《软件安全》实验报告

姓名：张丛 学号：2113662 班级：信安一班

**实验名称：**

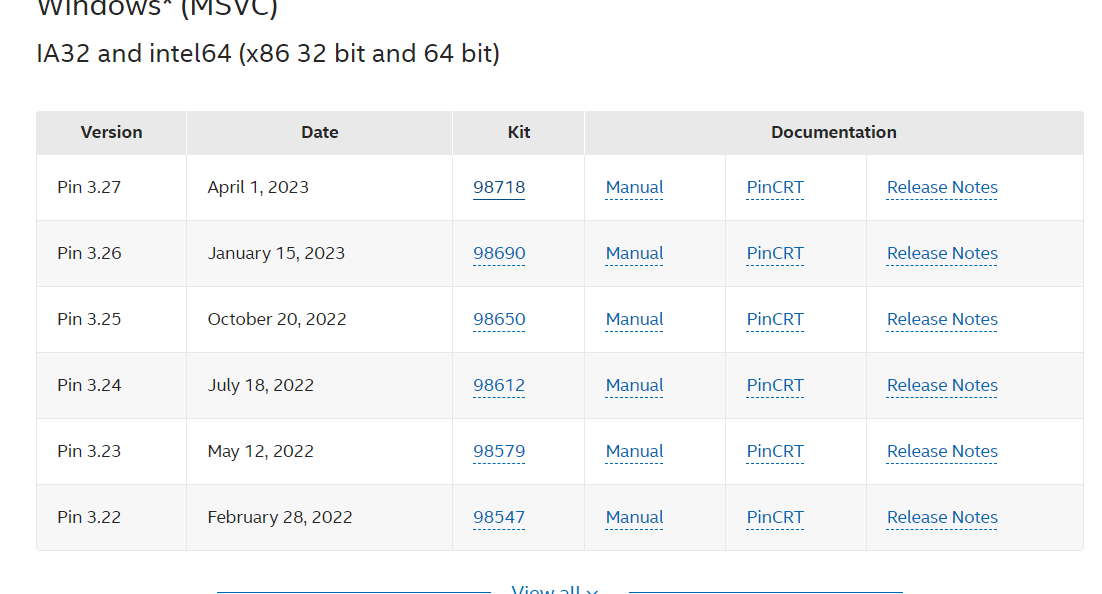
程序插桩及hook

**实验要求：**

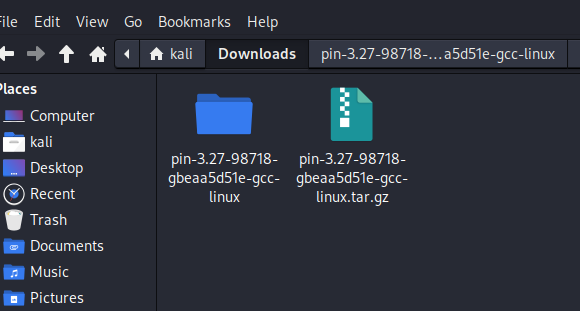
复现实验一，基于Windows MyPinTool或在Kali中复现malloctrace这个PinTool,理解Pin插桩工具的核心步骤和相关API，关注malloc和free函数的输入输出信息。

