

## DWord Shoot 软件破解实验

姓名： 汤清云 学号： 2013536

### 实验目的：

- 在 VC6.0 中使用 IDE 逐步调试
- 观察堆管理结构
- 记录 Unlink 节点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

### 实验报告：

#### 1. 逐步调试如下

初始地址：

Hp:0x003a0000

H1: 0x003a0688

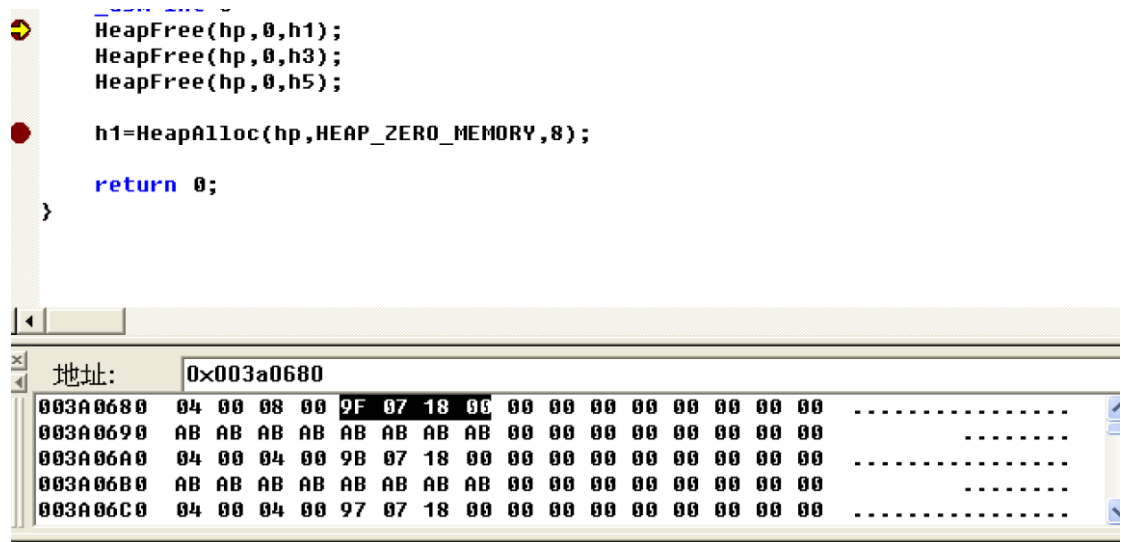
H2: 0x003a06a8

H3: 0x003a06c8

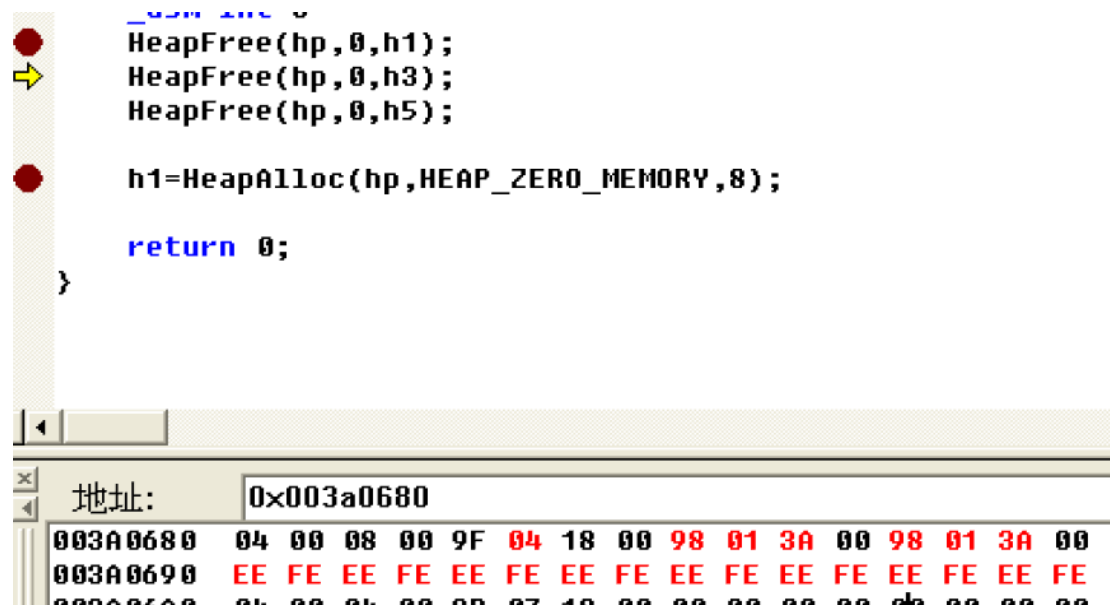
H4: 0x003a06e8

H5: 0x003a0708

H6: 0x003a0728

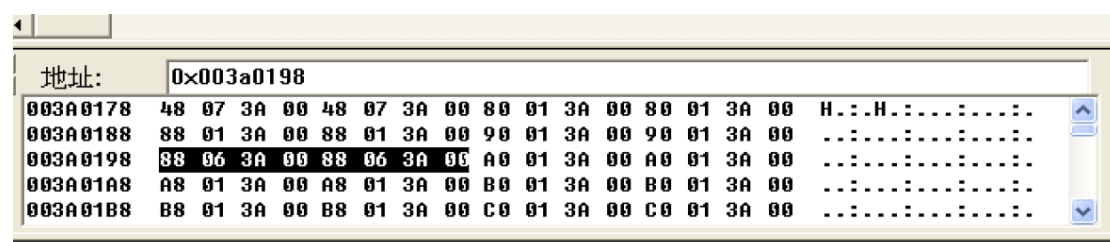


此时按下 F10:



即此时 h1 的 flink, blink 均指向 003a0198 (即空闲链表 f2)。

而 f2 的 flink, blink 均指向 003a0688 (即 h1 的块身)。



此时再次按下 F10:

地址:	0x003a0198																
003A0178	48	07	3A	00	48	07	3A	00	80	01	3A	00	80	01	3A	00	H...H.....
003A0188	88	01	3A	00	88	01	3A	00	90	01	3A	00	90	01	3A	00	.....
003A0198	88	06	3A	00	C8	06	3A	00	A0	01	3A	00	A0	01	3A	00	.....
003A01A8	A8	01	3A	00	A8	01	3A	00	B0	01	3A	00	B0	01	3A	00	.....
003A01B8	B8	01	3A	00	B8	01	3A	00	C0	01	3A	00	C0	01	3A	00	.....

F2 的 link 变为 003a06c8 (h3 的地址)

地址:		0x003a0680														
003A0660	80 06 3A 00 00 00 3B 00 0F 00 00 00 01 00 00 00	.....;														
003A0670	88 05 3A 00 00 00 00 00 40 07 3A 00 00 00 00 00	.....@.....														
