《堆溢出 Dword Shoot 模拟实验》实验报告

姓名：田晋宇　　学号：2212039　　班级：

实验名称：

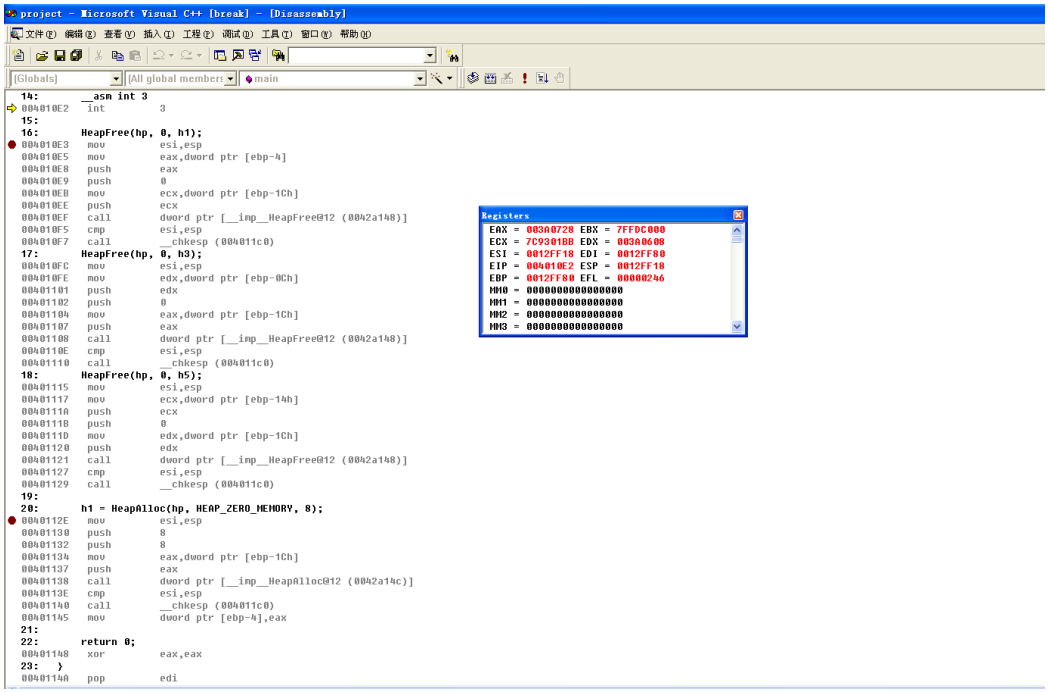
堆溢出 Dword Shoot 模拟实验

实验要求：

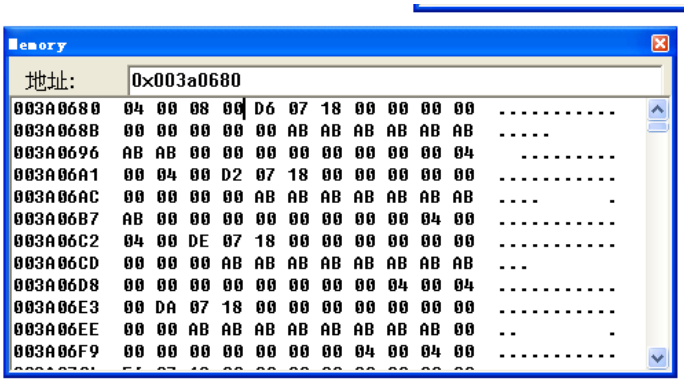
以第四章示例 4-4 代码为准，在 VC-IDE 中进行调试，观察对管理结构，记录 Unlike 节点时的双向空闲链表的状态变化，了解堆溢出漏洞下的 Dword Shoot 攻击。

实验过程：

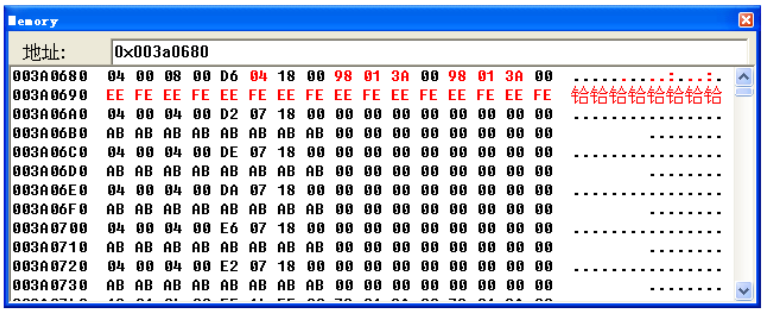
1. 将代码复制到 VC6 之后进入反汇编模式



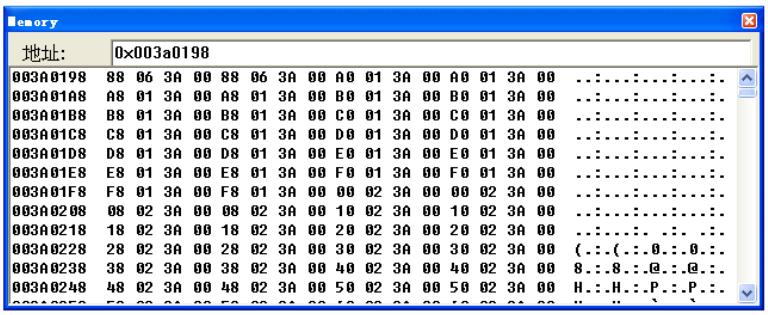
2. 找到 h1 申请的空间的地址，在 Memory 窗口中找到该地址，前 8 个字节存放块首相关信息，后面为块身的内容。



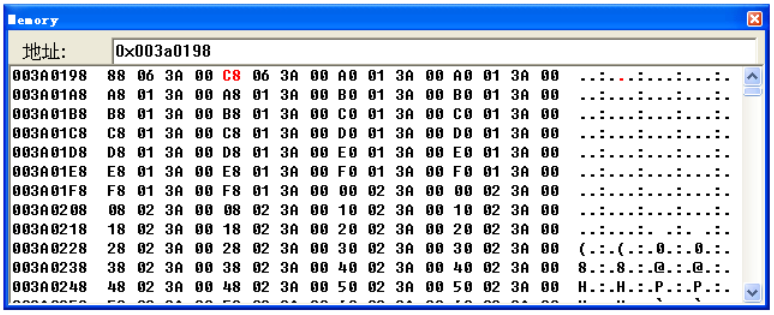
2. 执行释放 h1 空间的指令后，h1 被放入空闲堆链表中，此时块首发生改变，表示该堆为空闲状态，块身的信息表示在空闲堆双向链表中的前向指针和后向指针，由于此时链表中只有 h1 一个空闲块，因此前向后向指针值均为 00 3A 01 98。



3. 跳转到地址 00 3A 01 98，可以看到块首的信息只有被释放的 h1 空闲块。



4. 运行下一条指令之后，我们可以发现后向指针发生了改变，指向了刚刚释放的 h3。H5 释放的操作同理。



5. 执行 h1=HeapA1oc(hp.HEAP ZERO MEMORY8)后，h3 的后向指针变为 free[2]的地址，free[2]的前向指针变为 h3 的地址，这表明 h1 的前向指针的值(003a06c8)写入了 h1 后向指针指向的地址(003a0198)，那么我们可以通过堆溢出修改这两个值来实现 dword shoot。

心得体会：

理解了 Dword Shoot 攻击的原理，掌握了自助申请堆并进行管理的方法，以及对程序的堆管理有了更深刻的认知