理解赛题

增强现有Linux容器技术的文件系统隔离能力，抵御非法文件操作相关容器逃逸漏洞

其次在完成上述情况下减小性能开销

学习和问题

一，开始

1，学习

1. Linux的安装和基础使用
2. Docker的安装和基础了解
3. 要抵御漏洞，了解容器安全抵御机制
4. 复现漏洞理解漏洞攻击原理，寻求方法如何解决该漏洞

2，问题

1. 现在是通过复现漏洞来从相关方面加强，目前我能了解的加强是通过主机配置和相关权限限制来控制，比如设置文件所属权限，开启实时监控，文件异常行为检测
2. 如何编写一些检测程序来加强？怎么优化？
3. 最后是通过攻击来检测容器安全，我们如何相同的进行测试（不了解如何评判，大概通过漏洞复现可以比较慢的检测？还是说需要了解漏洞挖掘相关知识）

这个现在解决了

1. 复现结束后解决方案-安装最新版本docker？？？

二，再次思考

完全不清楚前进方向

主要目的是对现有轻量安全虚拟化技术进行优化或者提出新的方法

缺乏实践