003A0680	04 00 08 00 9F 04 18 00 C8 06 3A 00 98 01 3A 00	.....														
003A0690	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	铅铅铅铅铅铅铅														
003A06A0	04 00 04 00 9B 07 18 00 00 00 00 00 00 00 00 00	.....														

H1 的 flink 变为 003a06c8 (h3 的地址)

地址:		0x003a06c0															
003A06A0	04 00 04 00 9B 07 18 00 00 00 00 00 00 00 00 00	.....															
003A06B0	AB AB AB AB AB AB AB AB 00 00 00 00 00 00 00 00	.....															
003A06C0	04 00 04 00 97 04 18 00 98 01 3A 00 88 06 3A 00	.....															
003A06D0	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	铅铅铅铅铅铅铅铅															
003A06E0	04 00 04 00 93 07 18 00 00 00 00 00 00 00 00 00	.....															

Loaded 'ntdll.dll': no matching symbolic information found

此时 h3 的 flink, blink 也分别指向 f2 和 h1, 再次按下 F10:

地址:	0x003a0198																
003A0178	48	07	3A	00	48	07	3A	00	80	01	3A	00	80	01	3A	00	H...H.....
003A0188	88	01	3A	00	88	01	3A	00	90	01	3A	00	90	01	3A	00	.....
003A0198	88	06	3A	00	08	07	3A	00	A0	01	3A	00	A0	01	3A	00	.....
003A01A8	A8	01	3A	00	A8	01	3A	00	B0	01	3A	00	B0	01	3A	00	.....
003A01B8	B8	01	3A	00	B8	01	3A	00	C0	01	3A	00	C0	01	3A	00	.....

