课程编号： B080203110

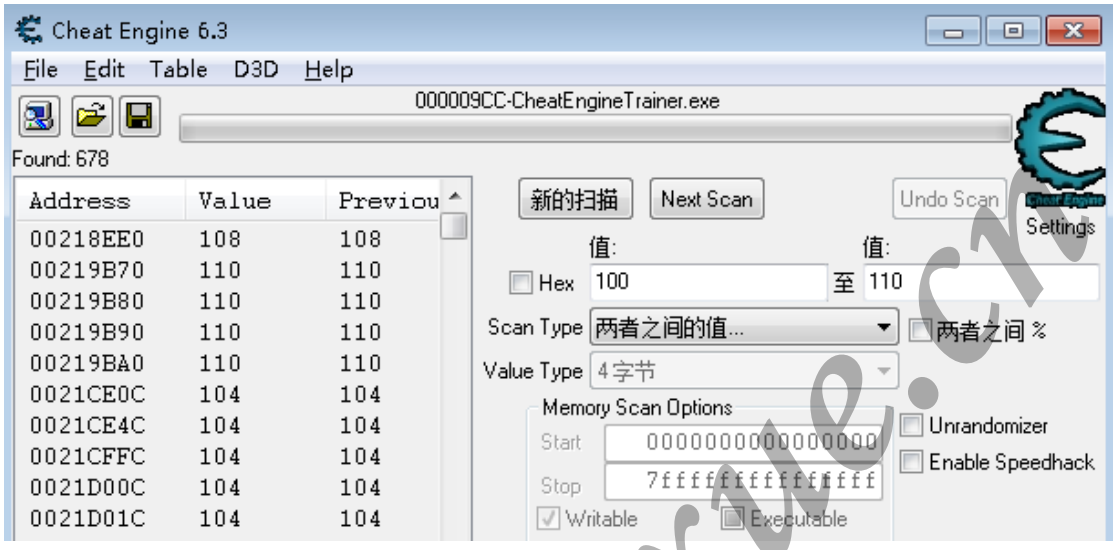
计算机系统安全
实验报告

姓　　名	薛旗	学　　号	20155362
班　　级	软信-1503	指　导　教　师	程维
实　验　名　称	破解与代码注入		
开　设　学　期	2017-2018 第一学期		
开　设　时　间	第 1 周——第 8 周		
报　告　日　期	2017.11.05		
评　定　成　绩		评　定　人	程维
		评　定　日　期	

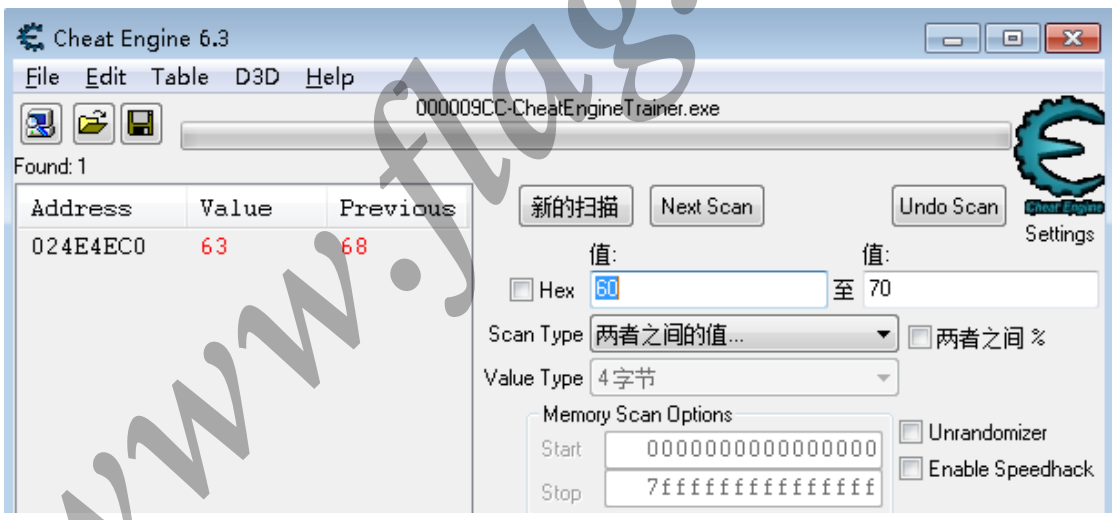
东北大学软件学院

实验一：

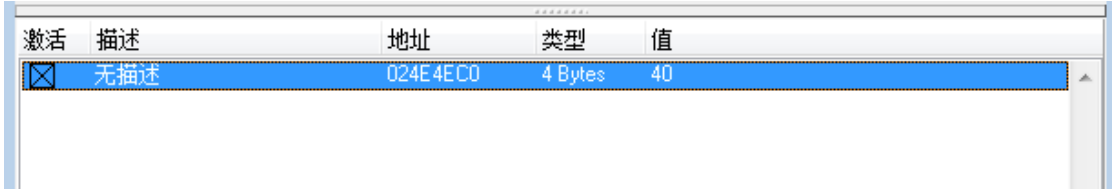
1.扫描类型选择两者之间的值，并根据倒计时秒数选择合适的区间逐步进行扫描，直到查找到唯一变量。



