**福建工程学院计算机科学与数学学院**

**实验报告**

**2024 – 2025 学年第 1 学期 任课老师： 许雪林**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **课程名称** | **软件逆向工程原理** | **班级** | **网安2202** | **学号** | **3220812128** | **姓名** | **章百琪** |
| **实验题目** | API钩取 | | **实验时间:2024.11.20** | 实验日期：  提交日期： | | | |
| **实验目的** | | | | | | | |
| （1）了解钩取的概念。  （2）掌握利用调试文件实现API钩取。 | | | | | | | |
| **实验内容** | | | | | | | |
| 1. 编写调试程序，生成exe文件，具体代码参见WriteFD文件夹；      1. 打开Notepad.exe，使用Process Explorer获取Notepad的进程ID号；   获取pid     1. 打开cmd，在提示符运行调试程序，注意要加上被调试程序的进程ID号；      1. 在记事本中输入字符，然后保存成F1.txt文件，关闭记事本；     打开F1.txt文件，注意观察保存的内容是否发生变化。    字符往后移了一位 | | | | | | | |
| **实验总结** | | | | | | | |
| 在这次API钩取的实验中，我学习了如何使用调试程序拦截和修改进程中的API调用。通过编写调试程序并附加到Notepad.exe进程，我成功地拦截了WriteFile函数，并修改了写入文件的字符内容，达到了字符往后移一位的效果。实验让我深入理解了进程调试、内存操作和API钩取技术 | | | | | | | |
| **教师评阅意见** | | | | | | | |
|  | | | | | | | |
| 教师： 年 月 日 | | | | | | | |