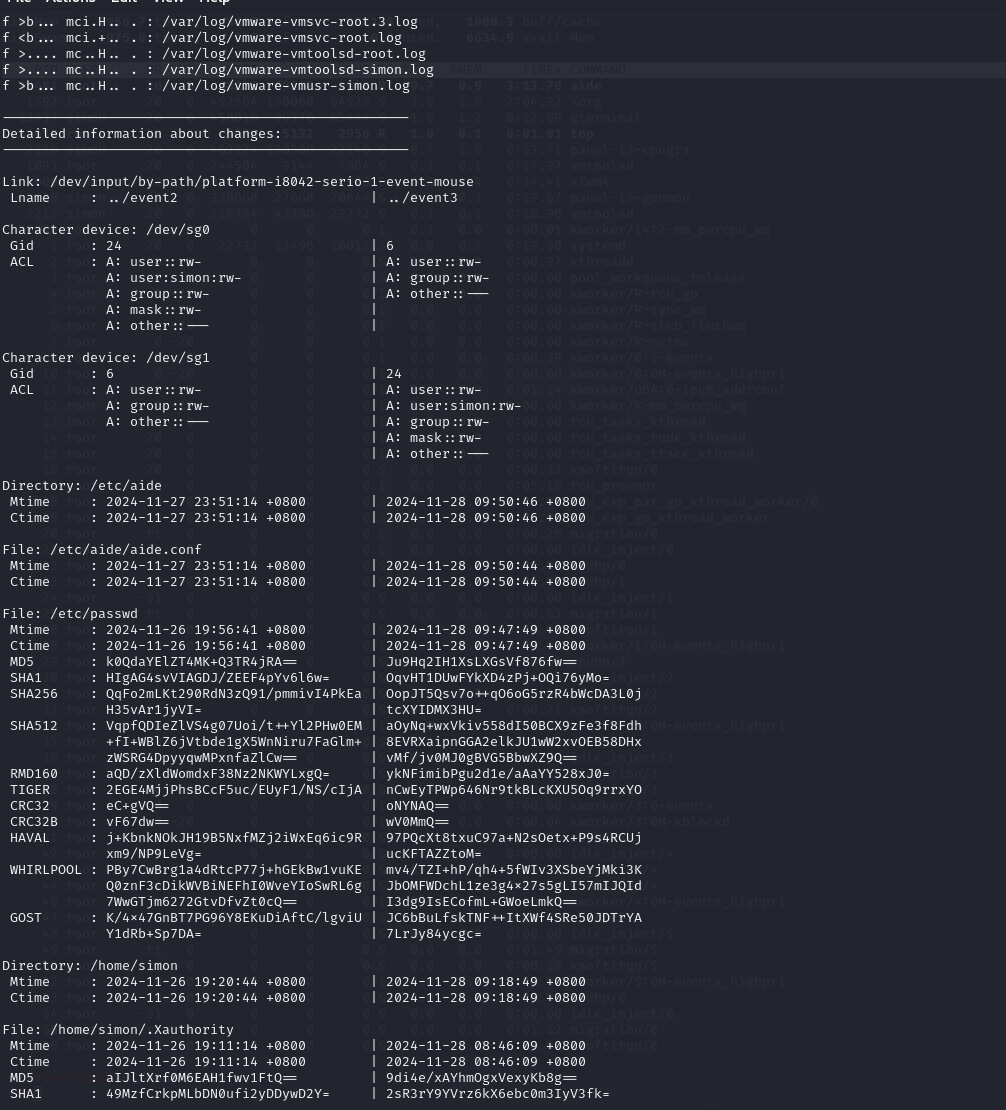
增加两行

初始化数据库

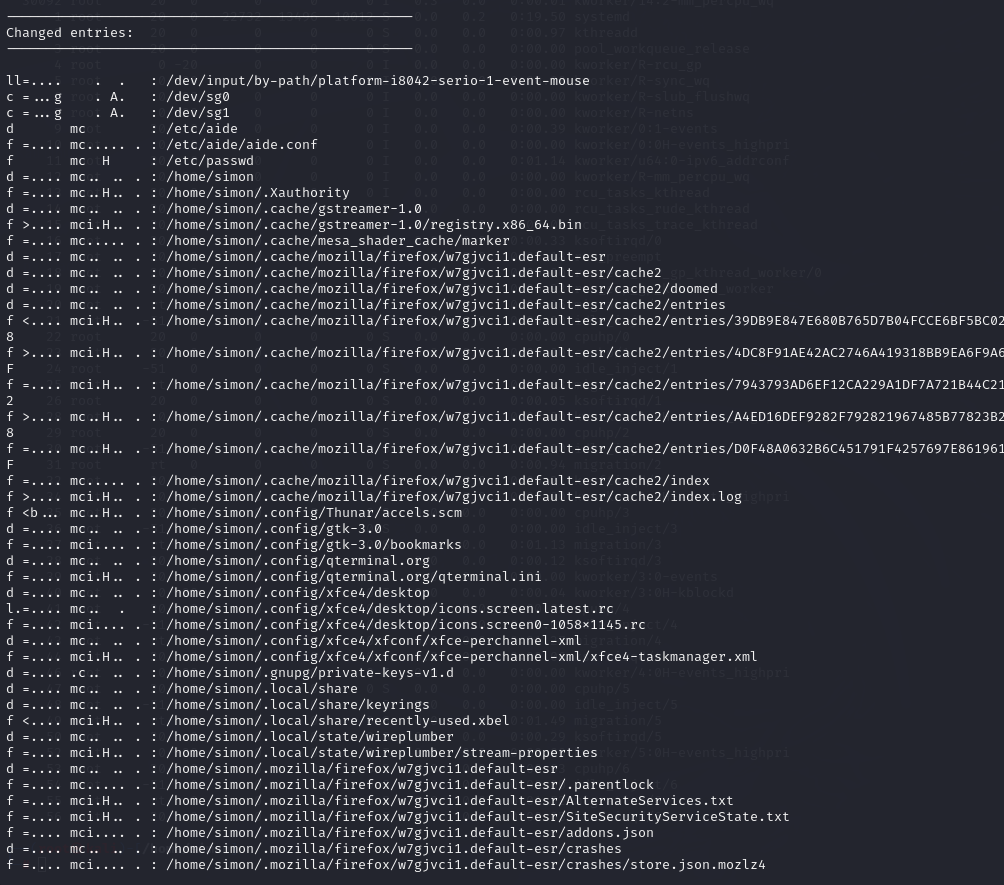


