《漏洞利用及渗透测试基础》实验报告

姓名：沙璇 学号：1911562 班级：信息安全

**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函数的输入输出信息。

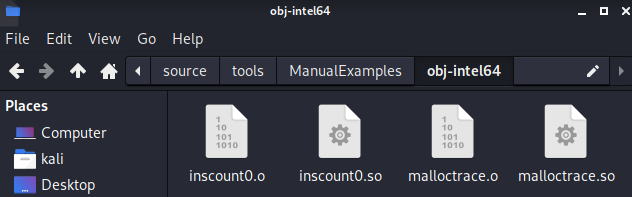
**实验过程：**

①首先，进入 source/tools/ManualExamples，对 malloctrace.cpp 进行编译来产生其对应的动态链接库：

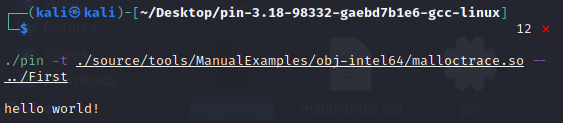




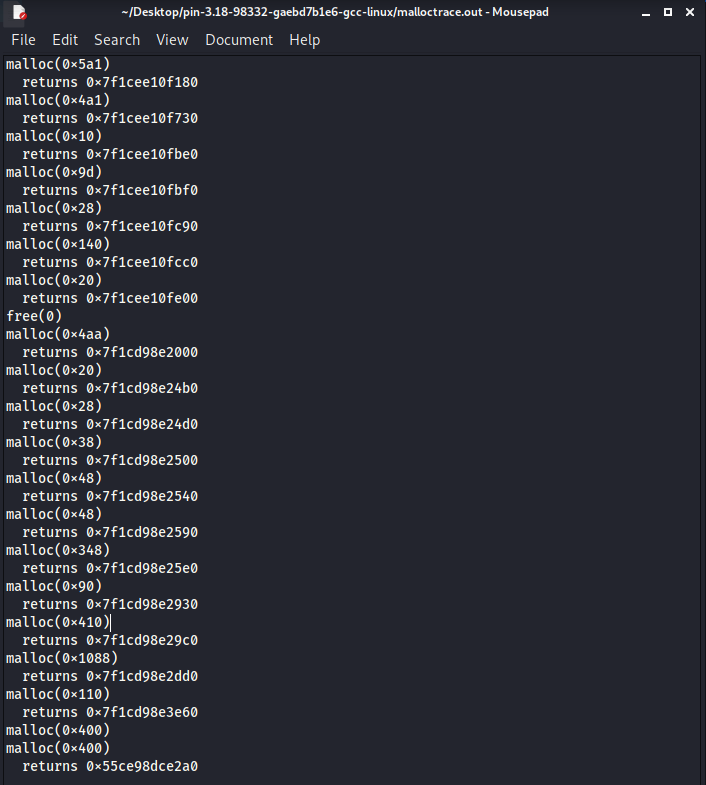
②进入 obj-intel64 文件夹确认一下，已经生成了malloctrace.so 这个动态链接库文件



编写一个简单的控制台命令程序 FirstC.c，并进行测试，

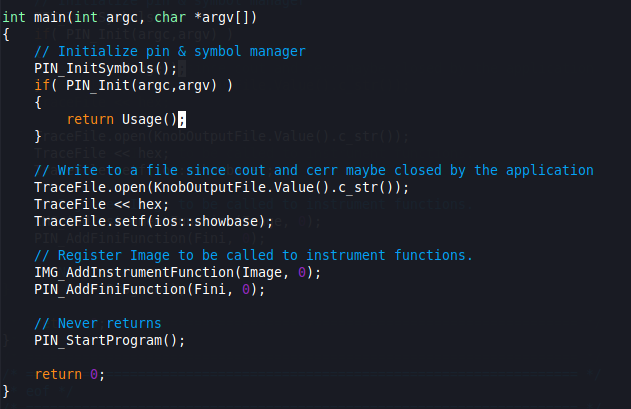


如上所示，成功执行。同时，在 pin-3.18 路径下增加了一个输出文件 malloctrace.out， 文件内容如下：



复现成功！

③打开 malloctrace.cpp 查看内容：



在 main 函数中：

初始化pin以及symbol manager。通过调用函数 PIN\_Init 完成初始化。

注册插桩函数。通过使用 INS\_AddInstrumentFunction 注册一个插桩函数，在原始程序的每哥指令被执行前，都会进入 image这个函数中。

注册退出回调函数。通过使用 PIN\_AddFiniFunction 注册一个程序退出时的回调函数 Fini，当应用退出的时候会调用函数 Fini。

启动程序。使用函数 PIN\_StartProgram 启动程序。

**心得体会：**

Pin 可以监控程序的每一步执行，提供了丰富的 API，可以在二进制程序程序运行过程中插入各种函数。