**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** | **常用的汇编指令** | | **实验时间:2024.9.26** | 实验日期：  提交日期： | | | |
| **实验目的** | | | | | | | |
| （1）掌握X86体系结构。  （2）掌握常用的汇编指令。  （3）掌握OD下调试可执行文件过程。 | | | | | | | |
| **实验内容** | | | | | | | |
| 1. 用OD工具打开一个exe文件，找出能够证明X86体系属于小端序的依据；   修改程序中的一个指针指向的地址值成12345678    将该指令设为新的epi，单步执行    检查对应的数据区域    对应的16进制数据值为78563412，由此可证，此程序为小端序   1. 在已经打开的内存空间中，练习以下指令： 2. 给一个存储单元赋数值87654321；   找到一个mov指令，将赋予的值修改成87654321    设置为新的epi，单步执行，检查数据区域    成功写入   1. 给寄存器EAX赋值12345678；   找到一个mov指令，将指令修改成    设置为新epi，单步执行，查看寄存器内的值    成功放入   1. 把（1）存储单元的数据赋给寄存器EAX；     设置为新epi，单步执行，查看寄存器窗口数据值    修改成对应的87654321  （4）将数值51H和52H相加，结果保存到EAX中，观察标志寄存器的变化；  将指令修改成这两条，将第一条设置为新epi，单步执行，查看寄存器区域内的变化    第一步    第二步    标志位没有发生变化，将数值改为61H和0A3H    执行    p标志位改变   1. 将EAX和EAX进行异或，观察哪些数据发生了变化；   添加新的指令，进行eax的异或    单步执行     1. 执行INC EAX指令，观察哪些数据发生了变化；     寄存器内eax值加一，p标志和z标志变为0     1. 把地址信息赋值给EDX，然后用EDX作为指针，将数据12345678赋值给指向的存储单元。   将要存放的地址通过lea指令赋给eax，再以eax值为地址，将对应的数据区域的值修改    对应地址的数据修改成功    2.观察在OD中，如何构造数组，尝试编写一段简单的汇编语言程序对数组进行读写操作，然后累加，累加和保存在指定的存储单元中。 | | | | | | | |
| **实验总结** | | | | | | | |
| 在这次实验中，我通过使用 OD（OllyDbg）工具，深入理解了 X86 体系结构和汇编语言指令的执行过程。整个实验让我对软件逆向工程的核心概念有了更清晰的认识，特别是以下几个方面的收获：  小端序的验证：通过修改内存中的数据，我成功地验证了 X86 架构采用小端序的存储方式。在将值 12345678 写入内存后，读取到的值为 78563412，这证明了数据在内存中是按小端方式存储的。这一实验让我进一步理解了 CPU 如何处理和存储数据，特别是在不同架构下的存储差异。  汇编指令的调试和修改：实验中，通过 OD 工具，我练习了多条汇编指令的执行过程，例如 MOV、XOR、ADD 和 INC 等。在实际操作中，我修改了 EAX 寄存器的值，观察寄存器和标志位的变化。这让我对汇编指令如何影响 CPU 的状态、如何影响标志寄存器有了更直观的理解。 | | | | | | | |
| **教师评阅意见** | | | | | | | |
|  | | | | | | | |
| 教师： 年 月 日 | | | | | | | |