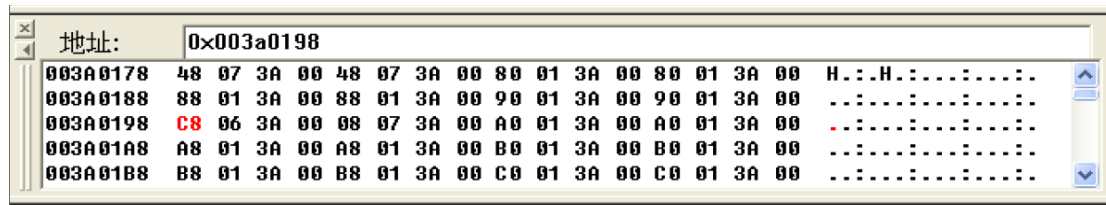
F2 变为 003a0708 (h5)

地址:		0x003a0680															
003A0660	80 06 3A 00 00 00 3B 00 0F 00 00 00 01 00 00 00	.....;															
003A0670	88 05 3A 00 00 00 00 00 40 07 3A 00 00 00 00 00	.....@.....															
003A0680	04 00 08 00 9F 04 18 00 C8 06 3A 00 98 01 3A 00	.....															
003A0690	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	铅铅铅铅铅铅铅铅															
003A06A0	04 00 04 00 9B 07 18 00 00 00 00 00 00 00 00 00	.....															

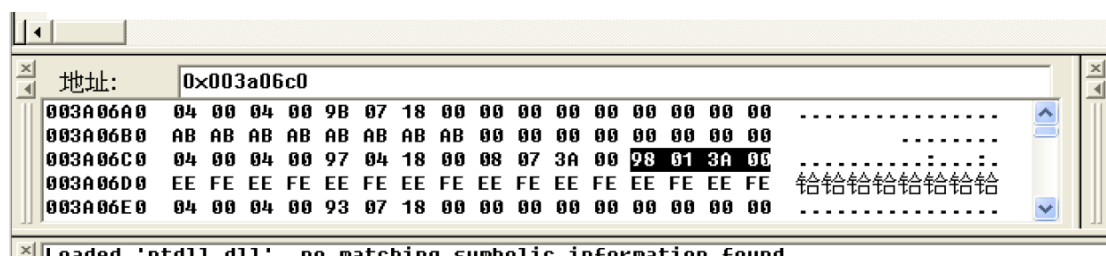
F2 指向 h5, h5 的 flink 指向 f2, blink 指向 h3, h3 的 flink 指向 h5, blink 指

向 h1, h1 的 flink 指向 h3, blink 指向 f2

即: (front) f2—h5—h3—h1 (back), 不更改代码向下执行:

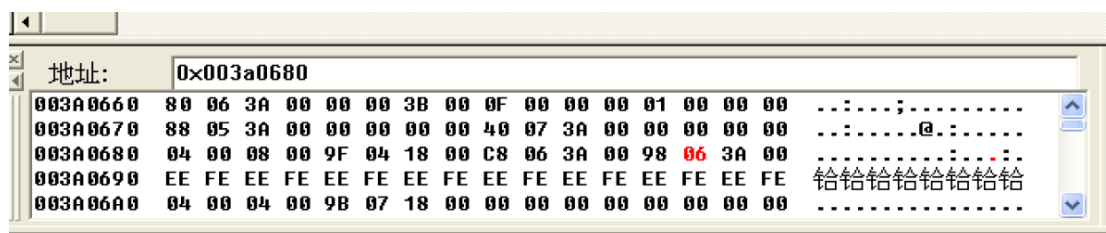


F2 指向了 003a06c8 (h3 块身), 说明 h1 被摘走, 再去查看 h3 的 blink, 变化为指向 f2:

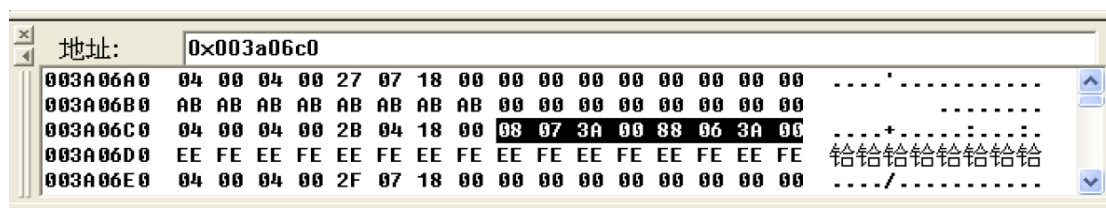


即: (front) f2—h5—h3 (back)

若篡改 h1 的 blink 为 003a0698:



再进行下一步时即发生 dword shoot



H3 的 blink 指向了 003a0688, 即它自身, 而非 f2, 说明发生 dword shoot.