

“网络安全综合实验（I）”实验报告

**题目： Windows桌面安全实践**

院 系 网络空间学院

专业班级 信安1901班

姓 名 李欣宇

学 号 U201911658

日 期 2020 年 11 月

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 评分表 | Windows桌面安全实践（50分） | | | | 完成（50分） | 成绩 | |
| 评分 项目 | 过程 | 分析与小结 | 撰写 | 创新 | 完成任务 | 合计 | 教师 |
| 分值 | 20 | 20 | 5 | 5 | 50 | 100 | 签名 |
| 评分 |  |  |  |  |  |  |  |

报告要求及评分规则

1.请按照模板给出的格式，包括行距、字体、段落格式等，完成报告；

2.报告封面保持一致(如实填写基本信息及完成日期)；

3.实验报告内容应包括：封面、评分规则、实验过程记录、实验问题分析与总结、参考文献及资料列表；

4提交：电子材料应包括本实验电子版（doc）、实验参考文献资料的电子资源文件（pdf）。

5.主要考察能力： 实验动手能力、问题分析与归纳能力、文档规范撰写能力、创新能力；

6.其他要求：可按指导老师要求的时间和提交方式提交；每次课实验报告可以单独提交；如果需要最终纸质报告的，可去掉模板中说明文字（斜体）之后，双面打印；

7.总评分=课程每次实验分数之和/课程实验次数。

其中：

每次实验分=实验完成分（50分）+实验报告分（50分）-扣分+加分；

计算方法：

实验完成分=（完成任务数量/总任务数量）\*50；

实验报告分=以下1-4项合计；

1）过程（要求：实验过程完整、清晰）(满分20)（优秀：18+ 良好：16+ 一般：14+）；

2）问题分析与小结（要求：有条理、细致）（满分20）（优秀：18+ 良好：16+ 一般14+）；

3）撰写（要求：语句通畅、格式规范）（满分5）（优秀：4+ 良好：3+ 一般：2+）；

4）创新（要求：见解独到、有创意）（满分5）（优秀：4+ 良好：3+ 一般：2+）；

扣分=报告迟交天数\*2分（满分10分）  （发现雷同抄袭的内容，该次实验不得分）；

加分=搜集整理与实验相关的学习资料作为附件，资料能帮助同学更好掌握相关知识的；获得同组人互评优秀的；提交最终报告时间为班级前3名。（满分5分）（项数\*1分）；

同组评价：

本实验中你的同组人姓名： 刘颖 学号： U201911663

你给同组人评价： 优 （优 良 中 及格）；

理由： 完成任务快速，质量较高，对我给予一定的帮助。

# 实验一：Win系统与桌面安全实践

## 实验环境及要求

**实验平台（1-2个虚拟机）：**

VMWare 12以上 或者 Virtual Box6.0以上。

配合安装：

1：windows7虚拟机

2：360 安全卫士

3：钩子工具Firewall Leak Tester

4：Wireshark截包工具

5：VC6或者VS2010开发环境

上述软件下载地址由教师在线公布。

虚拟机网络ip配置：采取NAT方式接入网络，IP动态获取

**实验分组（2人）**：

结合网络教学的实践课程，Win系统与桌面安全为一项基本技能，本实验要求每位同学独立完成，组员之间可以讨论交流。

**场景设置：**

2020年进入网络安全学院学习，开始思考自己网安兴趣到底在哪里。9月份的国家网络安全宣传周又要启动了，里面宣传的特别多的是个人隐私如何泄露。那你作为专业大学生，能不能不只是停留在文字宣传上，应该做一些实验，做一些技术验证呢？探讨下Win主机上我们的关键的个人信息是如何被窃取，如何被传输的呢？你需要掌握哪些技能呢？

根据上述场景，需要你完成以下操作，作为Windows系统安全与桌面安全实验通关考核。请你单独完成安装、编码、调试与测试，遇到问题可以与其他同学讨论，各自保留实验中的完整虚拟机截图，遇到问题，寻找解决方案，并做好记录，最后，将通关过程、记录的文字，整理成报告提交。

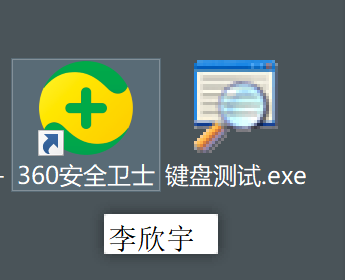
注意:以下关卡内容的可以通过参考资料获取更多说明。已经上传至在线课程平台。

## 实验任务（共6个小任务关卡）

### 任务1 安装VMWare与windows7虚拟机相关工具：

**注意在上个实验基础上，下载360安全卫士与钩子测试工具，安装并测试使用。**

过程记录：下载安装360与钩子测试工具



### 任务2 360安全卫士分析虚拟系统状态：

打开360安全卫士。

1. 打开系统优化功能，查看当前系统自动启动了哪些进程、服务以及组建,查阅资料，学习进程、线程的基本原理；
2. 打开网络流量监控功能，查看系统当前哪些进程对外通信，其通信地址、端口分别是什么；
3. 查看自启动进程与服务的签名，通过签名判断进程的合法性。

