

**汇编语言与逆向技术**

**课程实验报告**

**实验十： CTF（Capture The Flag）**

****

学 院 网络空间安全

专 业 信息安全

学 号 2212998

姓 名 胡博浩

班 级­­­­ 2022级信息安全

1. **实验目的**
   1. 熟悉静态反汇编工具IDA Freeware；
   2. 掌握对二进制代码内部逻辑关系的分析；
   3. 掌握对二进制代码的修改和保存。
2. **实验原理**
3. CTF

CTF是一种流行的信息安全竞赛形式，可意译为“夺旗赛”。其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。

CTF竞赛模式具体分为以下三类：

一、解题模式（Jeopardy）

在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含**逆向分析**、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。

二、攻防模式（Attack-Defense）

在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。

三、混合模式（Mix）

结合了解题模式与攻防模式的CTF[赛制](https://baike.baidu.com/item/%E8%B5%9B%E5%88%B6)，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。

1. 解题

Flag隐藏在game.exe的二进制代码中。通过对game.exe的修改，使game.exe能够顺利的执行，完成对Flag的解密。

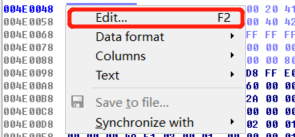


1. 技巧A：利用IDA Pro修改静态资源

* 第一步，在反汇编代码中（IDA View）找到静态资源。

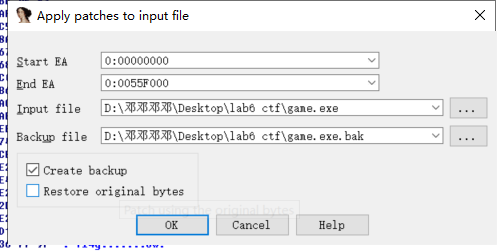


* 第二步，在十六进制视图中（Hex View）找到指定区域，右键选择Edit对资源进行修改。修改完毕后，右键选择Apply changes应用修改。





* 第三步，点击Edit->Patch program->Apply patches to input file，建议选中创建备份的选项，完成修改。

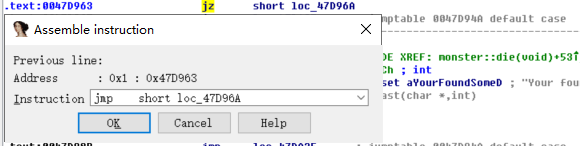


1. 技巧B：利用IDA Pro修改汇编指令

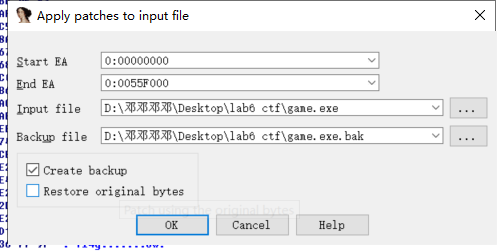
* 第一步，在反汇编代码中（IDA View）找到需要修改的汇编指令。



* 第二步，点击Edit->Patch program->Assemble，输入新的汇编指令。



* 第三步，点击Edit->Patch program->Apply patches to input file，建议选中创建备份的选项，完成修改。



1. **实验步骤**

1. 逆向分析game.exe二进制代码的主要逻辑结构和重要数据。

1）查找主要函数和流程：使用反汇编工具打开game.exe，查找程序的入口点，然后分析主要函数和流程。

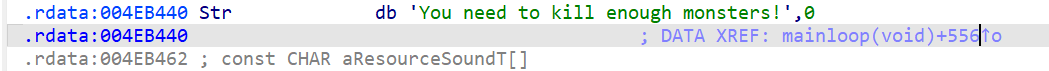
对于game.exe程序，它的主要流程如下：

首先，整个程序一共分为了4个关卡，四个关卡对应四个地图，玩家需要操控主角通过这四个关卡，然后会回到最开始的关卡，在这个关卡的地图的下方的海边找到最后的NPC并与之对话就可以得到最后的flag。

