# 软件安全第二、三次实验

### 1.时间

第二次：12月14日星期一下午7、8节课

第三次：待定

### 2.实验检查时间

在第四次实验统一进行检查

### 3.实验报告提交时间

考试前一周

### 4.提交方式

由班长或学委收齐后电子格式提交至308409399@qq.com邮箱，纸质报告交至计算机楼112研究生文翠娟代收。

### 5.实验内容

**实验(1)：**试利用windbg、DDK或SoftICE查看EProcess和PEB中活动进程相关信息，绘制出当前活动进程双向链表在内核态和用户态下的进程链表结构，并设计“断链”方法利用这两个结构体实现自己任意指定进程在任务管理器中的隐藏。

**实验(2)：**缓冲区溢出实验

调试课堂介绍的有关栈溢出、堆溢出实例、BSS溢出和格式化字符串溢出实例，围绕着这些实例采用的溢出方法，自行调整溢出使用的字符串，摸索并掌握控制程序流程的字符串设计方法，并分析其特征和规律。注意事项如下：

1. 栈溢出需要重点体验函数调用与返回过程中栈帧的结构与变化，以及返回函数地址（EIP）的控制方法
2. 堆溢出需要关注堆的大小、堆的反复创建与释放可能造成的碎片、连续创建堆之间的间隙
3. 格式化字符串需要关注各种格式化字符串结合自行设置的变量造成溢出的规律
4. BSS溢出对于指针函数的获取方法，可以自行设计一个PE文件

要求自行构建缓冲区溢出场景（漏洞利用和攻击字符串构型，比如说RNS、NSR等），利用线程注入的方法，通过缓冲区溢出实现权限提升的攻击代码。

**实验(3)：**完成一个简单的PE文件病毒核心机制的实现，具体要求如下：

1、自定义可执行文件的搜索范围；

2、要求能够自动识别PE文件类型；

3、利用节插入、节扩展或节添加（三者任选一种）方式完成病毒在PE文件中的感染机制；

4、利用注册表的系统调用API函数（创建键RegCreateKeyEx、打开一个键RegOpenKeyEx、读取键RegQueryValueEx、设置键值RegSetValueEx、删除键值RegDeketeKey）实现一种系统配置的修改，作为一种对系统使用过程中的病毒破坏机制；

5、利用C或C++，也可以利用MASM32或HAL语言（高级汇编语言）实现；