“网络安全综合实验（I）”实验任务书

Windows系统与桌面安全实践 （第3次实验）

实验者：

指导教师：付才 陈凯 刘铭 王美珍 肖凌

2020年11月

# 目　录

[1 实验一：Win系统与桌面安全实践 1](#_Toc56455750)

[1.1 实验环境及要求 1](#_Toc56455751)

[1.2 实验任务（共6个小任务关卡） 2](#_Toc56455752)

[2 小结：学习心得与体会 9](#_Toc56455753)

[参考文献： 10](#_Toc56455754)

# 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。

**参考资料**：《网络空间安全实践能力分级培养》第二章与第三章，人民邮电出版社。

**最终提交文档及写作要求**：本实验提交独立实验过程截图与小结。

**文档中包含内容**：1.完成任务的过程，包括主要截图及相应的过程说明文字.2.小结：总体感受、实验中遇到的最突出问题及收获、对实验环节的意见和建议 3.实验中查阅资料的页码、网址作为参考文献部分列表给出 4.参考资料通过浏览器的打印功能，以pdf文件方式保存，归档为：参考资料.zip，与报告一并提交。其中3-4为可选项。

**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：

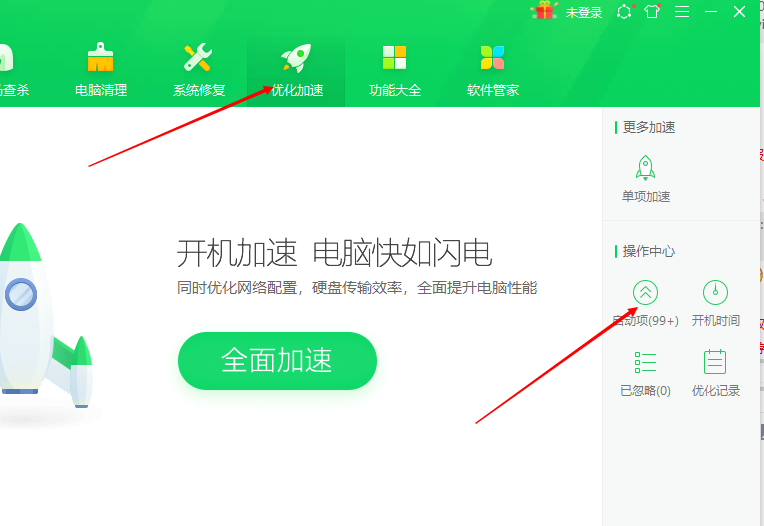
**注意在上个实验基础上，下载360安全卫士与钩子测试工具，安装并测试使用。**

详细步骤请自己截图补充。

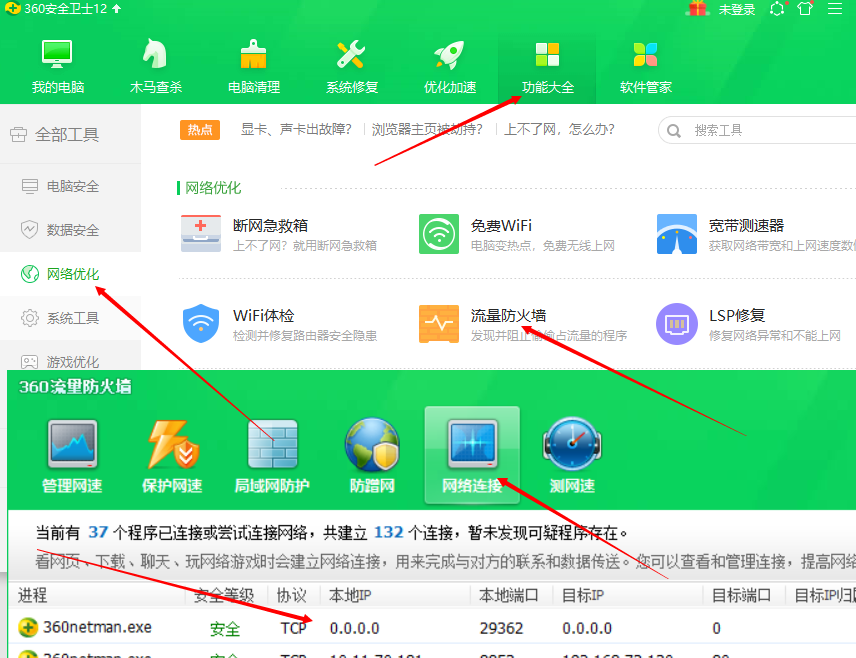
### 任务2 360安全卫士分析虚拟系统状态：

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；



1. 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；



1. 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。

### 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**：

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。

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。

测试上述自启动方式。另自己查阅资料，看看还有没有其他自动启动方式。

### 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。

### 任务5 进程与线程原理测试

**打开VC++6.0,完成以下步骤：**

1. 创建一个基于对话框的应用程序TestProcess。
2. 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。
3. 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。
4. 在源文件中，首先添加如下代码。

