chapter3：调试分析工具

1. Pe
2. Pe数据节分类：rsrc text idata data
3. 加壳
4. 加壳分类
5. 虚拟内存
6. 程序再定位 虚地址转到实地址
7. Pe文件注入 挂接代码完成跳转
8. 软件破解 SETE AL

Chapter4：软件漏洞

1. 缓冲区 连续内存区域 存放代码执行时的内存数据
2. 缓冲区溢出漏洞 缺乏边界检查
3. 栈溢出漏洞 覆盖临近区域的数据 从低地址向高地址
4. 堆溢出漏洞 覆盖不同堆块的数据
5. Dword shoot 任意位置写入任意代码
6. SEH结构溢出漏洞 覆盖 入口地址/异常函数处理处理句柄/seh链表
7. 单字节溢出漏洞