2021/03/30_壳_第2课_压缩壳的实现之加壳部分

笔记本： 壳
创建时间： 2021/3/30 星期二 10:20
作者： ileemi

压缩壳的代码实现

1. 加壳程序（压缩代码）
2. 解压缩程序

加壳程序实现步骤

1. 解析原PE，获取原PE数据，将其数据映射到内存中;
2. 获取压缩数据（使用WinAPI -- CreateCompressor）；
3. 获取解压缩代码（壳代码）；
4. 构建新PE，解压缩代码和压缩数据分别放置在不同的节区中，新PE共三个节。在新PE中添加一个空节用于在执行过程中解压原始PE的数据;
    - 构建代码节数据
    - 构建压缩数据节
    - 构建节表
    - 构建PE头（需要注意是否修改字段：NumberOfSections、OEP、SizeofImage、NumberOfRvaAndSizes等）
5. 将新生成的PE数据写入到文件