#include "Mmsystem.h"

#pragma comment(lib,"Winmm.lib");

int x=0;



在资源编辑器中，双击对话框第一个按钮，在事件响应中增加如下代码。

void CTestProcessDlg::OnButton1()

{

// TODO: Add your control notification handler code here

DWORD ThreadID;

CreateThread(0,0,Thread1,this,0,&ThreadID);

}

双击第二个按钮，在事件响应中增加如下代码。

void CTestProcessDlg::OnButton2()

{

// TODO: Add your control notification handler code here

DWORD ThreadID;

CreateThread(0,0,Thread2,this,0,&ThreadID);

}

F5编译运行，并点击按钮，测试其效果。注意打开任务管理器，查看进程与线程的变化。

1. 进程隐藏与显示

进程隐藏往往是病毒或者其他恶意软件的行为。进程隐藏有多种层次，最简单的是将界面隐藏起来，使桌面上看不到该程序，但任务管理器中可以看到；还有一种是任务管理器中也看不到，有些恶意软件甚至连执行的程序都没法在文件系统中找到。

本实验实现界面隐藏。

在对话框资源编辑器中，双击确定按钮，增加如下代码。

void CTestProcessDlg::OnOK()

{

// TODO: Add extra validation here

//CDialog::OnOK();

SetWindowText("TestProcess");

ShowWindow(SW\_HIDE);

}

注意注释掉CDialog::OnOK();

F5执行，单击确定，会发现该程序界面消失，但在任务管理器中该进程依旧在运行。

接下来，通过窗口查找将该隐藏的进程显示出来。

单击VS6.0中的project-Add to Project-New-Projects，在当前工程中增加一个对话框程序TestProcess2，在新增加的按钮事件响应中增加如下代码。

void CTestProcess2Dlg::OnButton1()

{

HWND h=::FindWindow(0,"TestProcess");

if(h!=INVALID\_HANDLE\_VALUE){

::ShowWindow(h,SW\_SHOW);

}

}

编译执行，单击该按钮，发现原来隐藏的界面显示出来了。这是界面程序隐藏的基本过程。

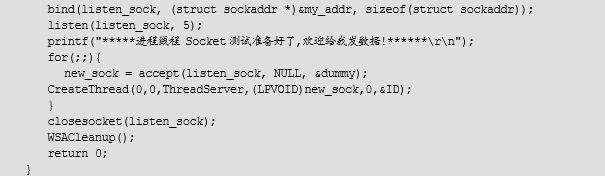
如果要实现在任务管理器中找不到该进程，则还需要配合函数钩子Hook技术，读者可以自己尝试实现，该技术将在分级培养后续中涉及。

### 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。

首先创建服务端接收数据的程序，通过VS C++6中的File-New-Projects，选择Win32 console Application,命名为TCPServer，代码如下。

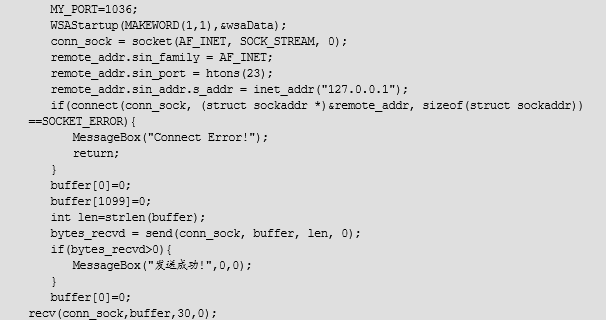




编译运行。

上述代码打开了本地的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()中增加如下代码。



上述代码采用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。

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。

### 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

学生自己总结本次实验的内容，心得体会，意见和建议。

# 参考文献：

这部分要求学生把查阅的资料整理出来，并附上pdf归档包，作为积累的内容。