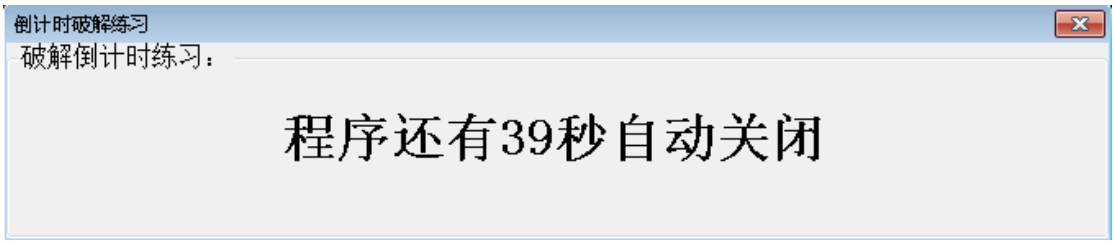
2.找到唯一变量。



3.双击该变量，将该地址转入下方列表。



4. 勾选“激活”选项，将数值锁定，可以发现倒计时程序数值不变。

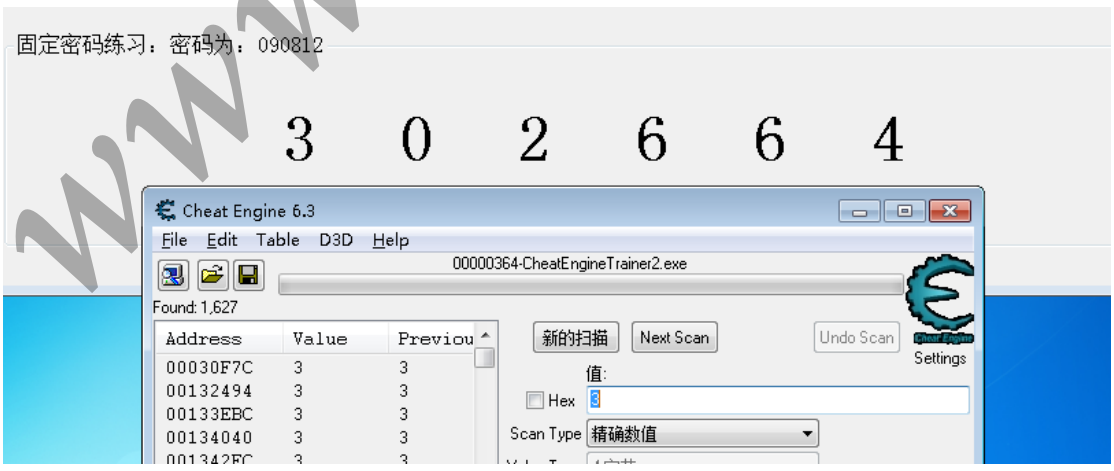


5.双击“值”处，在弹出的对话框中填入“9999”，单机确定，列表“值”处的值变为 9999.

