《软件安全》实验报告

姓名：曹瑜 学号：2212794 班级：密码科学与技术

**实验名称：**

堆溢出Dword Shoot模拟实验

**实验要求：**

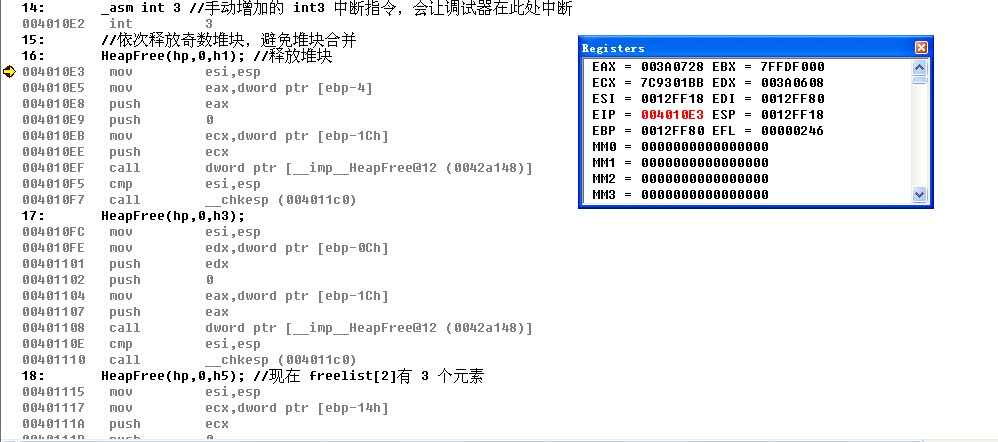
以第四章示例4-4代码为准，在VC IDE中进行调试，观察堆管理结构，记录Unlink节点时的双向空闲链表的状态变化，了解堆溢出漏洞下的Dword Shoot攻击。

**实验过程：**

1. 进入VC反汇编



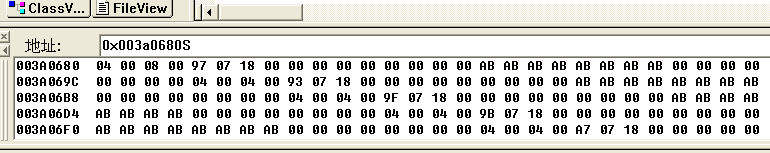
1. 观察堆管理结构



1. 记录链表状态变化：

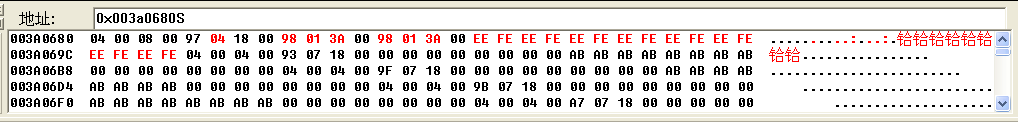
转到source处：

h1的块首地址为0x003a0688，块身地址为0x3a0680，执行前块身内容为0



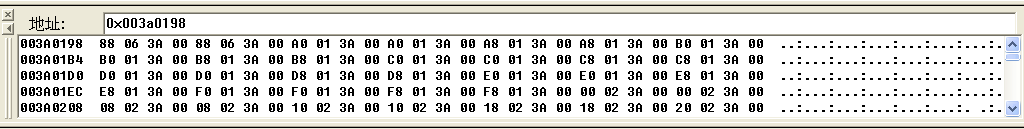
执行释放h1命令后：

Flink blink均发生改变为0x003a0198，即指向freelist[2]表



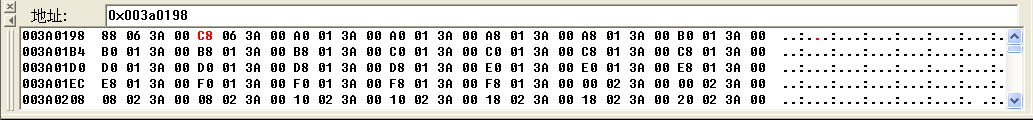
转到0x003a0198后，其前后项指针均为0x003a0688

表明此时freelist[2]中只存有h1；

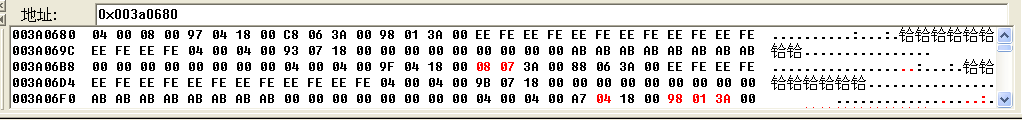


再执行释放h3的指令，此时freelist[2]的Blink发生了改变

变为0x003a06c8（指向h3）；

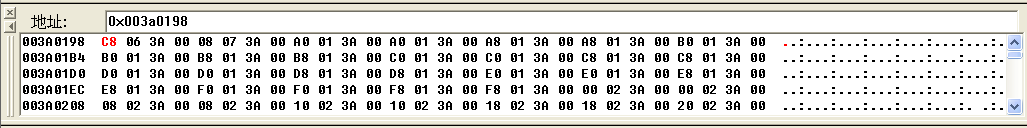


继续执行，h5也被放入freelist[2]



此时链表状态为：**freelist[2]<=>h1<=>h3<=>h5**

再执行移除h1的命令，观察0x003a0198地址处（freelist[2]）

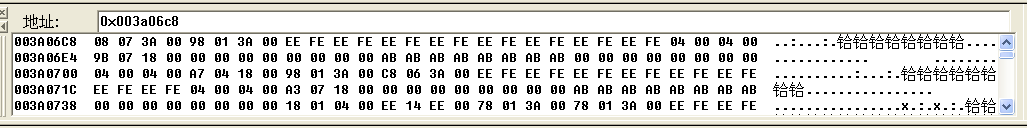


freelist[2]的Flink发生变化

实际发生了将 h1\_blink（值为 0x003a0198）地址处的值写为 h1\_flink的值的操作

此时观察h3处，其blink指向freelist[2]

实际发生了将 h1\_flink（值为 0x003a06c8）地址处的值写为 h1\_blink的值的操作



若在执行最后一条语句前修改h1的指针值，即可完成一次Dword Shoot攻击

**心得体会：**

通过实验，观察了堆管理结构，完成了堆的分配和释放，在vc6中观察了堆内存状态变化，了解了Dword Shoot攻击的发生原理；