Linux Behavior Tracker

# 核心功能

（1）命令执行与进程链记录

Hook execve/fork/exit 等系统调用，跟踪每条命令和子进程 分配唯一 trace\_id 标识每个命令链 建立父子进程树用于归因文件修改

(2)进程Lib树

读取 /proc/<pid>/maps + ldd，每个进程加载的库都映射在：/proc/<pid>/maps，解析含有 .so 的行，得到所有动态库路径。

（3）文件访问与修改行为监控

Hook vfs\_open, vfs\_write, vfs\_unlink 等 识别写操作的意图与范围（文件名、偏移、长度） 构建每条命令关联的所有文件行为图谱

（4）文件快照管理模块

写入前对目标文件进行只读快照备份 写入完成后再次快照用于对比 快照存储采用 trace\_id+时间戳命名，支持版本管理

（5）差异分析与报告生成

对两个快照版本进行 diff 支持字节级与行级对比 输出 JSON/HTML/Markdown 等格式报告 提供摘要信息（哈希变更、增删行数等）

（6）日志记录与查询

记录所有命令、文件路径、差异报告、时间、用户等元数据 可本地持久化为 JSON、SQLite 支持按用户、路径、时间段进行查询

# 难点

（1）写前快照与竞态问题

只备份写入“前后的写入区域”（局部 diff）

1. 在 vfs\_write 之前，通过 pread(fd, offset, len) 获取这段即将被写入的区域内容 → 作为“写前局部快照”
2. 在 vfs\_write 之后，再读取相同位置的内容 → 作为“写后局部快照”
3. 对比两个片段，生成局部 diff 结果

（2）系统调用追踪与内容恢复

（3）trace\_id 与进程链追踪

（4）快照存储效率与清理

（5）eBPF 程序设计