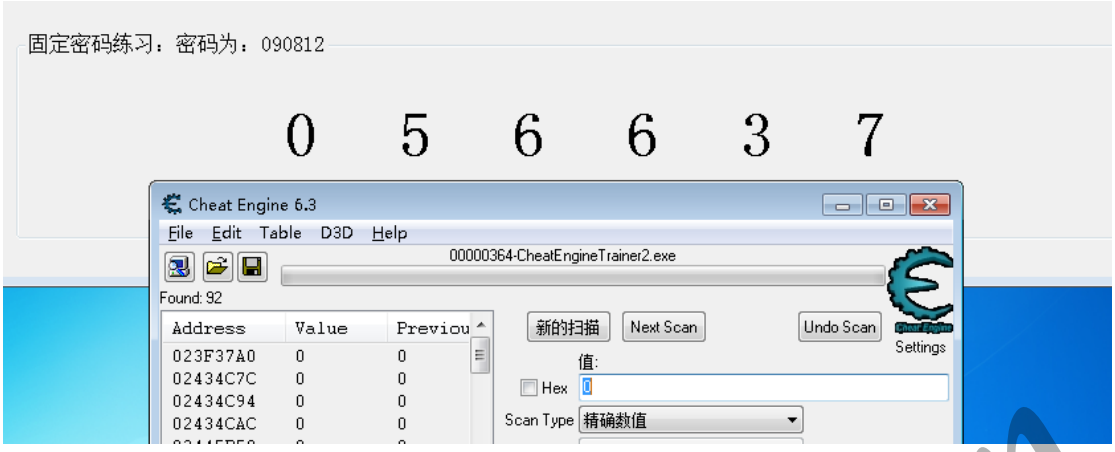
6.通过练习。

实验二：

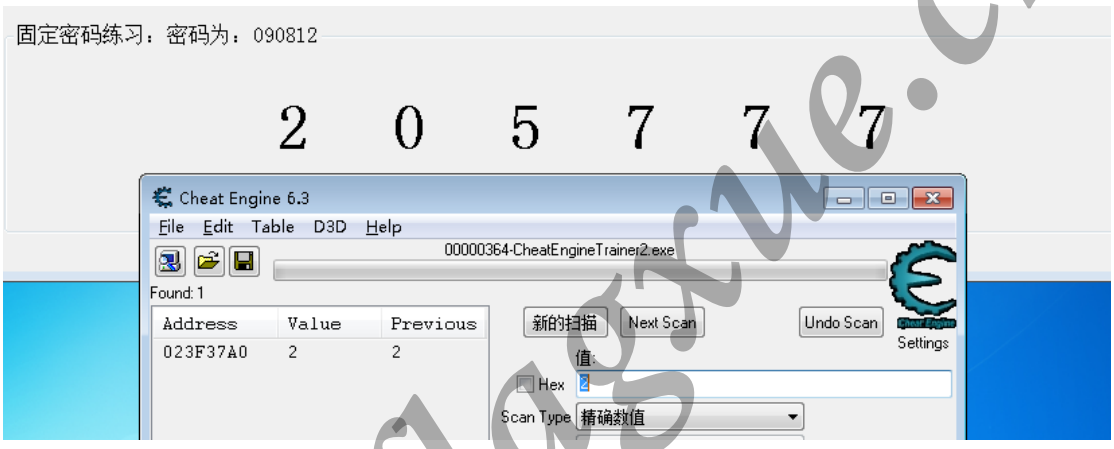
1.扫描类型：精确扫描，输入的扫描数值与动态密码的第一个值一致。



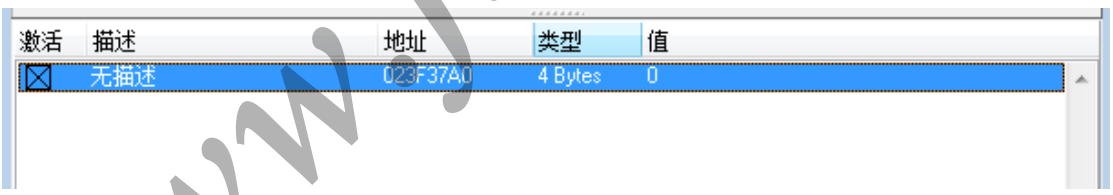
2.按第一步的方法进行多次扫描，直到得到唯一的地址信息。



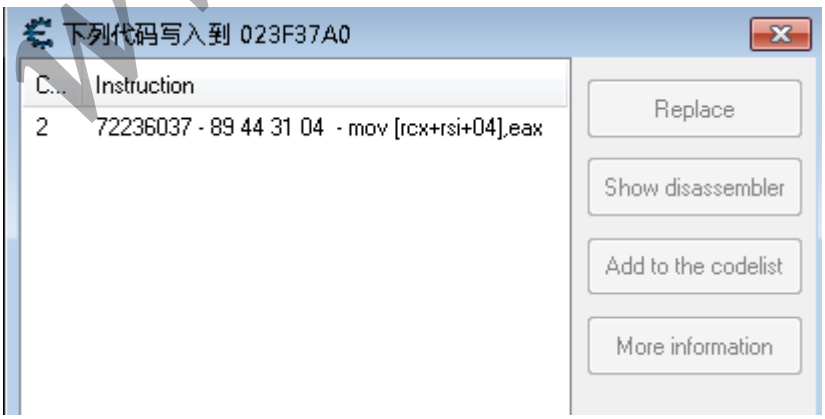
3.得到唯一地址信息。



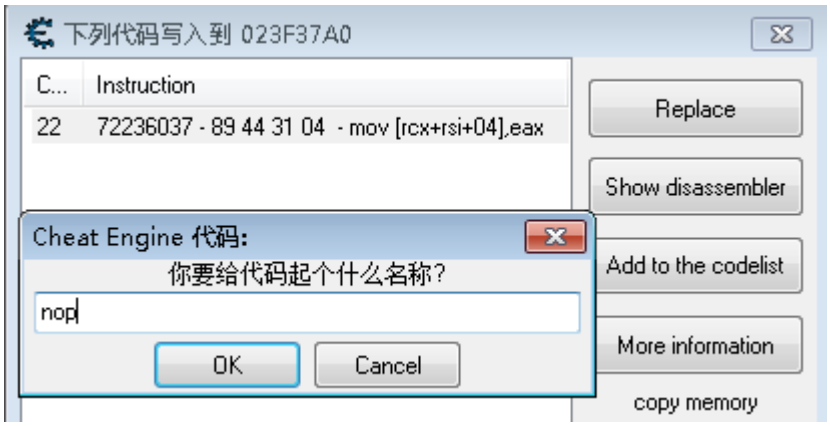
4.双击该唯一变量，将该地址转入下方列表。



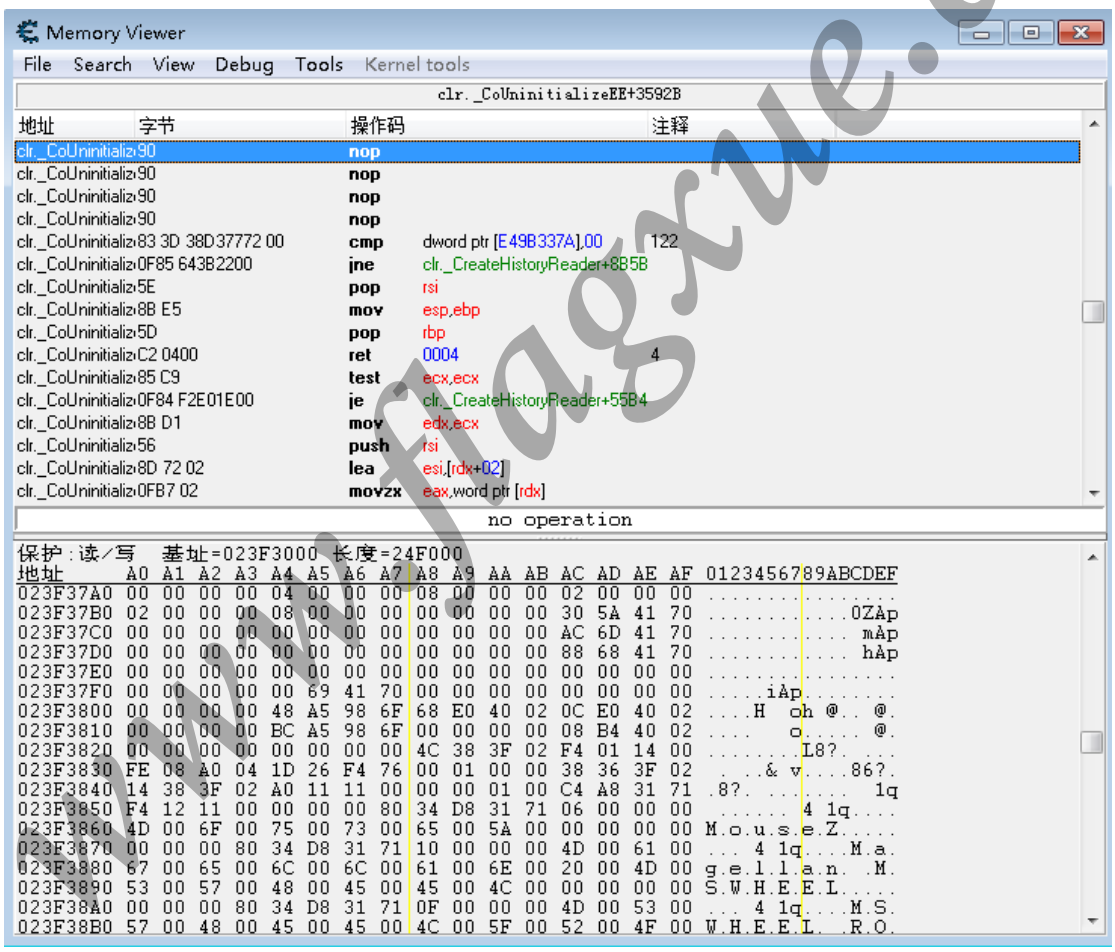
5.在 CE 下方的地址上右键，选择“Find out what writes to this address”。



