2019-3-9

第1题

题目要求

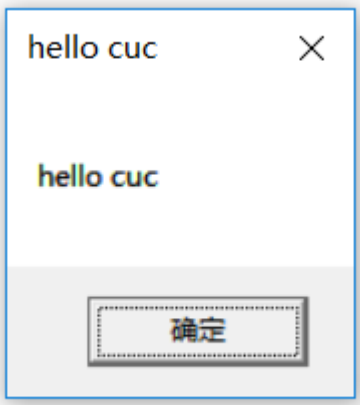
- 编写一个release版本的 hello world 程序。通过修改程序可执行文件的方式（不是修改源代码），使得程序运行后显示的内容不为hello world，变成 hello cuc!

实验步骤

- 编写程序

```
# include <windows.h>
int main()
{
    MessageBoxA(NULL, "hello world", "hello world", MB_OK);
    ExitProcess(0);
}
```

- 编译链接
  -
```
C:\Users\Narthil\Learning\2019-3\softwareAndSystemSecurity\t1>cl /c /O1 sss_01.c
用于 x86 的 Microsoft (R) C/C++ 优化编译器 19.11.25547 版
版权所有(C) Microsoft Corporation。保留所有权利。

sss_01.c
```
  -
```
C:\Users\Narthil\Learning\2019-3\softwareAndSystemSecurity\t1>link user32.lib kernel32.lib /nologo /entry:main /driver /
nodefaultlib /subsystem:windows /align:16 sss_01.obj /out:sss_01.exe
```
  - 用二进制编辑器winHex打开生成的`.exe`文件
  - `ctrl+F`找到字符串`hello world`所在的位置
  - 右键`world`对应的十六进制码，选择`edit -> fill block`进行修改，修改为`cuc`对应的十六进制码
  -
```
00000624  B6 03 00 00 00 00 00 00  9C 03 00 00 00 00 00 00  ¶       œ
00000640  68 65 6C 6C 6F 20 63 75  63 20 20 00 00 00 00 00  hello cuc
00000656  00 00 00 00 47 C4 7C 5C  00 00 00 00 0D 00 00 00      GÄ|\
```
- 运行程序
  - 

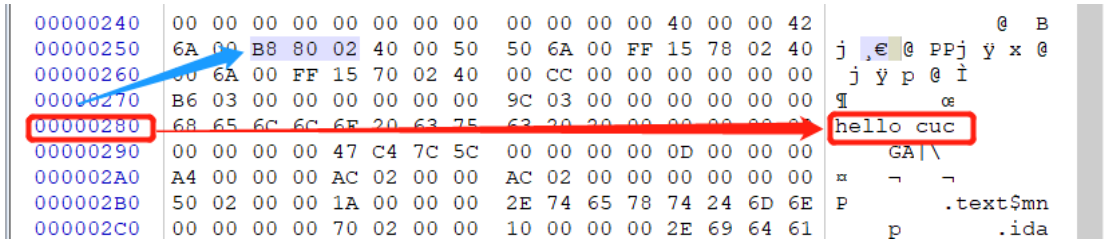
第2题

题目要求

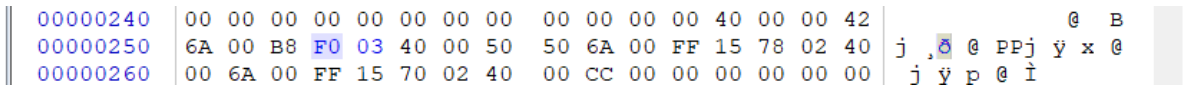
- 上一题的程序中，修改的显示内容变为一个很长的字符串（至少2kb长）。并且保证程序正常运行不崩溃。

实验步骤

- 生成反汇编文件找到基地址：`dumpbin /headers /nologo sss_01.exe > dump_1.txt`
  - 250 base of code
    270 base of data
    400000 image base (00400000 to 004003EF)
    10 section alignment
  - 基地址为00400000h
- 用`winHex`打开上一题生成的exe文件`sss_01.exe`
- 找到hello cuc的地址偏移为280h



  - 上数三行，可以找到指向存储该字符串的指针
- 在文件末尾添加一段长2kb的文字（我从之前毛概的题里截出来的
- 将250行的指针修改为末尾的地址`03F0`



- 保存并运行
- 运行结果

C.文化多样化持续推进C.从群众中来到群众中去D.中央工作会议15.新的历史条件下，党执政的基本方式是(C)A.群众工作B.多党合作C.依法执政D.改革创新二.多项选择题：1.党的十八届三中全会提出的全面深化改革的总目

C.文化多样化持续推进
C.从群众中来到群众中去
D.中央工作会议
15.新的历史条件下，党执政的基本方式是(C)
A.群众工作
B.多党合作
C.依法执政
D.改革创新
二.多项选择题：
1.党的十八届三中全会提出的全面深化改革的总目标指的是(AC)
A.完善和发展增强(ABCD)意识
A.政治意识
B.大局意识
C.核心意识
D.看齐意识
5.如何增强中国共产党依法执政的本领(AB)
A.坚持依法治国与依规治党有机统一
B.加快形成覆盖党的领导和党的建设各方面的党内法规制度体系
C.弘扬社会主义核心价值观
D.推进中国共产党的领导机构改革
6.全面增强党的执政本领，其中包括(ABCD)
A.学习本领和政治本领
B.改革创新本领和科学发展本领
C.依法执政本领和群众工作本领
D.狠抓落实本领和驾驭风险本领
7.确保党始终总揽全局、协调各方，必须(ABC)
A.增强政治意识、大局意识、核心意识、看齐意识
B.坚持和完善党的领导体制机制
C.坚持党的民主集中制原则
D.加强党的机构改革力度
8.中国共产党的领导是中国特色社会主义最本质的特征，这是由(ABD)决定的。
A.中国特色社会主义产生与发展的历史逻辑
B.中国特色社会主义迈向新征程的实践逻辑
C.中国特色社会主义普遍主义的理论逻辑
D.科学社会主义的理论逻辑
9.如何遵循马克思主义建党原则，使党成为统一整体的组织(BCD)
A.严肃组织风气
B.严明组织纪律
C.严格组织生活