《软件安全漏洞分析与发现》

第1次 作业

中国科学院软件研究所

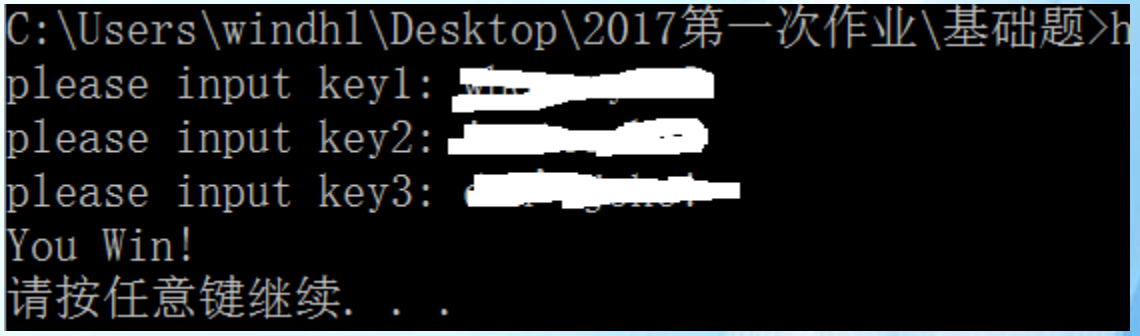
2018年3月28日

- 班级微信群：2018-漏洞课程

- 群名片：格式为“姓名-培养单位”，如“和亮-软件所”

- 作业安排
  - 基础题+挑战题
  - 题目发布时间：**2018年3月28日**
  - 作业提交内容：
    - 汇报PPT（基础题和附加题 必须）**需要如实写清楚每个人的分工情况**
    - 程序源码、使用说明（附加题 必须）
    - 其他材料（视频录像等 非必须）
  - 作业提交截止时间 **2018年4月12日 - 23:59:59**
  - 作业汇报：
    - 通知汇报：**2018年4月16日**
    - 汇报形式：由组长本人或推荐组员
    - 汇报时间：**2018年4月18日**
  - 格式要求：
    - 压缩包形式上传到课程网站
    - 命名规则：学员_姓名_培养单位.rar
    - 每组3-5人，压缩包内附组员名单

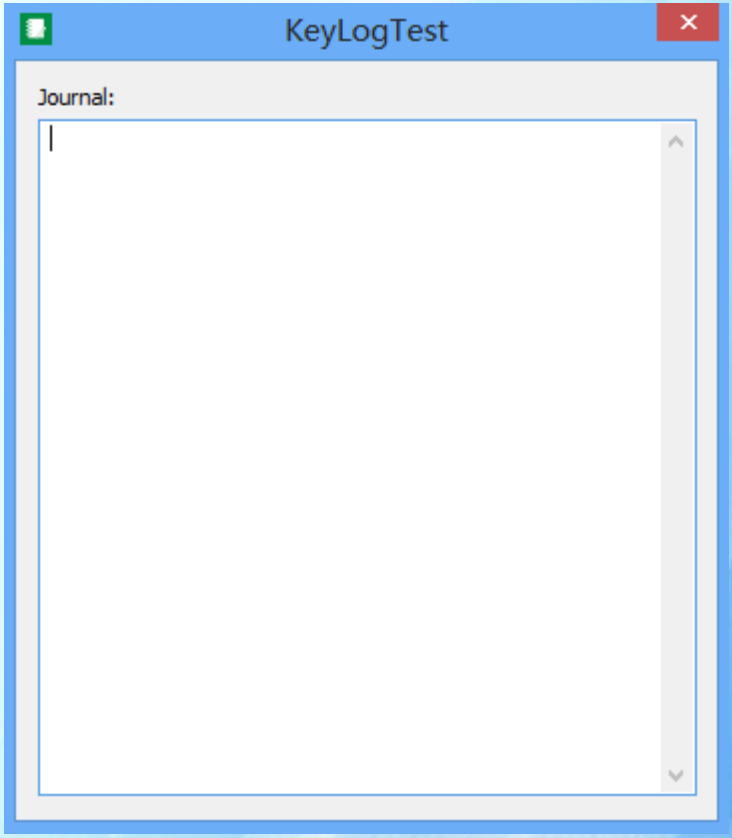
- 基础题(难度系数1)（80%）
  - 给定一个可执行文件和动态库
    - homework1.exe：程序主流程且负责对第一个密语进行解密(decode)
    - Dll2.dll：负责另外两个密语的解密(decode）
  - 猜出三个经过解密的密语
    - key1: 简单计算
    - key2: 复杂计算
    - key3: 移位计算