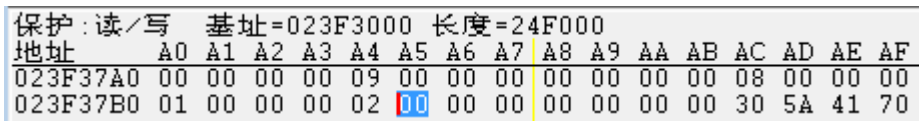
6.选中唯一信息，点击“Replace”，输入 nop 并确定。可以发现密码将被固定。



7.在 CE 下方地址信息上右键，选择“Browse this memory region”,进入内存查看器。



8.修改相应地址位置的数值，使最后的密码值为 090812。



9.通过练习。

实验三：

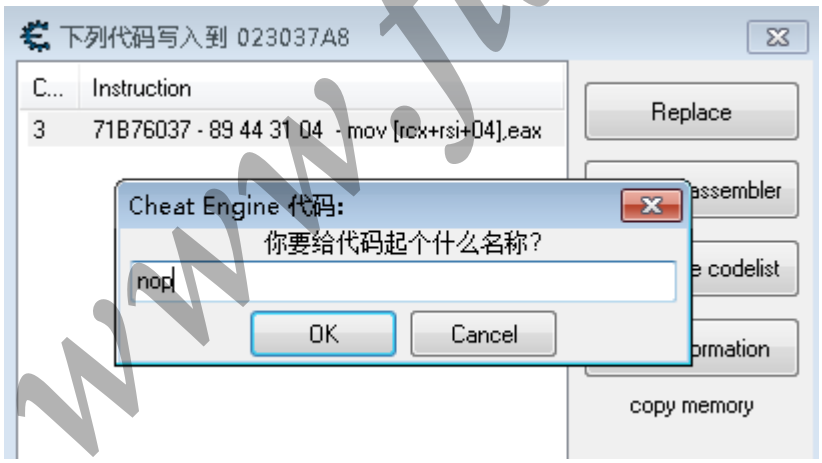
1. 扫描类型：精确扫描，输入的扫描数值与正确密码的第一个值一致。

2.多次扫描，直到扫描到唯一地址信息。

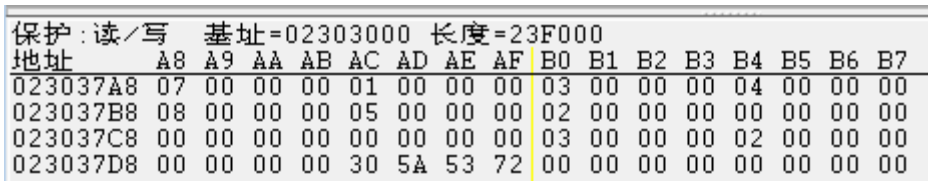
3.扫描得到唯一地址信息。

4.双击，将其加载到下方的地址列表中。

5.按实验二的方法，查找写入该地址的代码。选中唯一信息，点击“Replace”，输入 nop 并确定。可以发现密码将被固定。



6.可以看到当前的正确密码和动态密码信息，他们并不一致。

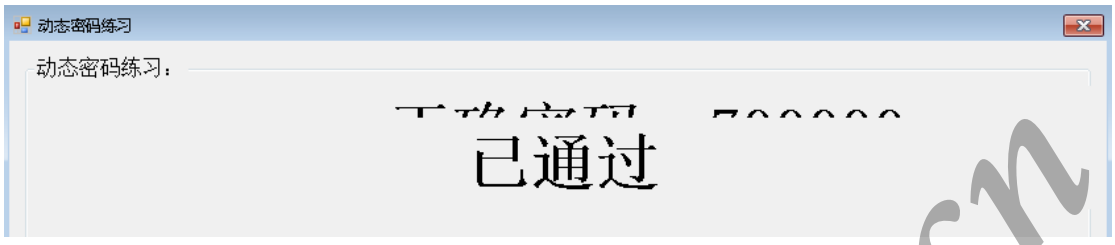


7.修改相应地址处的值，使正确密码和动态密码的值一致。

保护：读/写 基址=02303000 长度=23F000

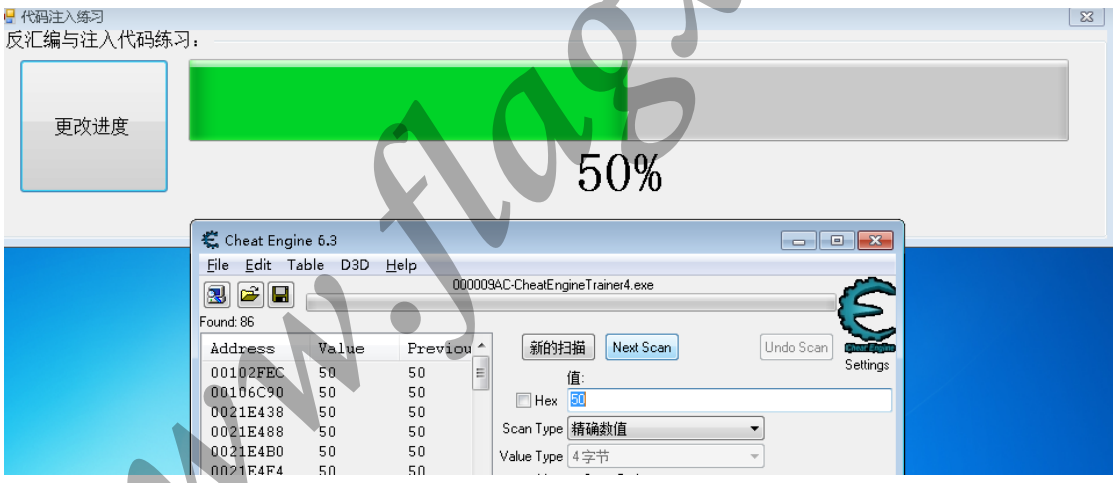
地址	A8	A9	AA	AB	AC	AD	AE	AF	B0	B1	B2	B3	B4	B5	B6	B7
023037A8	07	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
023037B8	00	00	00	00	00	00	00	00	07	00	00	00	00	00	00	00
023037C8	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