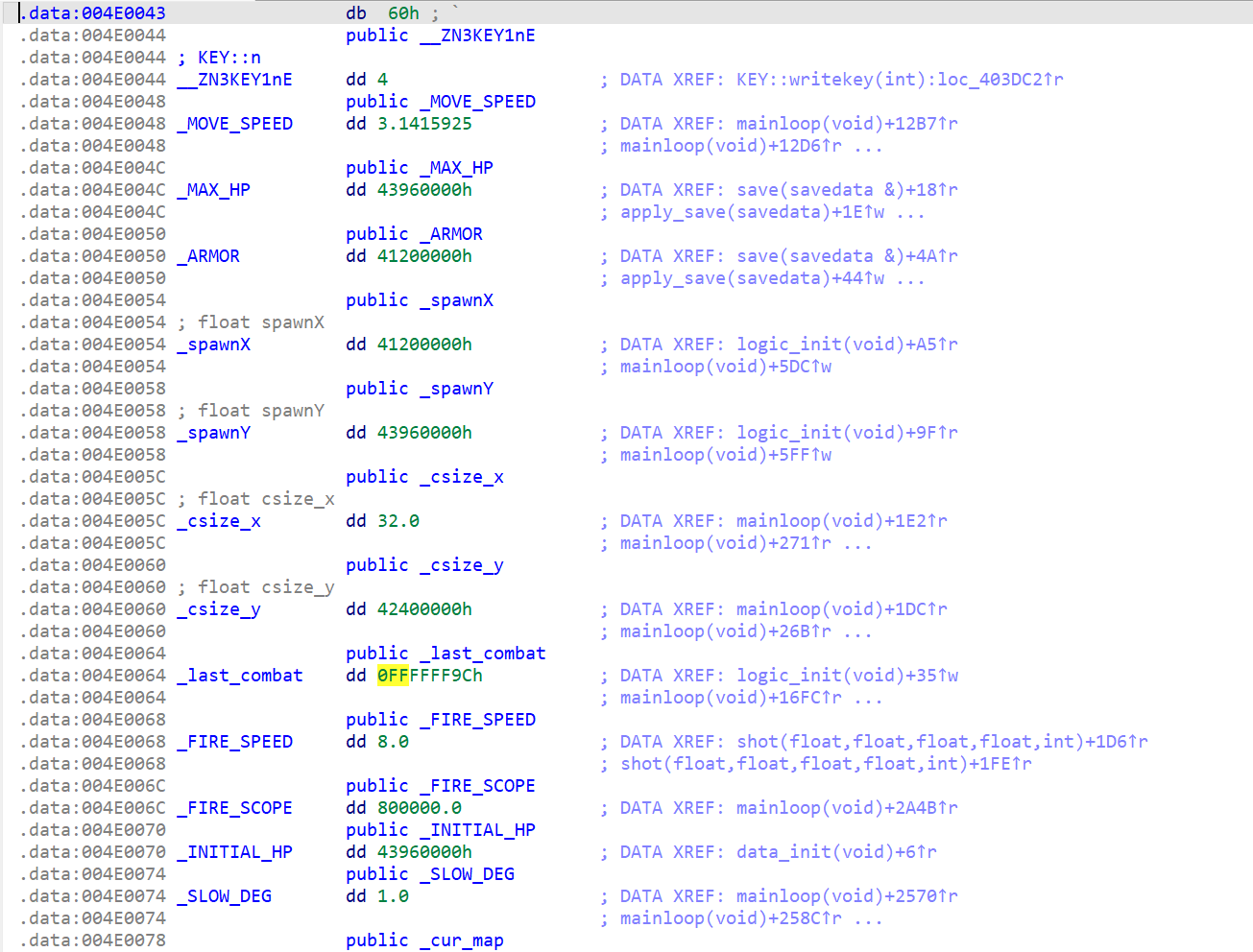


2）理解关卡切换条件：找到关卡切换的条件判断语句。

对于这四个关卡，每个关卡的通关条件是要击杀足够多的怪物，只有击杀的怪物数量足够后，才能进入下一个关卡。

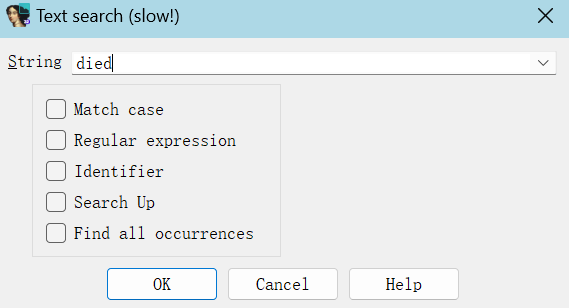


3）识别主角和怪物的关键数据：查找和理解主角和怪物的血量、移速、攻击范围、攻击力等关键数据的使用方式。



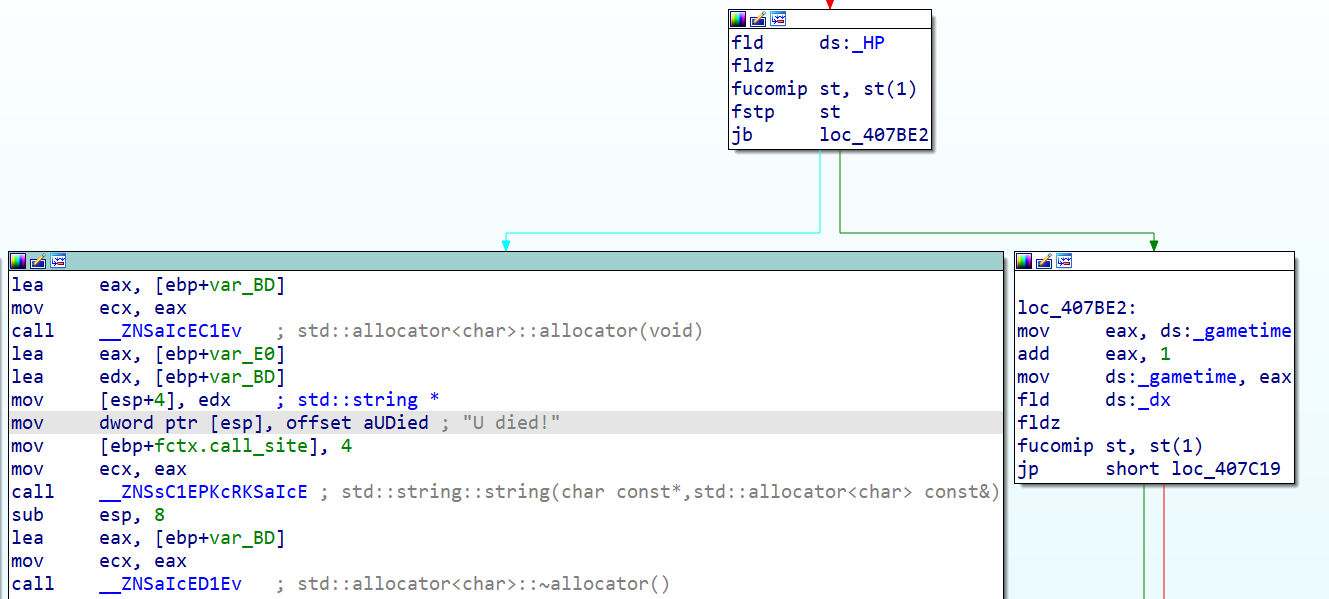
2. 修改game.exe二进制代码， 在实验报告中说明代码修改的具体过程。

1）打开游戏进行体验。体验后发现，角色死亡后，屏幕上显示“died”,因此在idapro中搜索此字符串，来找到游戏人物死亡判定的代码