过程记录：

（1）打开系统优化功能，查看自启动进程

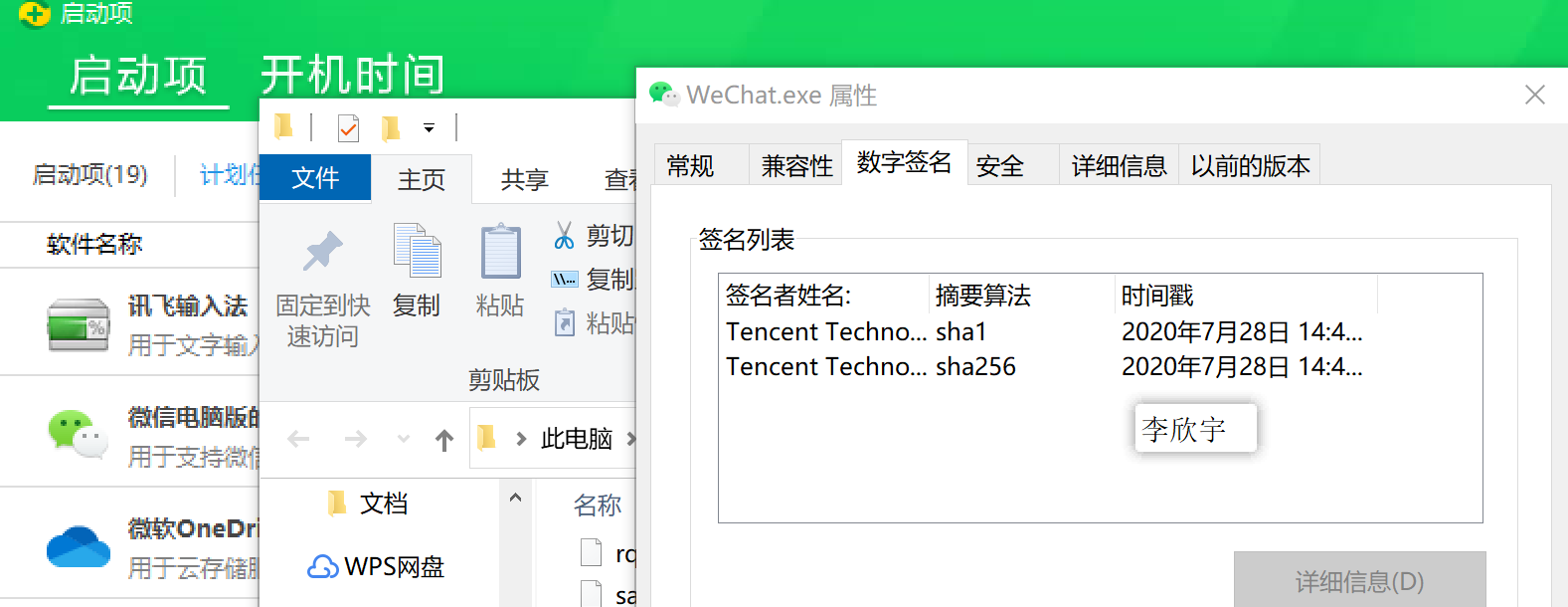


![KZI4KKJ)](8)(WIP[])PL~1](data:image/png;base64,)

