实验四 PE壳设计与验证

实验目的：

1. 验证PE文件结构构建
2. 验证PE文件壳的基本原理

实验内容：

1. 实现简单的跳转壳，在PE文件中添加新节，在新节其中加入跳转至原入口的指令(od中双击)，实现对原程序的启动。

FileHeader.NumberOfSections -> 4

TODO OptionalHeader.SizeOfHeaders（不用改，没超过对齐粒度）;

.SizeOfImage = 4000h + 100h 向上对齐 = 5000h

新的节表：

Name db 8: 2E 6E 65 77 73 65 63 00 (.newsec)

VirtualSize dd: 00 01 00 00 (100h)

VirtualAddress dd: 00 40 00 00（RVA，内存中的地址。前一个.data节VA为3000h，大小为0Dh，按照内存中对齐粒度为1000h，故VA设为4000h）

SizeOfRawData dd: 00 02 00 00 （文件中对齐粒度为200h，故大小为200h）

PointerToRawData dd: 00 0A 00 00（前一节在文件中的起始为800h, 文件中大小为200h）

PointerToRelocations dd: 00 00 00 00

PointerToLinenumbers dd: 00 00 00 00

NumberOfRelocations dw: 00 00

NumberOfLinenumbers dw: 00 00

Characteristics dd: 20 00 00 60 （节的属性：可读，可执行，代码）

偏移量: A00h, LordPE -> RVA: 4000h

OptionalHeader.AddressOfEntryPoint: 00 40 00 00(RVA)

entry point : 0C 10 00 00 -> 00 40 00 00

添加指令：

jmp 40100C

1. 实现PE文件加密壳，对原程序代码节(.text)内容异或运算(010editor工具)，在原程序中加入新节实现对原代码节内容解密并启动运行。 把这段代码加入第1问的节中，（lordPE中把text节的flag加上可写）

pushad

mov ecx, 1000h

mov ebx, 1000h

mov edx, 400000h

add ebx, edx

add ecx, ebx

xor *byte* ptr ds:[ebx], 15h

inc ebx

cmp ebx, ecx

jl 404014

popad

jmp 40100Ch

成功