**实验过程：**

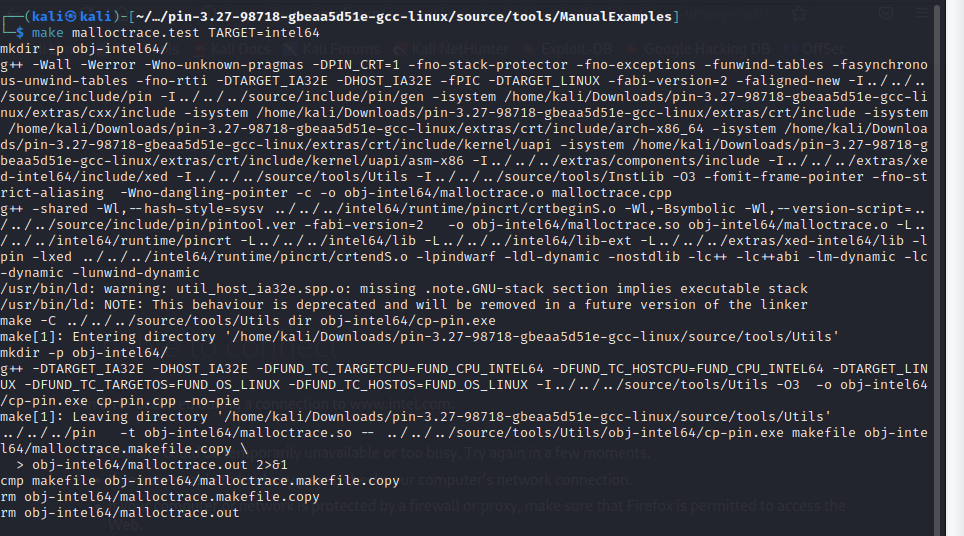
1. 通过kali的火狐浏览器下载PinTool：

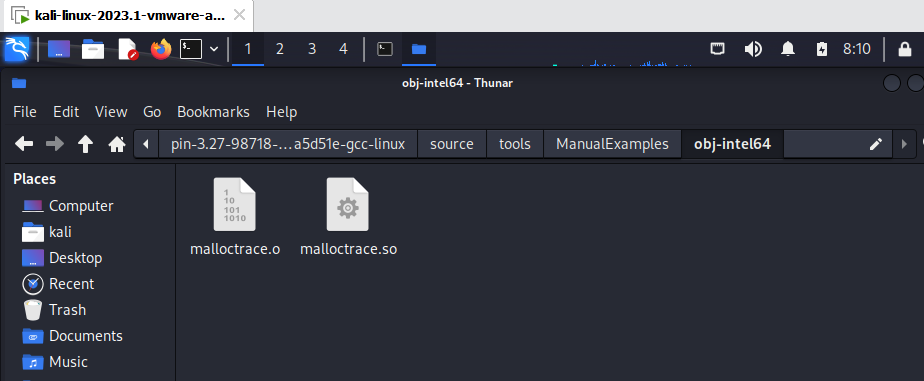


解压：

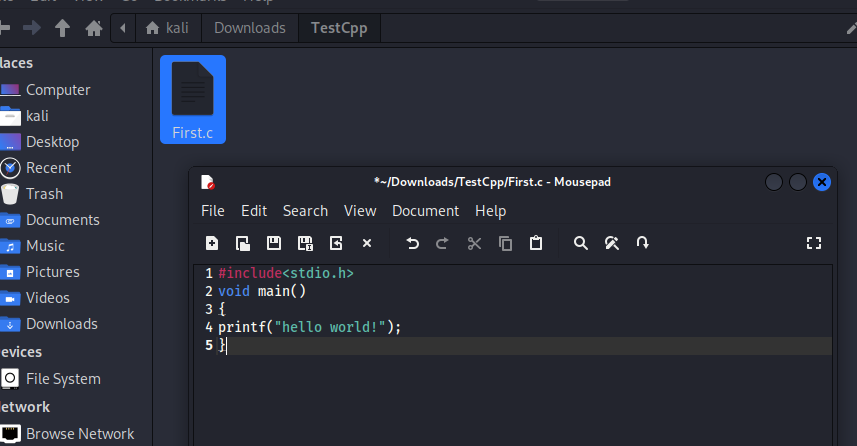


1. 编译，产生动态链接库（malloctrace.cpp）

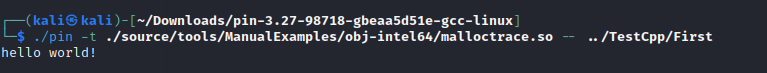




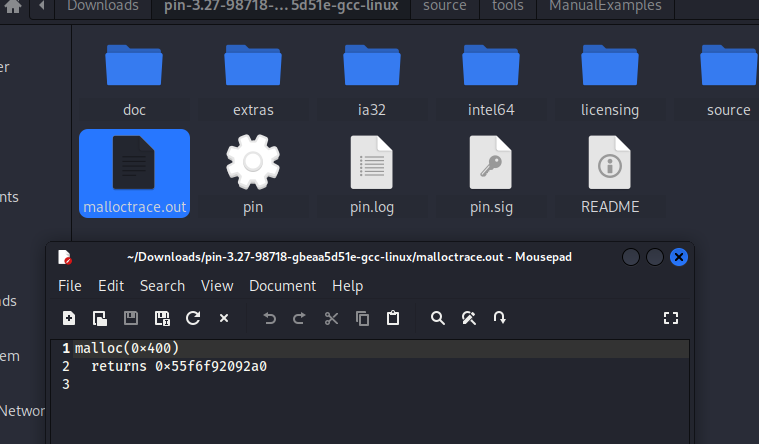
1. 编写测试程序，编译，使用Pin插桩



程序运行结果：



插桩输出文件：



1. 分析输入输出信息：

可以在文件中查看甚至修改Pin指令：



在pin工具中，每个函数的参数是从堆栈中获取的。

在Image函数中free函数使用与malloc函数相同的Arg1Before函数来捕获其参数，由于malloc函数调用先发生，使用相同的函数导致对malloc函数进行调用之后内存可能没有被释放，free函数不能捕获正确的参数，free函数可能调用失败。

**心得体会：**

通过实验，下载并运用了PinTool对程序进行了插桩。

实验PinTool进行插桩的核心步骤：

1. 编译pin文件获取相关函数的动态链接库
2. 编译测试目标程序
3. 对编译程序进行插桩

对malloc和free函数的输入输出信息有了更多了解。