（2）使用网络流量监控功能，查看哪些进程对外通信，并查看地址与端口



（3）查看自启动进程与服务的签名（以微信为例）



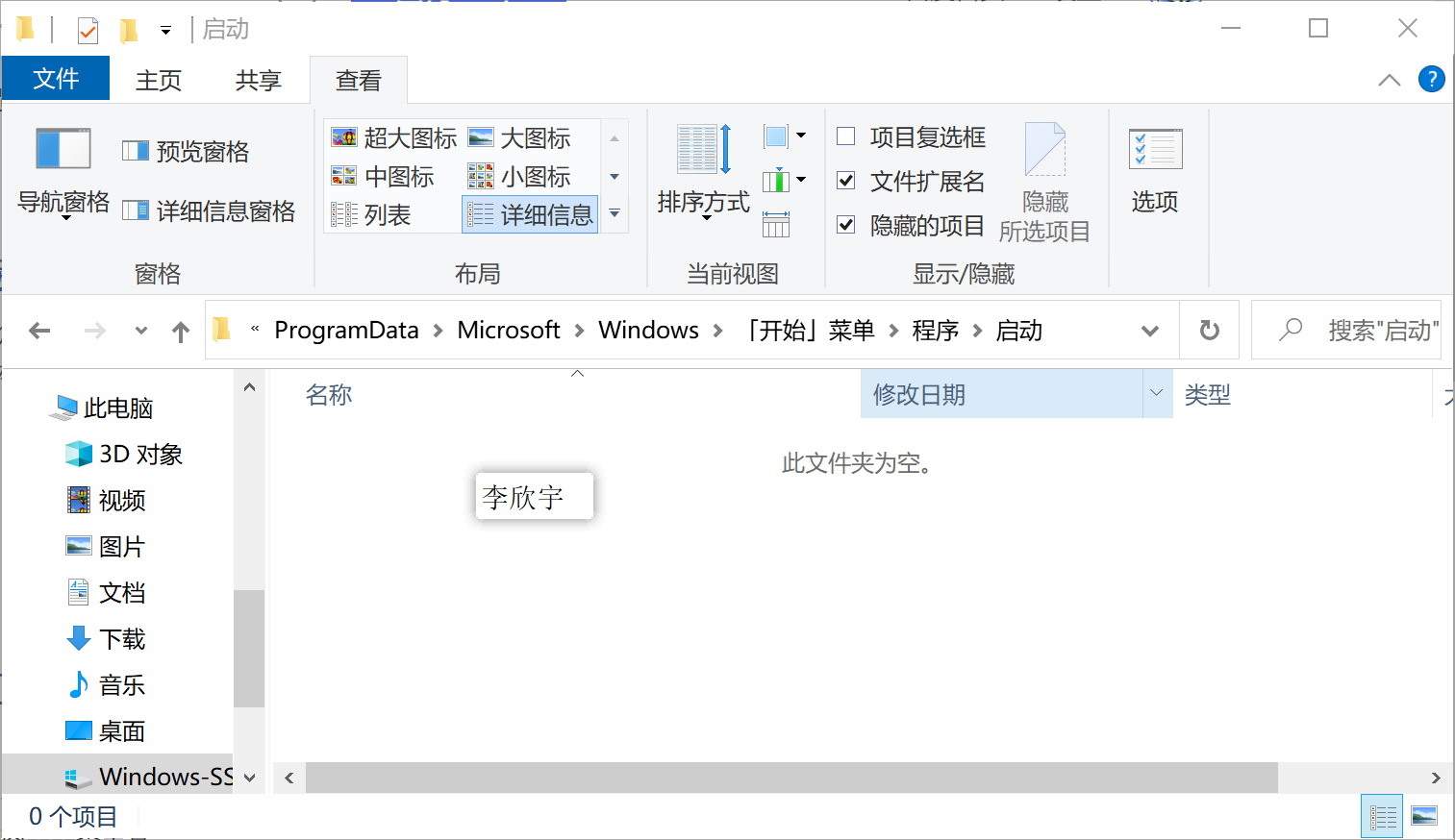
### 任务3 Windows自启动进程测试

在虚拟机中测试Windows进程自启动的原理。

过程记录：

1. 对所有用户有效的启动文件夹

这是寻找自动启动程序的第二个重要位置，不管用户用什么身份登录系统，放入该文件夹的快捷方式总是自动启动，这是与用户专有的启动文件夹的区别所在。该文件夹一般在C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp。



