C3课后思考

- 【程序入口点】PE被装载之后，第一条语句的代码在什么位置？
- 【地址转换】PE文件开始运行之后，其在内存中的镜像数据与磁盘上的文件数据有哪些差异？VA、RVA以及文件偏移的转换关系是什么？
- 【代码补丁】可在代码节自行增加代码使目标程序完成更多功能么？
- 【序号引入】PE文件如何通过序号引入外部函数？
- 【函数引入机制】在程序运行的过程中，程序的控制权具体是转交给外部DLL的函数的，程序又是如何收回控制权回到自己代码的？
- 【函数HOOK】如何对引入的DLL文件的API函数进行拦截（HOOK）？
- 【资源封装与装载】能够在可执行程序中存储并在运行时释放其他可执行程序么？
- 【图标修改】如何提取/替换/新增目标程序中的图标（或其他资源）？
- 【重定位】DLL文件中哪些部分的数据是需要重定位的？为什么？
- 【程序签名】二进制可执行程序被签名之后，对其任何地方进行都会导致签名验证失效么？

C3课后练习（1/2）

- 修改函数入口点地址，使得test.exe直接弹出第二个消息框。
- 打开test.exe，对其中给定任意RVA地址，将其转换成文件偏移，并在文件中找到对应数据。
- 修改test.exe的代码段，使其弹出第三个消息框（包含自己学号和姓名）
- 修改test.exe，删除文件中引入函数节的MessageBoxA字符串，之后自行进行相应调整，使得test.exe弹框功能恢复正常。
- 编写一个弹出消息框的msg.dll文件，仅修改test.exe的引入函数节部分数据，使得test.exe运行时自动加载msg.dll，并弹出消息框。
- 首先删除test.exe引入函数节所有数据，然后将所有引入的DLL名字及函数名重新定义在引入函数节开始部分，之后继续修改引入函数节其他部分（需要时可再修改DataDirectory相关项），使得该程序再次恢复原有功能。

C3课后练习（2/2）

- 使用OD启动test.exe停留在开始位置，然后对内存进行修改，使得再次继续运行程序调用MessageBoxA函数后均先弹出计算器程序（system(“calc.exe”)）。
- 使用16进制编辑器提取ZoomIt程序中尺寸最大的图标，并存储为.ico文件，确认ico文件打开正常。
- 将test.exe程序的ImageBase从00400000H修改为00600000H，然后通过对该程序其他位置进行相应修改，使得该程序功能恢复正常。
- 使用工具（如signtool.exe）对test.exe进行签名，查看文件签名信息，并比对签名前后test.exe文件的变化。尝试修改签名后的程序，但是不影响签名的有效性。

挑战自己

1. 在保证MiniPE-760.exe(760字节)程序功能不变的情况下，修改该文件，使其体积最小（当前记录：田杨-XP系统下192字节）。
   - 该文件可从附件中下载。
   - 修改弹出窗口的信息为自己的信息。
   - 不能对函数地址进行硬编码，不能使用函数序号引入。