**《软件逆向工程》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **年级、专业、班级** | | **2022级信息安全** | | | **姓名** |  |
| **实验题目** | **PE壳设计与验证** | | | | | |
| **实验时间** | **2024/11/1** | | **实验地点** | **DS3401** | | |
| **实验成绩** |  | | **实验性质** | **□验证性 □设计性 ☑综合性** | | |
| 教师评价：  ☑算法/实验过程正确； ☑源程序/实验内容提交； ☑程序结构/实验步骤合理；  □实验结果正确； □语法、语义正确； ☑报告规范；  其他：  评价教师签名： 杨吉云 | | | | | | |
| 1. 实验目的 2. 验证PE文件结构构建 3. 验证PE文件壳的基本原理 | | | | | | |
| 二、实验项目内容   1. 用二进制编辑软件构建一个可以弹出对话框的PE文件。 2. 实现简单的跳转壳，在PE文件中添加新节，在新节其中加入跳转至原入口的指令，实现对原程序的启动。 | | | | | | |
| **三、实验过程或算法（源程序）**  实验1.用二进制编辑软件构建一个可以弹出对话框的PE文件            实验2.实现简单的跳转壳，在PE文件中添加新节，在新节其中加入跳转至原入口的指令，实现对原程序的启动 | | | | | | |
| 四、实验结果及分析和（或）源程序调试过程  实验1.用二进制编辑软件构建一个可以弹出对话框的PE文件   1. 编写MZ、NZ头   MZ:    NZ:     1. 编写section table      1. 编写.code节      1. 编写.data节      1. 编写.idata节      1. 运行exe文件，弹出对话框，成功     实验2.实现简单的跳转壳，在PE文件中添加新节，在新节其中加入跳转至原入口的指令，实现对原程序的启动   1. 修改PE头中NumberOfSections中的3为4，增加一个节表，命名为.shell，作为壳所在节，并在原节表末端插入200h为创建新节表的空间，将PointerToRawData加上200h对齐修改后的偏移地址。   NumberOfSections修改为4    .shell节表：    在原PE文件末端补上.shell节表的节区，大小为200h个字节    修改PE头中的SizeOfImage，把原来的值加上PE头中的SectionAlignment的值（即1000h）  修改前：    修改后：    修改PE头中的AddressOfEntryPoint为.shell的VirtualAddress  修改前：（1000h）    修改后：（4000h）     1. 在olldbg中打开修改后的PE.exe文件   因为修改了程序入口地址，初始显示地址就是00404000h，即.shell节的内容    双击，在弹出窗口输入JMP 00401000    点击汇编，选择写入的JMP指令右键->复制到可执行文件->选择，保存为另外一个exe文件，该exe文件在.shell节中补充了JMP代码实现跳转功能     1. 运行exe文件，成功弹出对话框   成功跳转到原程序入口地址00401000h，跳转壳实现成功    弹出对话框： | | | | | | |