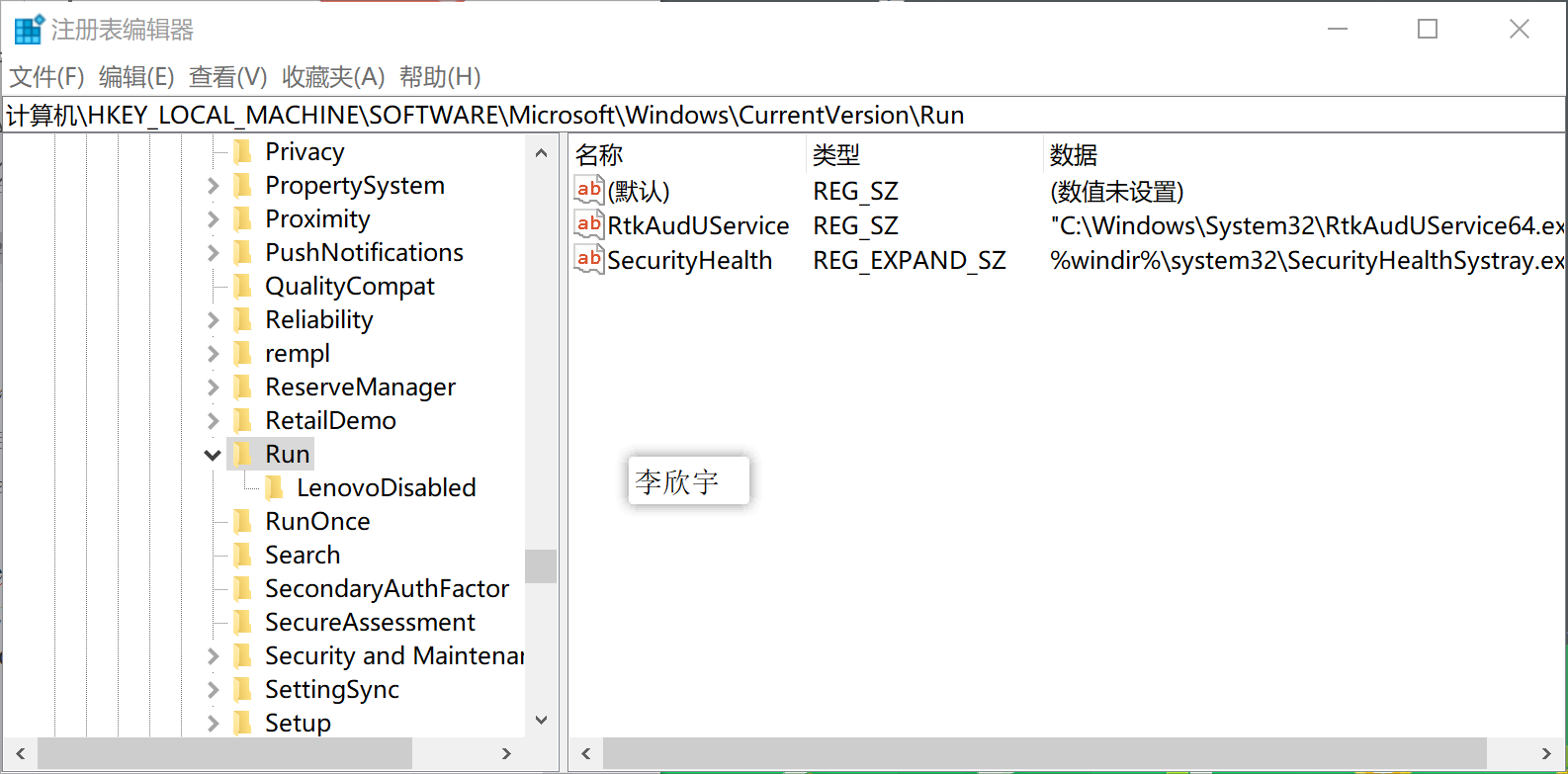
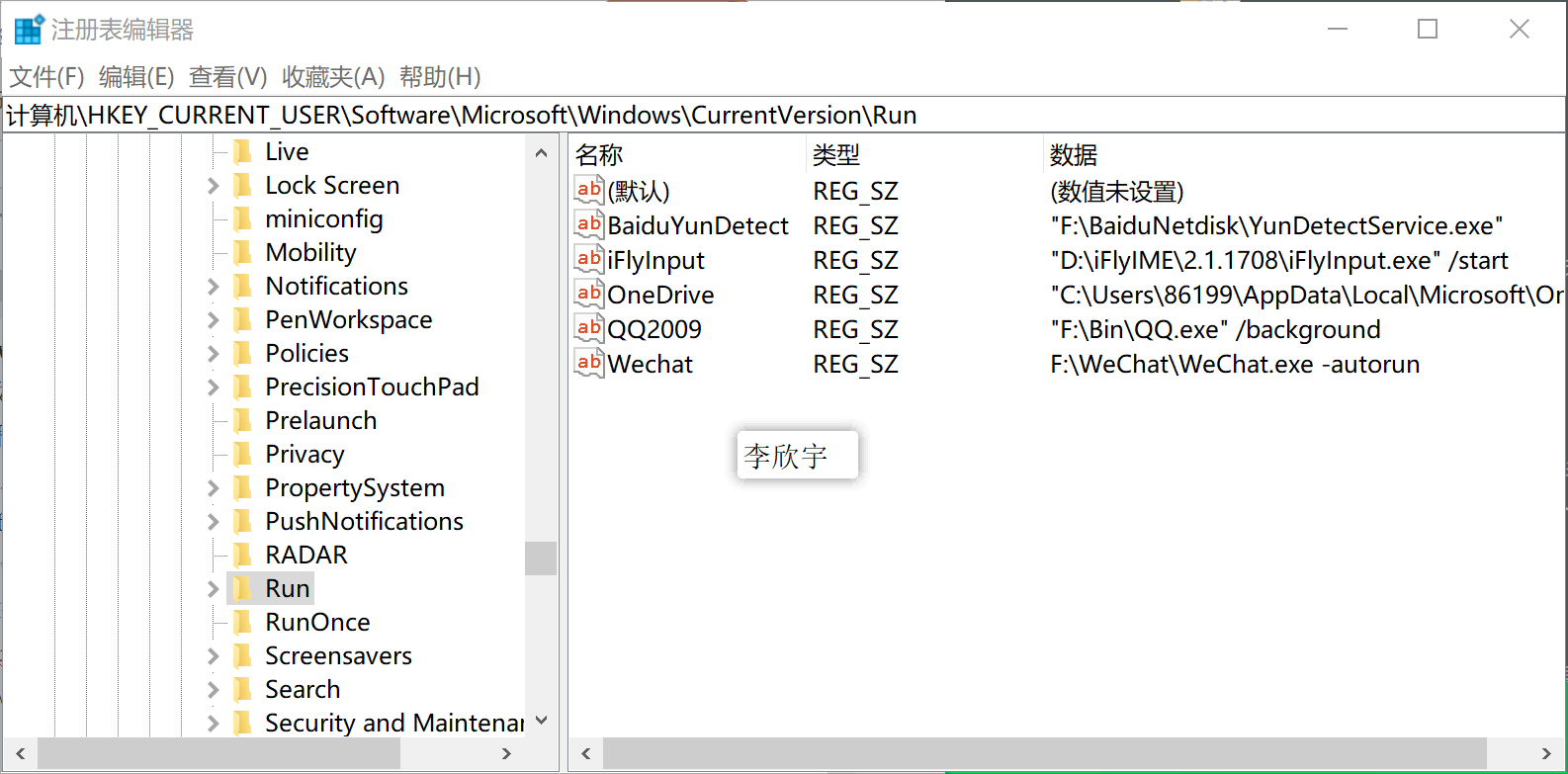
2) RunServices注册键

RunServices注册键指定的程序紧接RunServicesOnce指定的程序之后运行，但两者都在用户登录之前。RunServices的位置是HKEY\_CURRENT\_USER\Software\ Microsoft\ Windows\CurrentVersion\RunServices和HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\RunServices。

无。

3) Run注册键

Run是自动运行程序最常用的注册键，位置在HKEY\_CURRENT\_USER\ Software\ Microsoft\ Windows\CurrentVersion\Run和HKEY\_LOCAL\_MACHINE\SOFTWARE\ Microsoft\ Windows\CurrentVersion\Run。HKEY\_CURRENT\_USER下面的Run键紧接HKEY\_ LOCAL\_MACHINE下面的Run键运行，但两者都在处理“启动”文件夹之前。