8.当正确密码和动态密码值一致时，显示已通过。

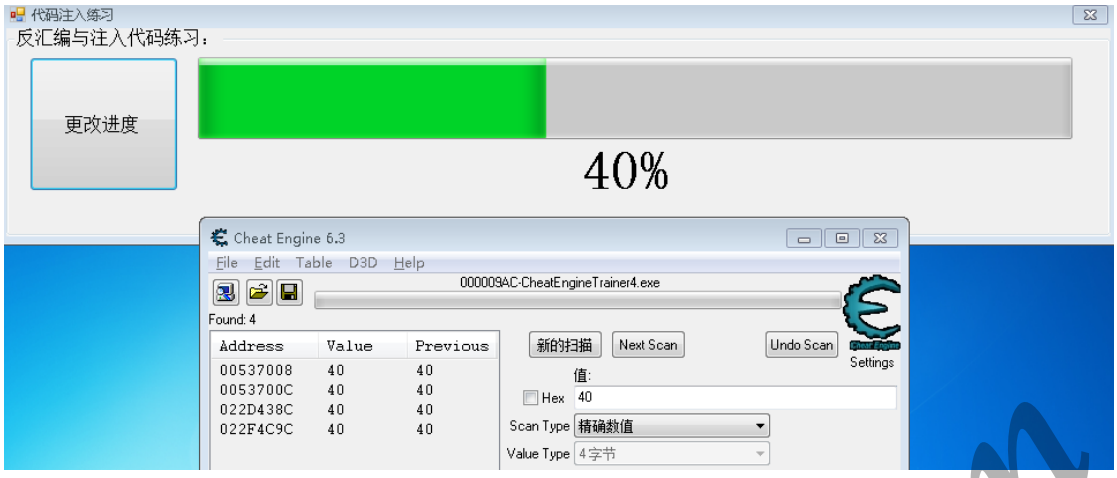


实验四：

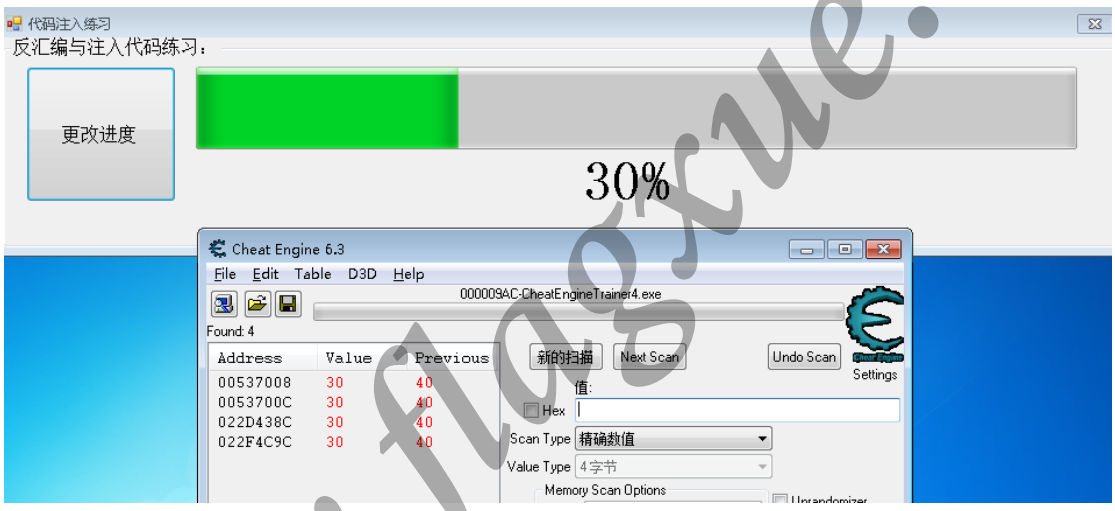
1.精确扫描，扫描值为进度值 50。