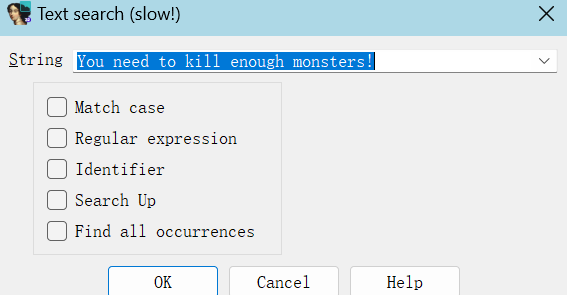
****

跳转到程序代码中，将jb改成jmp，就实现了不死的功能。

****

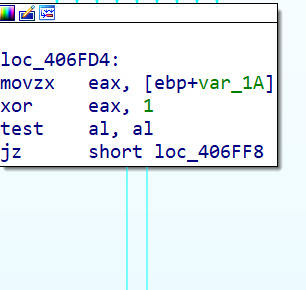
2）继续闯关，进入下一关时却给出如下提示：You need to kill enough monsters!

再次利用ida pro搜索字符串You need to kill enough monsters!





跳转到程序代码中，将jz改成jmp，就可以直接开始下一关。

****

3）继续游戏，没有其他问题，游戏通关。

1. **实验结果**

运行游戏，未再出现相关失败提示，最后通关并得到flag:

flag{a2fdkd80xo}