### 任务4 Windows钩子测试

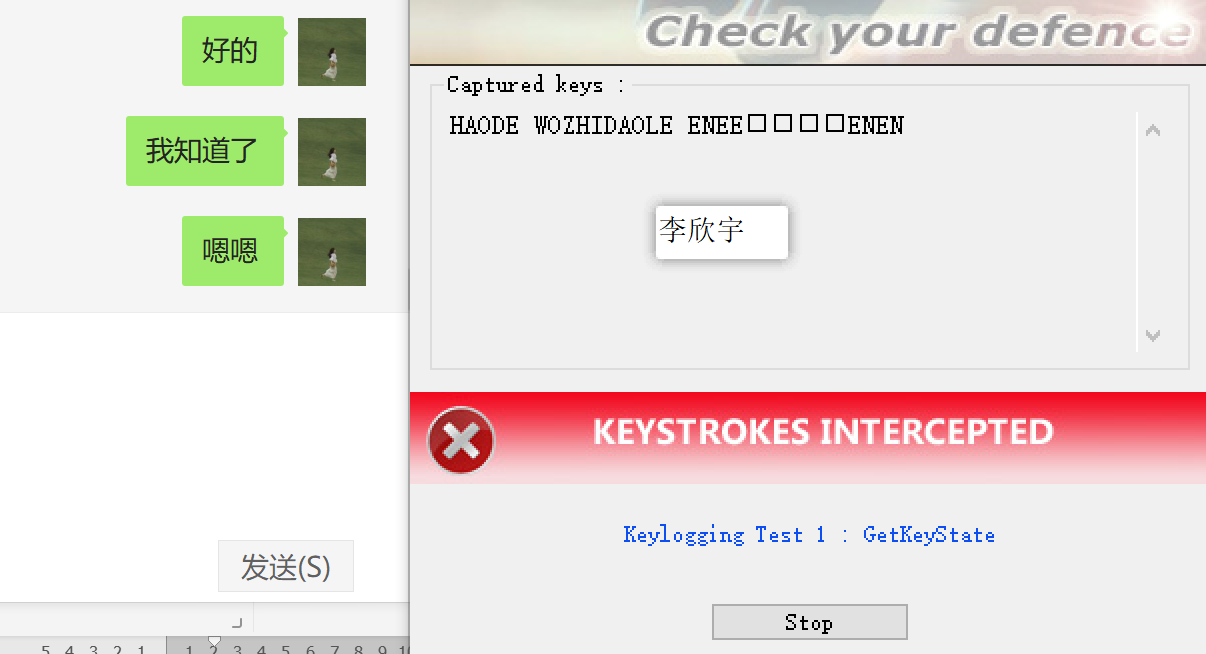
钩子的本质是一段用以处理系统消息的程序，通过系统调用，将其挂入系统。钩子的种类有很多，每种钩子可以截获并处理相应的消息，每当特定的消息发出，在到达目的窗口之前，钩子程序先行截获该消息、得到对此消息的控制权。此时在钩子函数中就可以对截获的消息进行加工处理，甚至可以强制结束消息的传递。而键盘钩子，只是为了截获键盘消息的。全局钩子可以捕获在Windows平台下任意窗口上的键盘操作。本实验通过钩子工具测试各个应用程序的防密码窃取性能。测试使用的键盘钩子Firewall Leak Tester共集成了7种原理不同的钩子,可以用来验证应用程序是否能够抵抗钩子截获。

1. 测试桌面版QQ/微信/淘宝 等三款社交购物软件输入框是否能够抵抗钩子截获密码；
2. 选取至少3款网上银行或者证券公司的登录页面，测试是否能够抵抗钩子；
3. 分析自己的测试过程，并探讨如何改进防止口令被窃。

过程记录：

（1）选取 qq、微信聊天对话框、网页版淘宝

经测试，qq输入的密码不能被截获，但是淘宝和微信聊天对话框得输入内容都会被截获



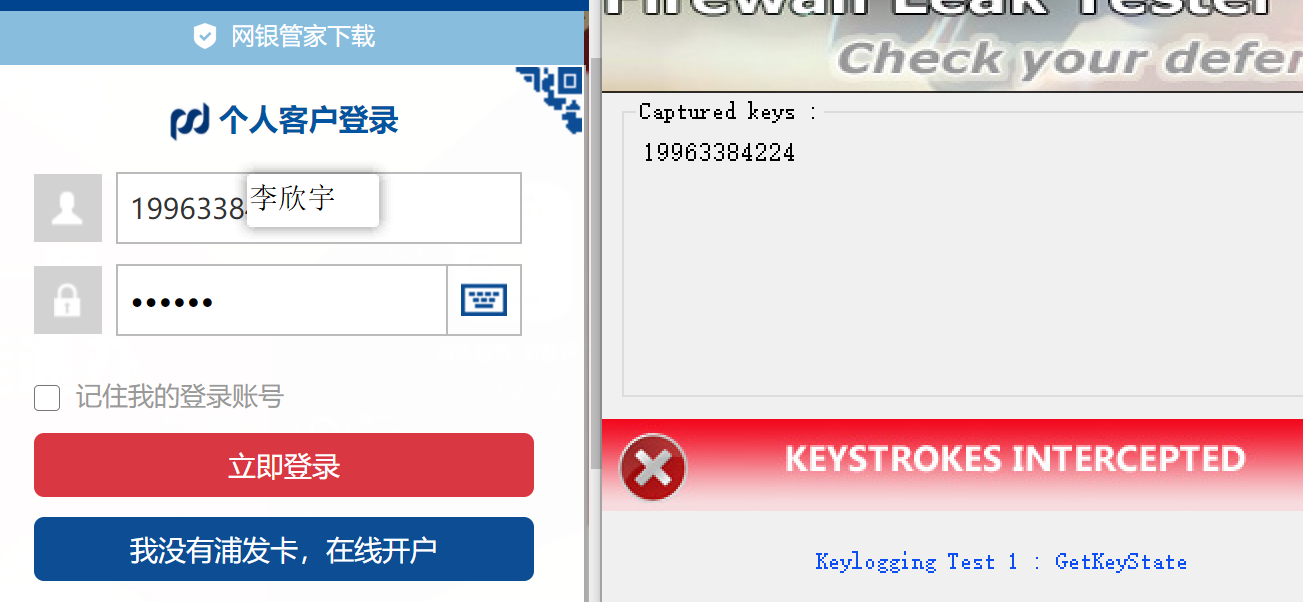
![}CNBL$1](I@_SLC[F]E]FXI](data:image/png;base64,)