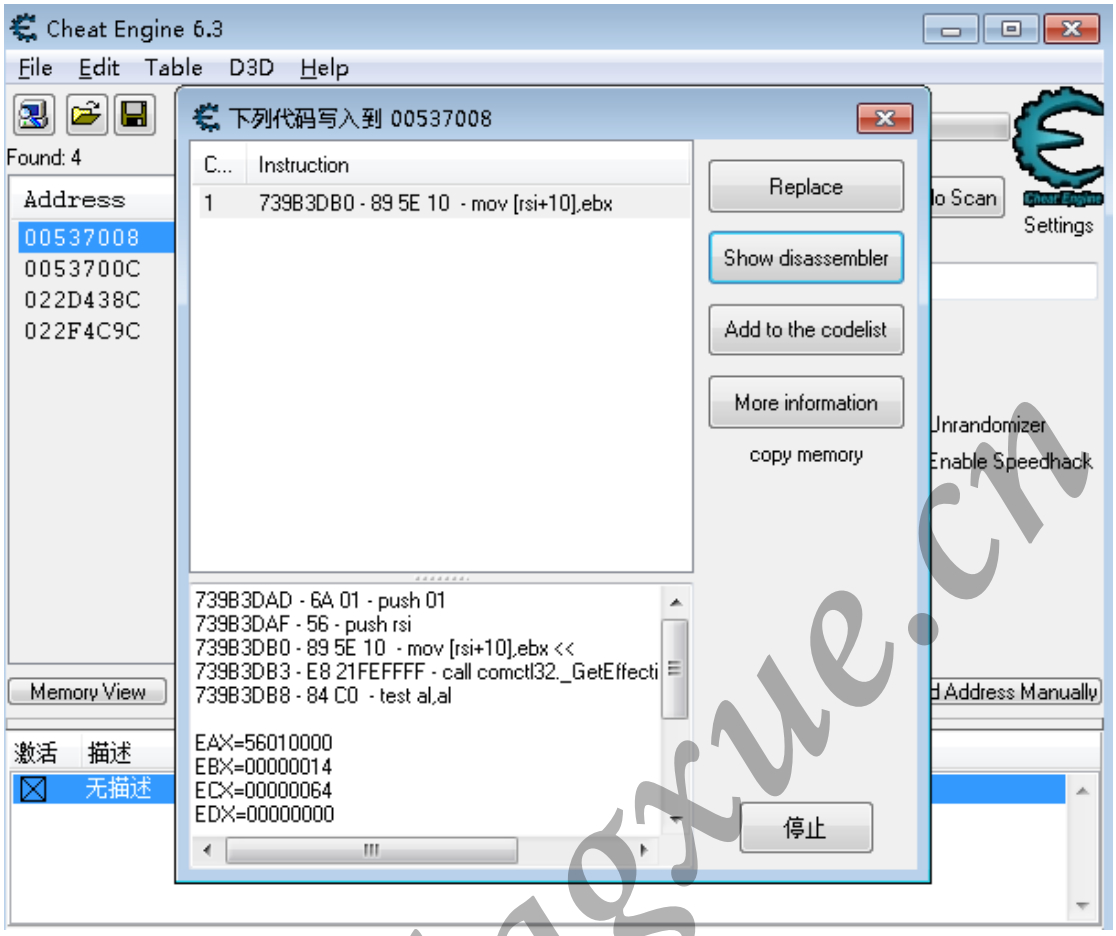
2.点击更改进度，继续扫描，扫描值为进度值 40。



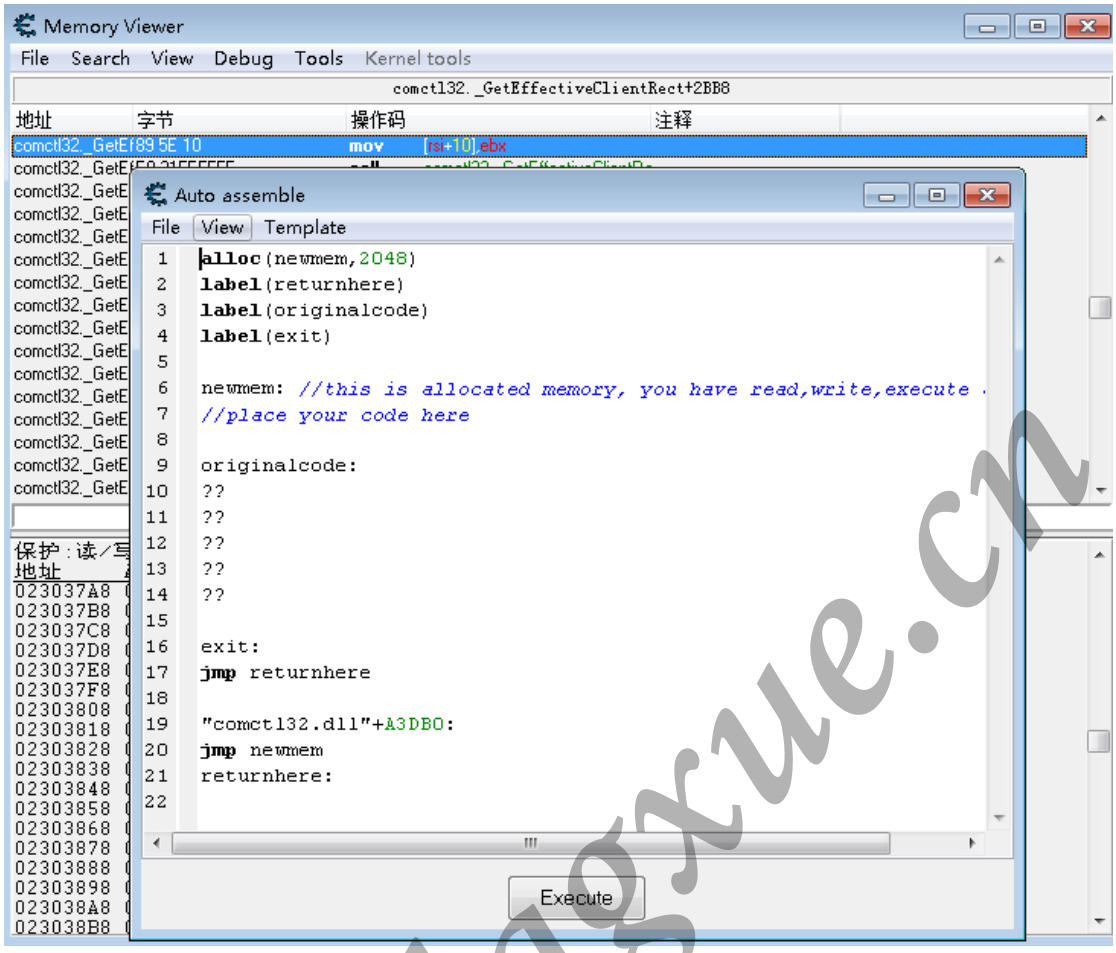
3.点击更改进度，观察发现，地址信息数量仍为 4，不再发生改变，因此以下操作需在这四个变量上进行尝试。



