《漏洞利用及渗透测试基础》实验报告

姓名：孙蕗 学号：2112060 班级： 信安1班

**实验名称：**

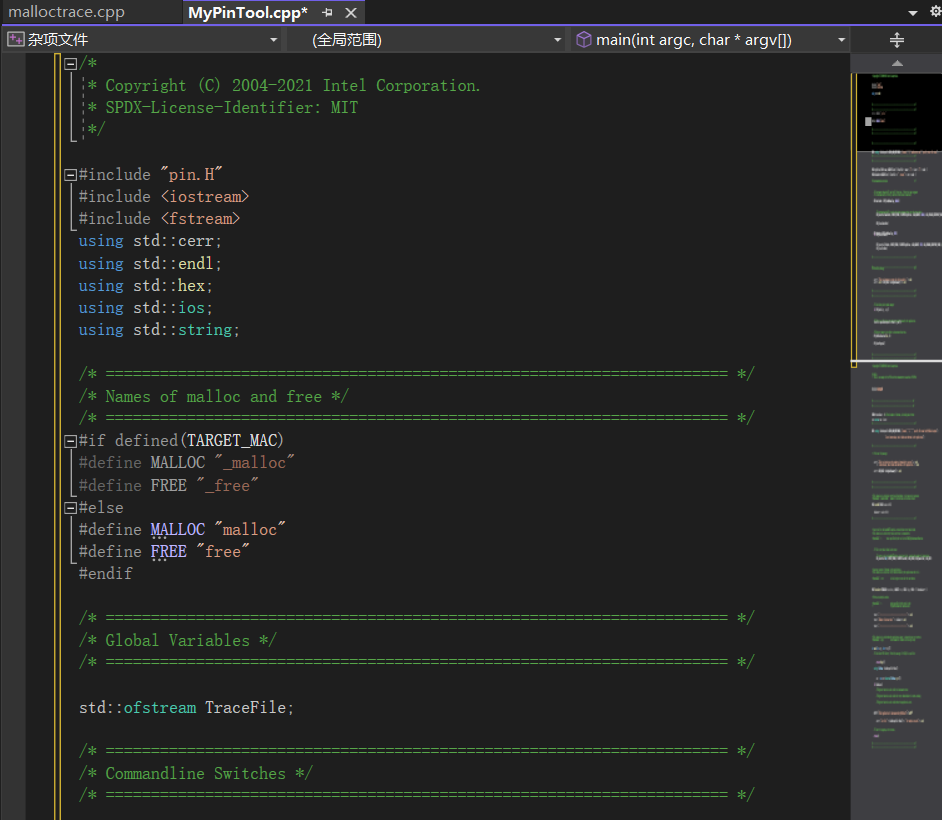
程序插桩及hook实验

**实验要求：**

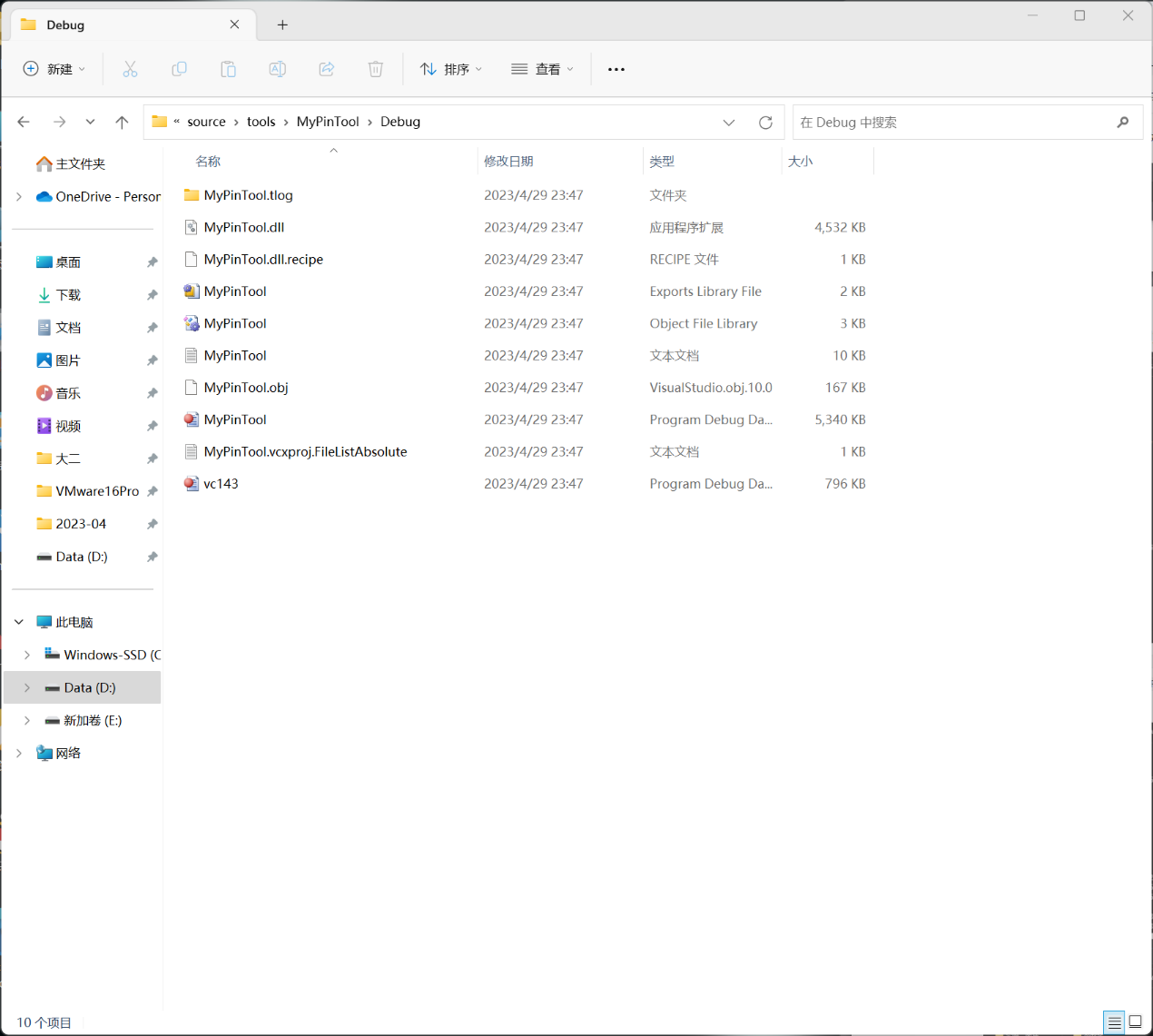
复现实验一，基于Windows MyPinTool或在Kali中复现malloctrace这个PinTool，理解Pin插桩工具的核心步骤和相关API，关注malloc和free函数的输入输出信息。