(2)选取中国银行、中国建设银行、浦发银行三个电子银行登录界面进行测试

测试发现，中行与建行密码输入时均会被钩，浦发银行不会钩到密码







（3）钩子实际上是一个处理消息得程序段，通过系统调用，把它挂入系统，每当特定消息发出，在没有到达指定窗口前，钩子程序就先捕获该消息，即钩子函数先得到控制权。如果要防止口令被截获，可以安装对应网站提供的安全插件，或在最初不小心打开钩子软件时有360拦截，对此进行拦截，避免钩子程序运行。也可以卸载钩子程序。

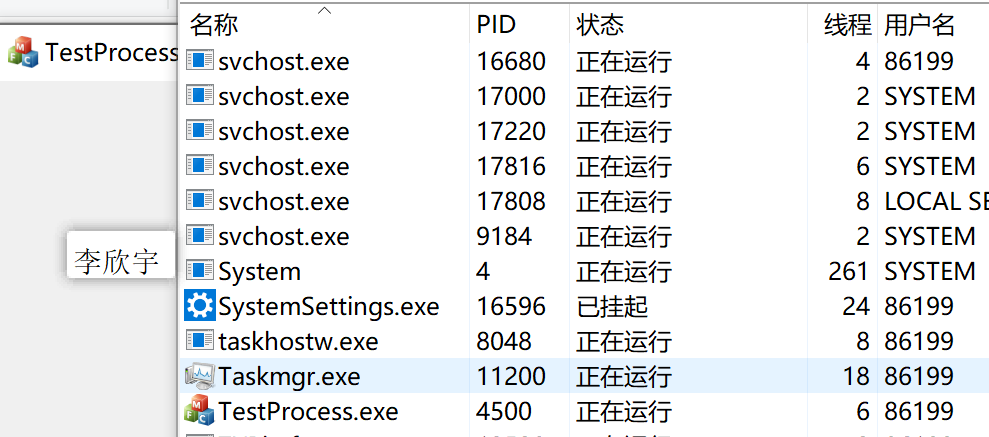
### 任务5 进程与线程原理测试

1. 进程与现成测试

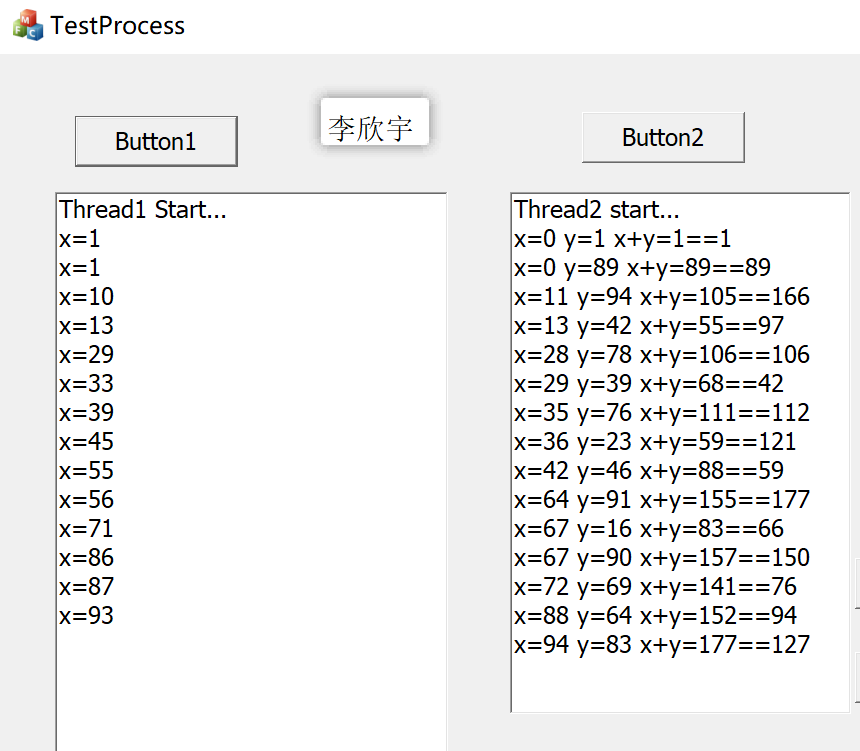
过程记录：

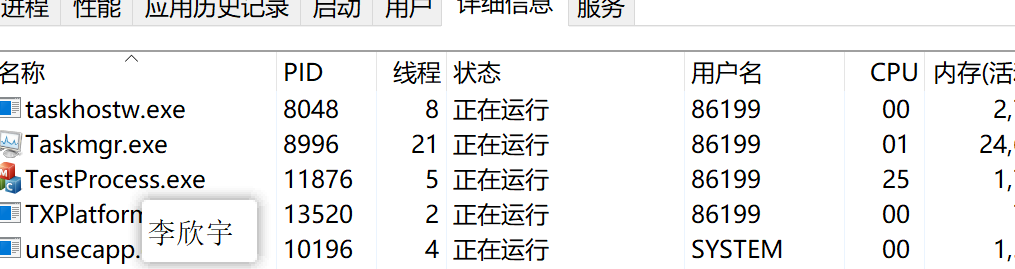
1）创建一个基于对话框的应用程序TestProcess。

