《软件安全》实验报告

姓名：梁婧涵 学号：2112155 班级：1120

实验名称：程序插桩及Hook实验

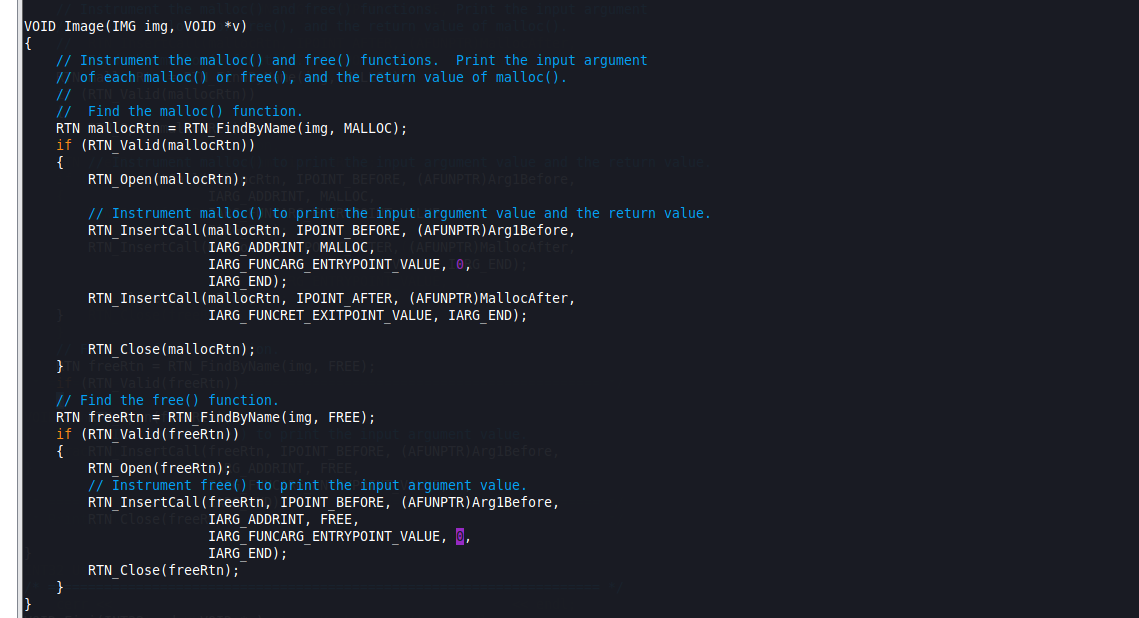
实验要求：

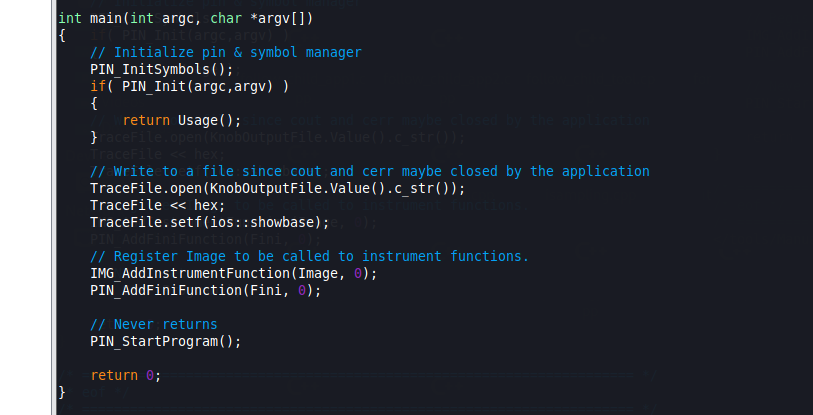
复现实验一，基于windows mypintool或在kali中复现malloctrace这个pintool，理解pin插桩工具的核心步骤和相关API，关注malloc和free函数的输出信息。

实验过程：

1.下载并安装，得到pintool工具

2.把malloctrace.cpp的代码赋值到mypintool.cpp





3.Image函数中我们根据函数名找到malloc执行（后面free函数同理），进行函数回调，记录数据。

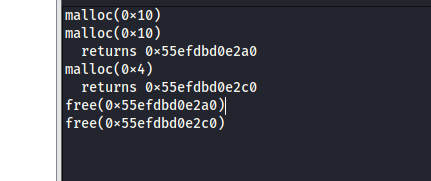
4.通过IMG\_AddInstrumentFunctionhan数注册Image的回调函数，将在加载新镜像时候执行，镜像级插桩

5.测试：首先用make mypintool.test TARGET=intel64命令生成对应的so文件

gcc编译我们的测试程序：



6.插桩：./pin -t ./source/tools/MyPinTool/obj-intel64/malloctrace.so -o my.out -- ../testcpp/malloc



追踪到了malloc语句和free，参数：4\*4，1\*4，free对应地址

心得体会：

通过本次实验了解到了插桩过程及hook实验的原理和细节，初步了解pintool工具的使用方法，在进行程序插桩和Hook实验时，我需要仔细分析程序的逻辑结构，并选择合适的插桩点或Hook点。我学会了如何使用插桩工具或编写Hook代码，以在程序执行过程中监控、修改或扩展其行为。实验中的操作过程需要耐心和细致，也需要不断的尝试和调试，这让我对实际软件开发中的调试和测试工作有了更加深刻的认识。

实验中，我通过对插桩和Hook后的程序行为进行观察和分析，得出了一些结论。我学会了如何对实验结果进行客观的评估和总结，分析插桩和Hook对程序性能、安全性、可维护性等方面的影响。同时，我也对实验中可能遇到的问题和解决方法有了更深入的认识。

通过本次实验，我对程序插桩和Hook技术有了初步的掌握，我意识到这两种技术在软件开发和安全领域中有着广泛的应用。我可以通过进一步深入研究和实践，将这两种技术应用于实际项目中，提高软件的性能、安全性和可维护性，并探索其在其他领域的应用潜力。