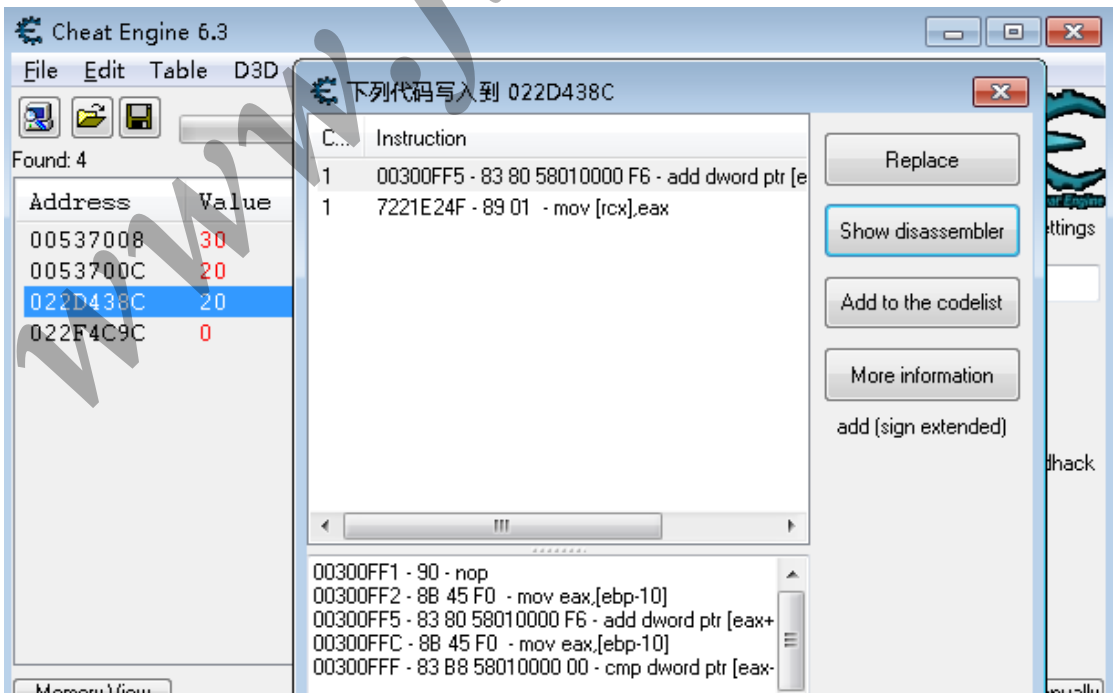
4.首先尝试第一个。类似实验二和实验三的方法，查找写入该地址的代码。



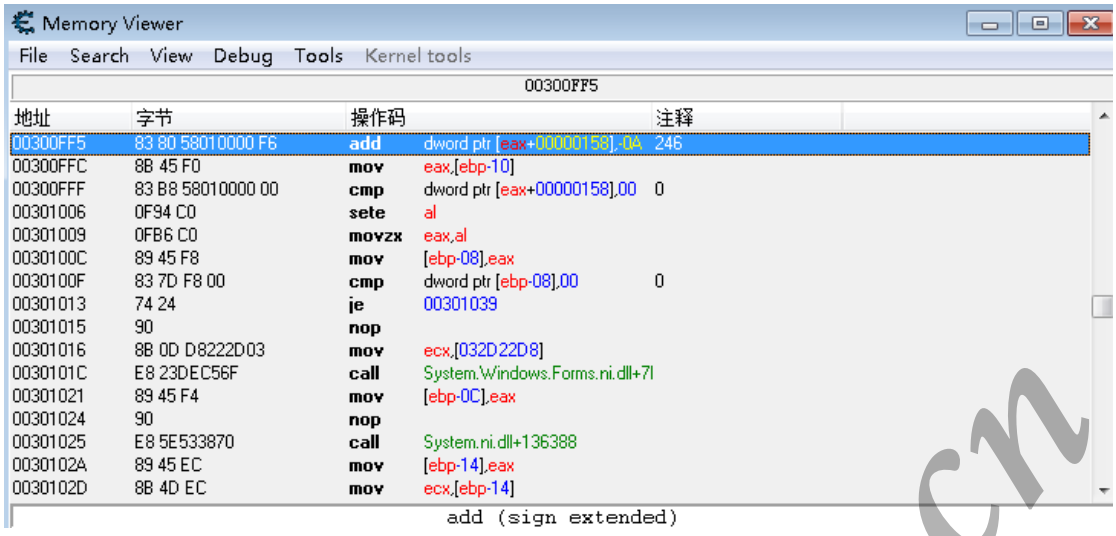
5.点击“Show disassemble”,显示反汇编，打开内存查看器。在“Tool”菜单中选择“Auto assemble”(自动汇编)，在弹出的界面中，选择“Template”菜单项下的“Code injection”(代码注入)，然后在弹出的地址填写窗口处点击确定，可发现自动汇编已帮我们创建了一部分代码。通过实践观察，该部分代码对解决问题没有帮助，继续实践。



