2021/03/31_壳_第3课_压缩壳的实现之壳部分

笔记本: 壳
创建时间: 2021/3/31 星期三 10:01
作者: ileemi

- 解压缩代码

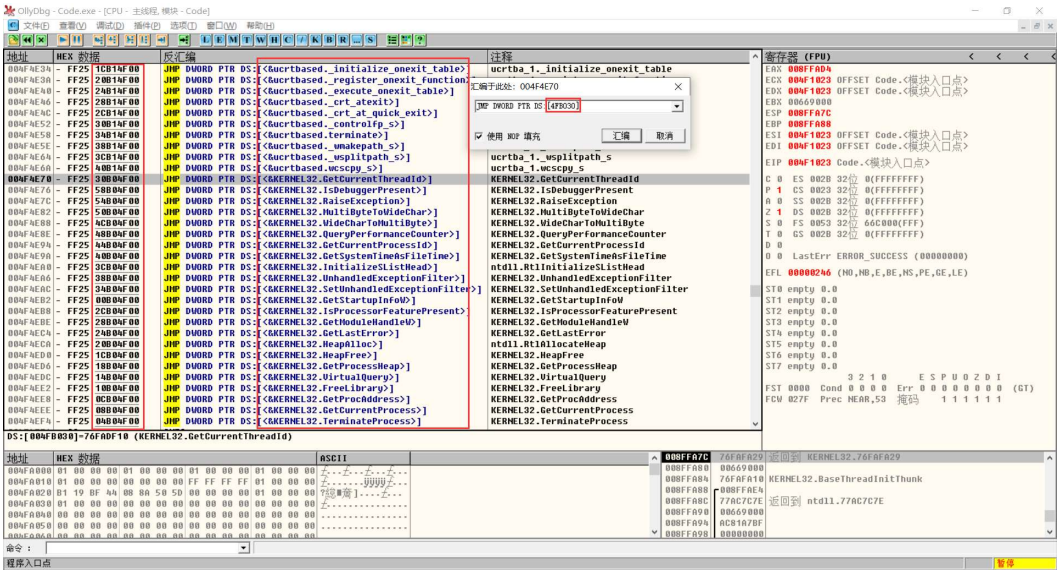
解压缩代码

> 解压缩代码在加壳后的PE中正常运行就需要满足 "这段代码中没有访问绝对地址的指令"。
> 地址无关代码（shellcode）：代码中没有访问绝对地址的指令，该代码就可以在程序的任意地址上进行运行。

VS 编译程序对应的指令中含有绝对地址的条件：

- 访问了全局变量
- 调用了WinAPI

带有绝对地址的指令，都是需要进行重定位的指令，对于需要进行重定位的汇编指令在OllyDbg中都会在其对应的汇编指令下画上一个横线，如下图所示：



使用VS生成不能包含有绝对地址的指令就需要使用C配合VS的编译选项：

1. 开启随机基址;
2. 程序切换为Release版（Debug中会添加一些方便调试的代码）；
3. 切换为Release版后会有一些main函数之前的初始化代码，所以就需要将原程序的入口点 "main" 进行替换。项目属性 --> 链接器 --> 高级 --> 入口点 --> "Entry" （新的入口函数）；
4. 关闭 "安全检查（/GS-）"。项目属性 --> C/C++ --> 所有选项 --> 安全检查 --> 更改为 "禁用安全检查（/GS-）";

5. 防止函数被内联，可以在项目属性页中禁用优化或者修改 "内联函数扩展选项" --> "只适用于 __inline (/Ob1)";