1. 编译、链接后，在Debug目录下生成一个可执行程序TestProcess.exe，该程序运行起来，就会形成一个进程。打开任务管理器，就可以看到TestProcess.exe进程，该进程有1个线程。



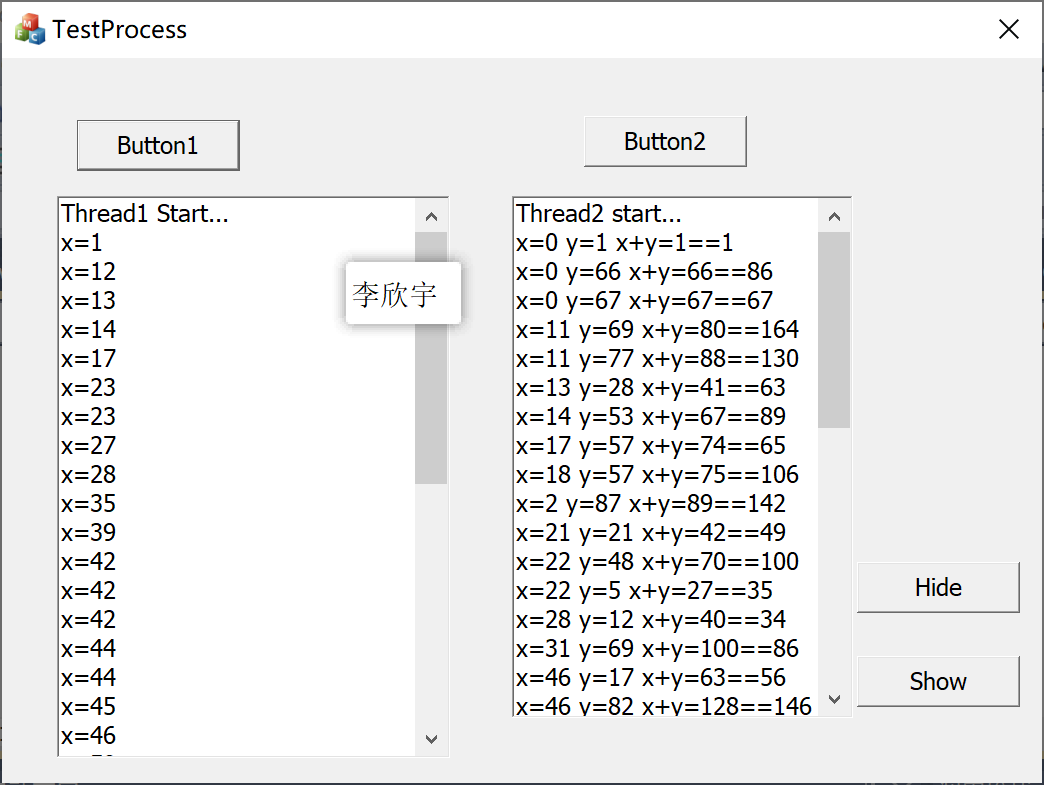
1. 现在通过该进程，创建多个线程进行测试。首先在界面上放入两个按钮与两个ListBox。
2. 在源文件中，首先添加老师给予的代码，调bug
3. 点击按钮测试效果,并打开任务管理器查看线程





1. 进程隐藏与显示

过程记录：在两个按钮下分别添加以下代码，可实现进程后台运行



### 任务6 程序如何通过网络连接发送数据

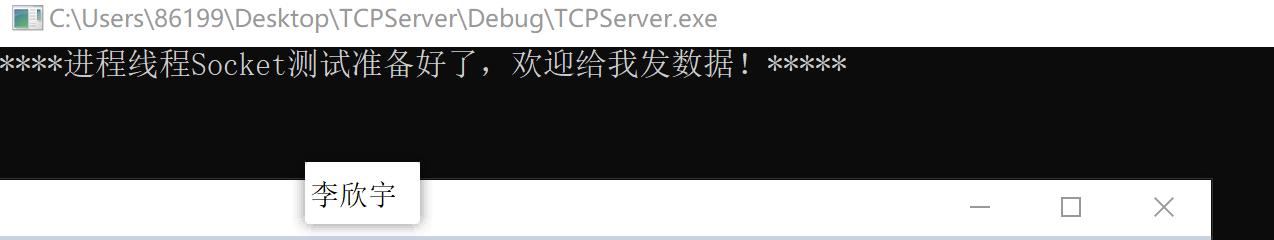
本实验主要实践有关网络连接的基本过程，有关网络通信的更多知识可以参阅计算机网络专业课程。

