软件与系统安全：任务二

1.首先我们用dumpbin来查看可执行文件的文件结构，并将内容存入txt文件

```
C:\Users\core\Documents\package>dumpbin /all hello.exe
Microsoft (R) COFF/PE Dumper Version 14.15.26726.0
Copyright (C) Microsoft Corporation.  All rights reserved.
```

2.通过观察我们发现文件的第一个节表.text部分的起始地址为00401000，该部分存储着调用函数的参数指针地址

```
SECTION HEADER #1
   .text name
      21 virtual size
    1000 virtual address (00401000 to 00401020)
     200 size of raw data
     400 file pointer to raw data (00000400 to 000005FF)
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
60000020 flags
         Code
         Execute Read

RAW DATA #1
  00401000: 55 8B EC 6A 00 68 00 30 40 00 68 08 30 40 00 6A  U.ìj.h.0@.h.0@.j
  00401010: 00 FF 15 08 20 40 00 6A 00 FF 15 00 20 40 00 5D  .?.. @.j.?.. @.]
  00401020: C3                                               ?
```

3.随后在.data段的节表内容中，我们观察到MessageBox显示的内容是从地址为00403008开始的

```
SECTION HEADER #3
   .data name
      15 virtual size
    3000 virtual address (00403000 to 00403014)
     200 size of raw data
     800 file pointer to raw data (00000800 to 000009FF)
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
C0000040 flags
         Initialized Data
         Read Write

RAW DATA #3
  00403000: 73 65 63 63 69 6F 6E 00 48 65 6C 6C 6F 20 77 6F  seccion.Hello wo
  00403010: 72 6C 64 21 00                                   rld!.
```

4.再往后看，我们发现该可执行文件所应用的存储空间到0040400f就结束了，因此之后的所有空间都是没有被占用的

```
SECTION HEADER #4
  .reloc name
      10 virtual size
    4000 virtual address (00404000 to 0040400F)
     200 size of raw data
     A00 file pointer to raw data (00000A00 to 00000BFF)
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
42000040 flags
         Initialized Data
         Discardable
         Read Only

RAW DATA #4
  00404000: 00 10 00 00 10 00 00 00 06 30 0B 30 13 30 1B 30  .........0.0.0.0
```

5.因此我们用二进制文件从00404010的位置开始输入我们想要的内容

```
00 10 00 00 10 00 00 00 06 30 0b 30 13 30 1b 30 .........0.0.0.0
54 68 65 72 65 20 61 72 65 20 69 64 65 61 6c 20 There are ideal
73 65 72 69 65 73 20 6f 66 20 65 76 65 6e 74 73 series of events
20 77 68 69 63 68 20 72 75 6e 20 70 61 72 61 6c  which run paral
6c 65 6c 20 77 69 74 68 20 74 68 65 20 72 65 61 lel with the rea
6c 20 6f 6e 65 73 2e 54 68 65 79 20 72 61 72 65 l ones.They rare
6c 79 20 63 6f 69 6e 63 69 64 65 2e 4d 65 6e 20 ly coincide.Men
61 6e 64 20 63 69 72 63 75 6d 73 74 61 6e 63 65 and circumstance
73 20 67 65 6e 65 72 61 6c 6c 79 20 6d 6f 64 69 s generally modi
66 79 20 74 68 65 20 69 64 65 61 6c 20 74 72 61 fy the ideal tra
69 6e 20 6f 66 20 65 76 65 6e 74 73 2c 73 6f 20 in of events,so
74 68 61 74 20 69 74 20 73 65 65 6d 73 20 69 6d that it seems im
70 65 72 66 65 63 74 2c 61 6e 64 20 69 74 73 20 perfect,and its
63 6f 6e 73 65 71 75 65 6e 63 65 73 20 61 72 65 consequences are
20 65 71 75 61 6c 6c 79 20 69 6d 70 65 72 66 65  equally imperfe
63 74 2e 54 68 75 73 20 77 69 74 68 20 74 68 65 ct.Thus with the
20 52 65 66 6f 72 6d 61 74 69 6f 6e 3b 69 6e 73  Reformation;ins
74 65 61 64 20 6f 66 20 70 72 6f 74 65 73 74 61 tead of protesta
6e 74 69 73 6d 20 63 61 6d 65 20 4c 75 74 68 65 ntism came Luthe
72 61 6e 69 73 6d 3b 54 68 65 20 73 75 6e 20 61 ranism;The sun a
6c 73 6f 20 72 69 73 65 73 20 69 73 20 61 20 66 lso rises is a f
61 6d 6f 75 73 20 77 6f 72 6b 20 6f 66 20 74 65 amous work of te
68 20 67 72 65 61 74 20 41 6d 65 72 69 63 61 6e h great American
20 61 75 74 68 6f 72 20 48 61 6d 69 6e 67 77 61  author Hamingwa
79 20 61 6e 64 20 69 74 20 69 73 20 62 61 73 65 y and it is base
20 6f 6e 20 68 69 73 20 6f 77 6e 20 65 78 70 65  on his own expe
```

6.并将指定位置的指针地址更改为00404010

```
55 8b ec 6a 00 68 00 30 40 00 68 10 40 40 00 6a U嫻j.h.0@.h.@@.j[
00 ff 15 08 20 40 00 6a 00 ff 15 00 20 40 00 5d .  .. @.j.  .. @.
```

7.再次运行exe应用程序时，发现显示内容已经被替换

seccion

There are ideal series of events which run parallel with the real ones.They rarely coincide.Men and circumstances generally modify the ideal train of events,so that it seems imperfect,and its consequences are equally imperfect.Thus with the Reformation;instead of protestantism came Lutheranism;The sun also rises is a famous work of teh great American author Hamingway and it is base on his own experiences.It told a story of a solider after World War 2.It is a book worth reading.

确定