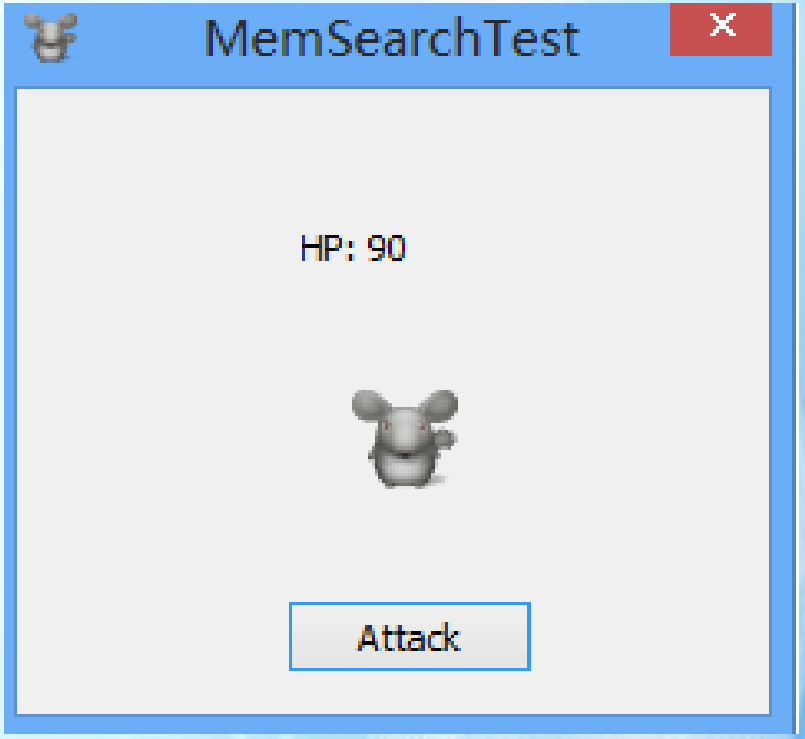
  - 汇报基本要求：
    - Do It Yourself!
    - 可提供作业形式：程序流程图、程序分析报告、……
  - 提示
    - 使用IDA Pro (F5)进行静态逆向或者动态内存调试
    - 若采用静态方法，key1可在主程序中寻找，key2和key3需要在动态库中寻找答案
    - 原始Dll2.dll文件经过简单加密，请注意正确输入第一个密语后生成的中间文件

- 挑战题
  - 选做题（二选一）（20%）：
    - **键盘精灵（难度系数 2）:**实现针对模拟记事本程序的按键信息记录
    - **我生永恒（难度系数 3）:**保证模拟游戏中小老鼠不被打死
  - 加分题 （+5）：
    - **盗梦空间（难度系数 3）:**通过进程注入Explorer.exe进程空间，启动目标程序
- 汇报要求：
  - 1. 技术思路、技术方案，以及方案优缺点讨论
  - 2. 任务完成的演示视频录像

- 键盘精灵（木马病毒入门）
  - 请开发一个键盘记录工具
    - 记录且仅记录用户键入右侧图示记事本程序的按键信息
  - 提示：
    - 运行环境：Windows XP系统
    - 键盘钩子（SetWindowsHookEx)
    - 键盘状态查询（GetKeyState）
    - 键盘驱动（IRP Hook）



- 我生永恒（游戏外挂入门）
  - 附件是一个攻击小老鼠的游戏
    - 每次点击”Attack”按钮，小老鼠的血量减10，当小老鼠血量减到0时游戏结束
  - 请开发一个小工具
    - 锁定该游戏中小老鼠的血量，使其永生
  - 提示：
    - 运行环境：Windows XP系统
    - 内存热补丁，搜索内存空间中老鼠血量对应变量，保持该变量不变



- 盗梦空间（Hacker入门）
  - 该程序直接点击后弹出对话框，但在Windows命令行下启动程序不会弹出对话框
  - 请开发一个小工具
    - 该工具能够加载该程序，使其弹出对话框
  - 提示：
    - 运行环境：Windows XP系统
    - 直接点击时，程序进程创建由Explorer.exe完成
    - 尝试注入Explorer.exe，在该进程中创建线程，由该线程启动该程序