对于计算机系统来讲，往往存在多种网络服务与连接，同时打开多个端口以及向其他服务器发起多个网络连接，可以通过桌面安全软件360安全卫士查看这些网络连接。同时用Wireshark查看发送数据报文。

过程记录：

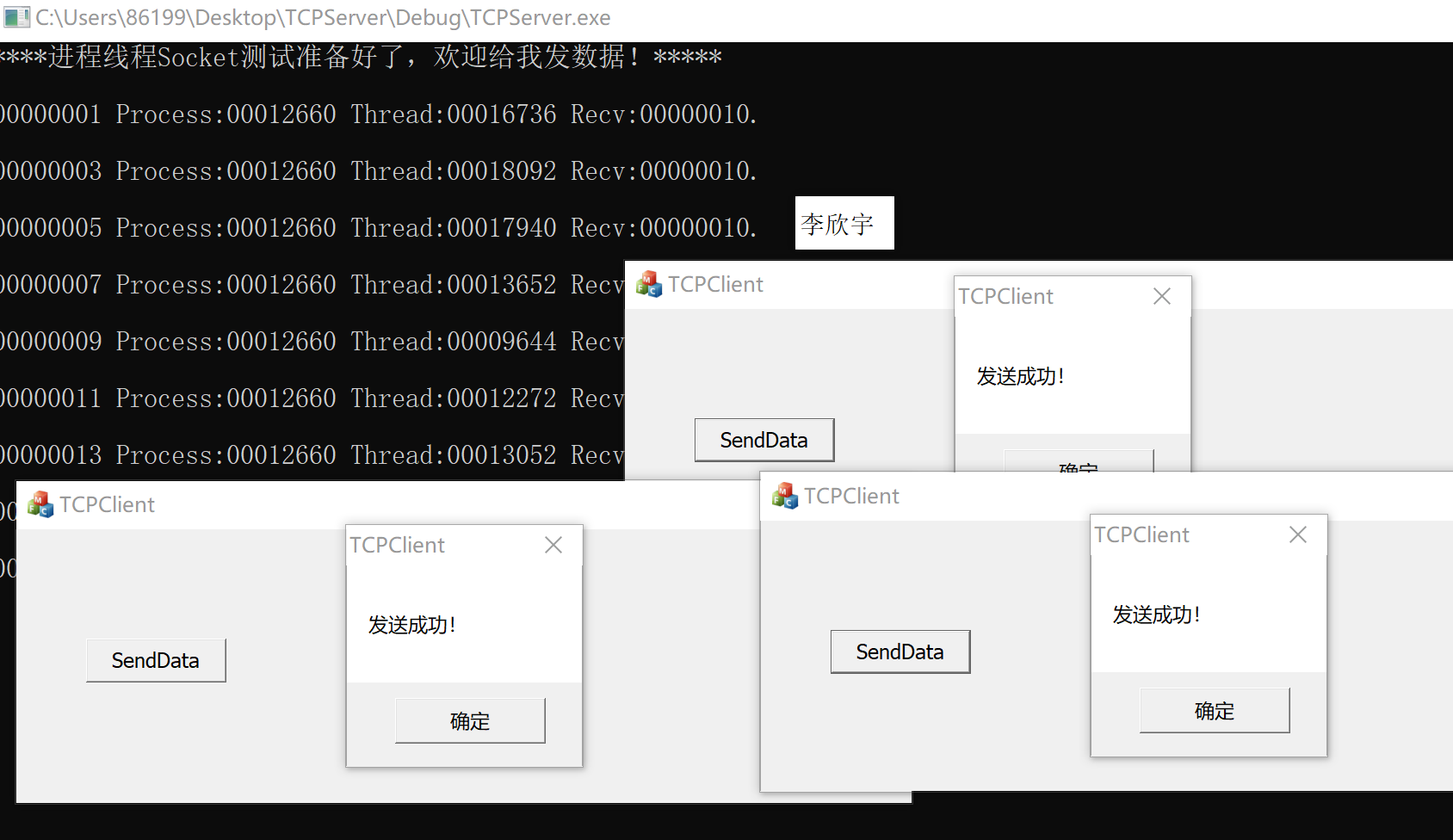
首先创建服务端接收数据的程序，通过VS2010中的File-New-Projects，选择Win32 console Application,命名为TCPServer，加上老师给的代码，编译运行。

该代码打开了本地的1036号端口，运行后，等待客户端向本端口发起TCP连接进行数据发送或者接收。



接着，创建网络连接客户端程序，在按钮事件响应void CTCPClientDlg::OnOK()中增加老师给的代码。

此代码采用TCP向服务端的1036号端口发起网络连接，并发送buffer中的数据后，接收服务器的返回数据。可以实现多线程同时发送数据。



### 扩展阅读：

请结合前面的钩子程序、进程、线程以及网络通信程序，分析木马程序如何把个人信息发送出去，你能写出这样一个密码发送程序吗？

# 小结：学习心得与体会

通过本次实践，虽然没能亲手写代码，但是通过对照老师的代码敲的时候也体会到了多线程是如何实现的，包括前面对360查看自启动项、注册表等，进一步对我们的系统内部架构进行了解，虽然还只是浅层次的，但仍有所得。最后一项任务程序通过网络连接发送数据不仅让我学到了相关知识，更让我体会到其中的乐趣，安全其实是一件很有意思的事。