**实验过程：**

1. 修改MyPinTool.cpp文件，将malloctrace.cpp复制到mypintool.cpp中



1. 打开MyPinTool.vcxproj文件，整个项生成后，在debug路径下生成了一个MyPinTool.dll文件。



1. 使用pin命令，可以完成程序插桩

在cmd中进入D盘pin文件夹，输入指令pin -t D:\pin\source\tools\MyPinTool\Debug\MyPinTool.dll -- cmd /c dir



malloctrace.out文件

malloc(0x4000)  
malloc(0xffce)  
malloc(0xffce)  
malloc(0xffce)  
free(0x2b14638)  
free(0x2b04660)  
free(0x2af0680)  
malloc(0xffce)  
malloc(0xffce)  
free(0x2b14638)  
malloc(0xffce)

malloc(0xffce)  
malloc(0xffce)  
malloc(0xffce)  
malloc(0xffce)  
malloc(0xffd2)  
malloc(0xffd2)  
malloc(0xffce)  
malloc(0xffce)  
malloc(0xffce)  
free(0x2ba84f0)  
free(0x2b98518)  
free(0x2b88540)  
malloc(0xffce)  
free(0x2b98528)  
free(0x2b78560)  
free(0x2b68580)  
malloc(0xffce)  
free(0x2b98528)  
malloc(0xffce)  
malloc(0xffce)  
malloc(0xffce)  
malloc(0xffce)  
free(0x2bb87a8)  
free(0x2b78558)  
free(0x2b68580)  
free(0x2b98528)  
malloc(0xffd2)  
malloc(0xffce)  
free(0x2b98528)  
malloc(0xffce)  
free(0x2b98528)  
malloc(0xffce)  
free(0x2b98528)  
malloc(0xffce)  
free(0x2b98528)  
malloc(0xffce)  
free(0x2b98528)  
malloc(0xffce)  
free(0x2b98528)  
malloc(0xffce)  
free(0x2b98528)  
malloc(0xffce)  
free(0x2b98528)  
malloc(0xffce)

free(0x2b98528)  
malloc(0xffce)  
free(0x2b98528)  
malloc(0xffce)  
free(0x2b98528)  
free(0x2bb87a8)  
malloc(0xffce)  
free(0x2b98528)  
free(0x2b54598)  
free(0x2b445c0)  
free(0x2b345e8)  
free(0x2b24610)  
free(0x2b14638)  
free(0x2b04660)  
free(0x2af4688)  
malloc(0x919)  
  returns 0x10a30c60  
malloc(0x220)  
  returns 0x10a31588  
free(0x10a30c60)  
malloc(0x54)  
  returns 0x10a314f0  
malloc(0xc)  
  returns 0x10a31550  
malloc(0x18)  
  returns 0x10a31568  
free(0x10a305b8)  
free(0x10a31550)  
free(0x10a314f0)  
free(0x10a31568)  
free(0x10a30ce8)

1. 分析malloctrace.out文件

程序追踪了程序中的malloc()和free()的调用情况,多次调用malloc()和free()函数，其中malloc()的参数为分配内存的大小，free()的参数为要释放的内存地址。

**心得体会：**

Pin可以监控程序的每一步执行，提供了丰富的API，可以在二进制程序运行中插入各种函数。学习使用PinTool的基本用法，理解PinTool的基本框架，学习使用Pintool进行插桩。