花了41分钟

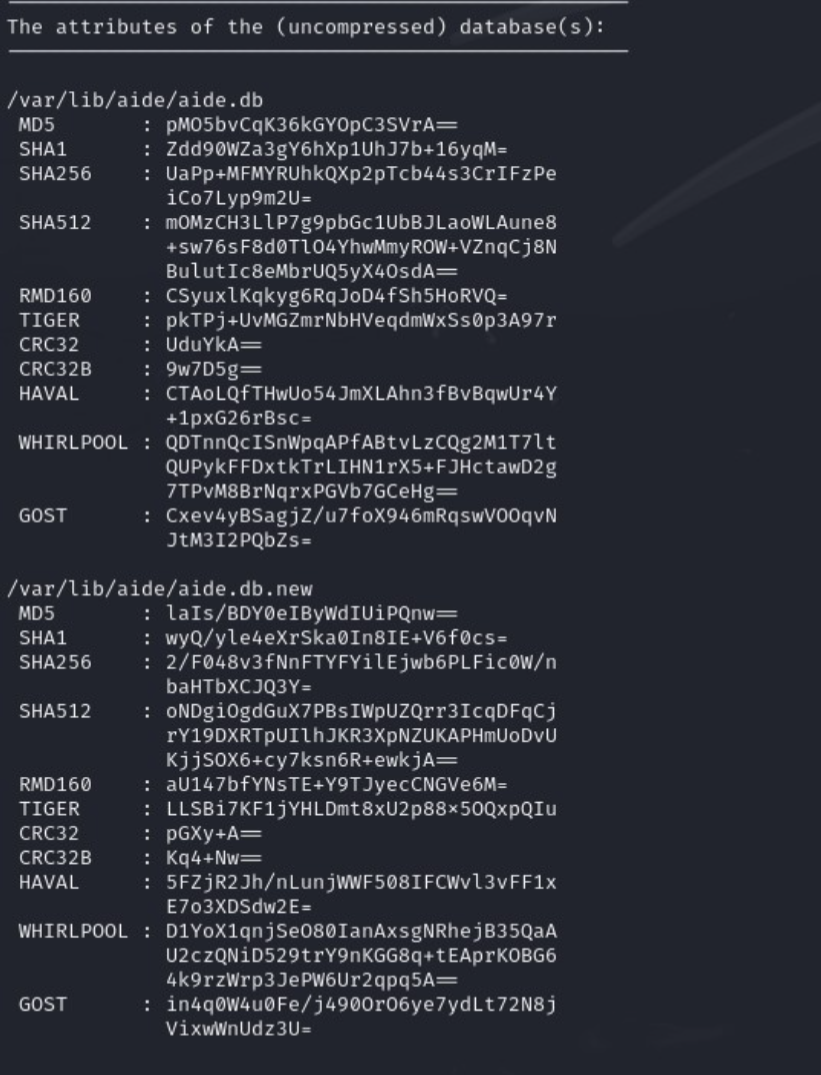


进行完整性检测

然后修改再次检查

得到

记录下的修改的地方





得到最后的差别