# 第一次实验：PE文件格式分析实验

（2020-2021学年上学期软件安全课程实验）

时间：2020-11-9下午7、8节课

一、实验目的：

1. 熟悉各种PE编辑查看工具，详细了解PE文件格式
2. 重点分析PE文件文件头、引入表、引出表，以及资源表
3. 调研并总结PE文件格式与PE病毒之间的关系
4. 自己制作一个尽可能小的PE文件

二、实验运行环境：

虚拟机下任何WINDOWS系统

三、实验准备：

下载相关工具和软件包：UltraEdit、Ollydbg、PEVIEW、Stub\_PE、PEditor（预先网上下载最新版本）

四、实验内容：

1、使用UltraEdit观察Notepad.exe数据，制作该PE文件基本结构图，格式如下：MZ头部+DOS stub+PE文件头+可选文件头（含数据目录）+节表+节（请注意地址对齐方式）

2、Ollydbg对该程序进行初步调试，了解该程序功能结构，在内存中观察该程序的完整结构（请注意地址对齐方式）

3、

4、调试并修改notepad.exe程序（请注意不要修改功能代码，仅修改程序菜单项名称或者弹出窗口文本内容或窗口提示框标题）

5、找到系统SYSTEM32目录下的user32.dll文件，用UltraEdit打开并分析该文件导出表，找出 MessageBoxA的地址，并验证该地址是否正确。

6、用UltraEdit修改notepad.exe程序的引入表，使得该程序仅可以从kernel32.dll中引入LoadLibrary和GetProcAddress函数，而不从user32.dll导入任何函数。

7、在代码节中写入部分代码利用上述导入的两个函数获取 MessageBoxA的函数地址，使得notepad.exe程序的原有功能正常。

8、自学探索类实验：熟悉资源表。利用PEview.exe熟悉资源表的结构，利用PEview.exe分析PEview.exe程序；用UltraEdit修改PEview.exe，使得该文件的图标变成PEview.ico

9、选做实验：熟悉eXeScope工具的实用，并利用该工具汉化PEview.exe程序

1. 注意

若实验过程中notepad.exe的修改被系统拒绝，分析一下原因，实在无法解决，可以自行寻找另外一个满足实验要求的应用级的可执行文件继续实验。

1. 实验检查时间

四次实验完成后统一检查

1. 报告提交时间

[考试前三天由各班班长或学委统一收齐后，电子版发至308409399@.QQ.COM邮箱，纸质报告交到计算机楼112实验室文翠娟处。](mailto:考试前三天由各班班长或学委统一收齐后，电子版发至308409399@.QQ.COM邮箱，纸质报告交到计算机楼112实验室文翠娟处。)