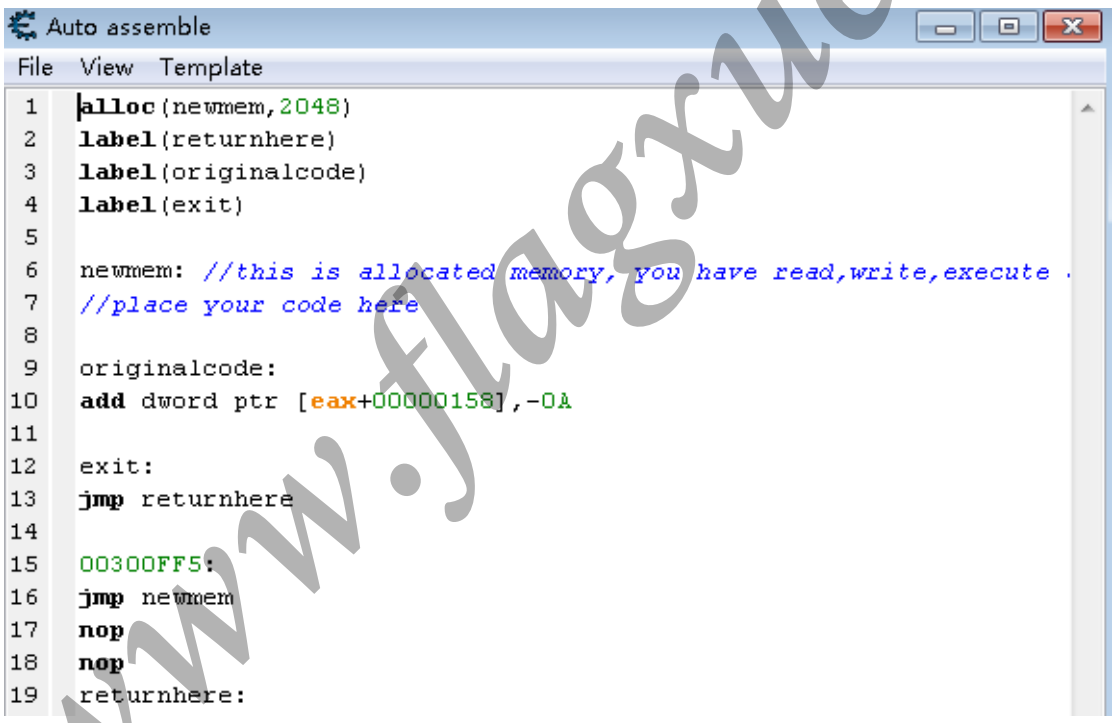
6.通过实践，第三个地址变量对解决问题有帮助。此处只展示对解决问题有帮助的操作方法。按以上类似的方法，查找写入该地址的代码。



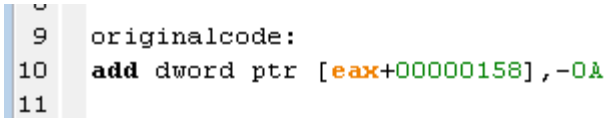
7.打开内存查看器。



8.同样的操作方法，进入代码注入界面，研究代码。



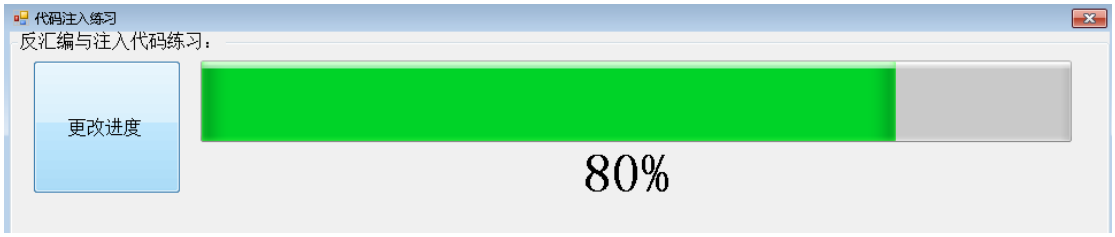
9.可以发现第 10 行的代码是解决问题的关键。源码通过累加-0A，使得每次点击“更改进度”按钮，进度递减 10。我们可以从这里下手，解决问题。



10.将累加-0A 改为+0A，注入后的代码通过累加+0A，使得每次点击“更改进度”按钮，进度递增 10。点击“Execute”完成代码注入。

```
originalcode:
add dword ptr [eax+00000158],+0A
```

11.点击“更改进度”按钮，使进度递增到 100。



12.进度达到 100，通过练习。

教师评语或**评价表格**：（任课教师可根据实际情况，做适当调整）

评语及评价表格的字体颜色为红色

评价表格示例：（考核标准与教学大纲中的实验考核标准一致）

考核标准	得分
（1）正确理解和掌握实验所涉及的概念和原理（10%）；	
（2）按实验要求合理设计数据结构和程序结构（20%）；	
（3）能设计测试用例，运行结果正确（20%）；	
（4）认真记录实验数据，原理及实验结果分析准确（40%）；	
（5）实验报告规范（10%）。	