网安实践（三）暨首次Windows应用开发

键盘钩子（HOOK）相关

Problems

* 实验手册提供的Firewall Leak Tester是一款非常古老的应用，从检索到的信息看，上次更新可能还在10年以前

Solutions

* 大部分能检索到的hook信息都非常古老，在知乎上查询到可以用两种方法自行开发键盘钩子
  + 方法一：使用ctypes库利用Windows Api
  + 方法二：使用封装在Keyboard库中的hook函数
* 两种都给出了实例代码
* 发现使用虚拟键盘可以有效避免这一问题

多线程相关

Problems

* 首先想到的是python的threading库
  + 查询发现python的多线程本质上是依然是在解释器内运行的伪多线程
* 暂定采用C++ thread库

Solutions

* 开发环境选择vscode+gcc
* 基本实现了创建多个进程和销毁的功能
  + 利用windows api实现了进程窗口隐藏，但依然可以从任务管理器中观察到
  + 缺少的功能：按钮和图形界面（可以考虑tkinter实现）

TCP网络编程相关

Problems

* 给出的代码比较混乱（比如，为什么要用Windows媒体api呢？），决定用python socket/tcp重写

Solutions

* 查询知乎和socket库后简单编写了服务器和客户端socket通讯的python实现
  + 可以以此为基础开发简单的网络应用
  + 发现C/C++的socket库和python基本一致

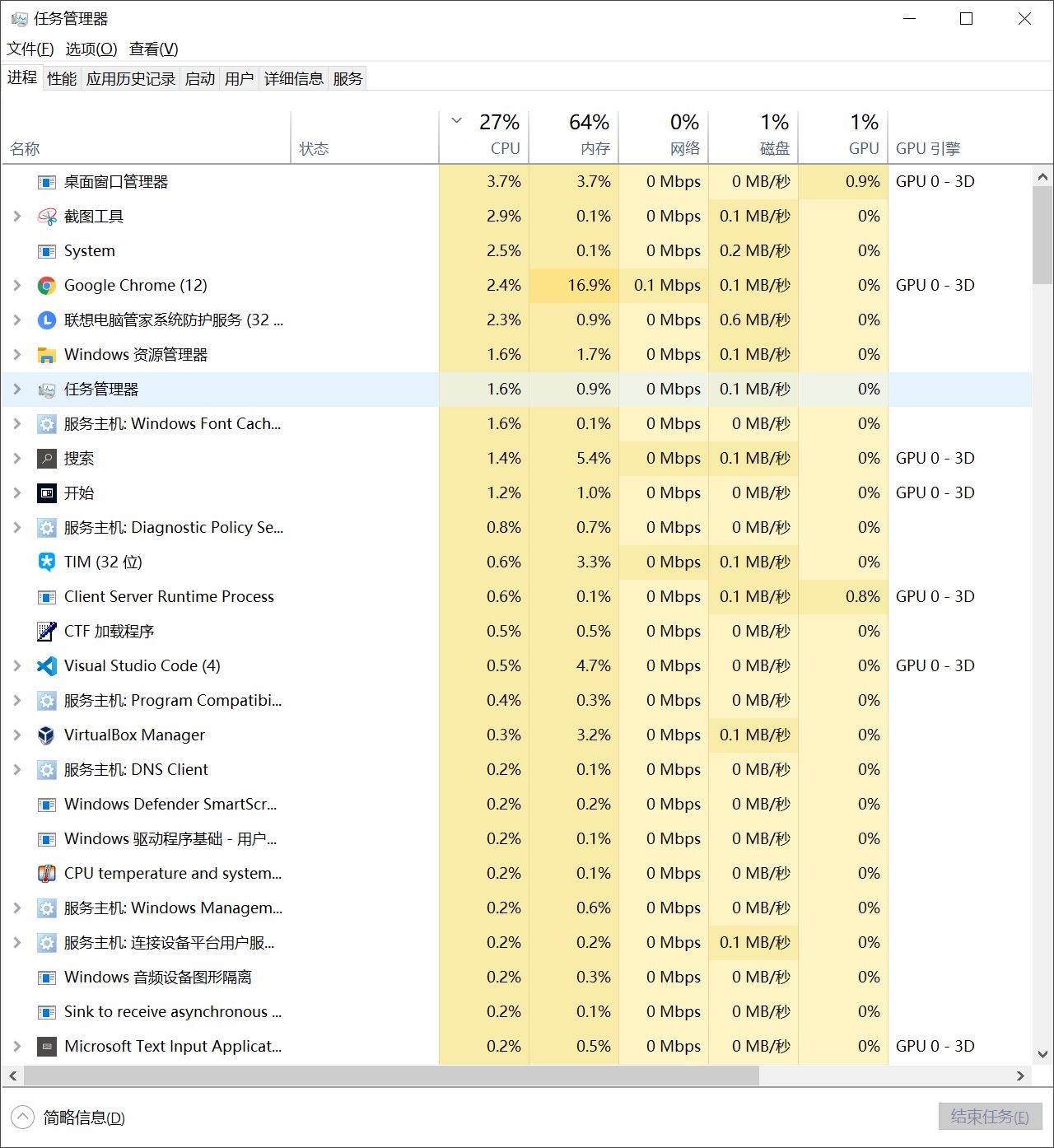


图1 通过任务管理器查看进程和线程

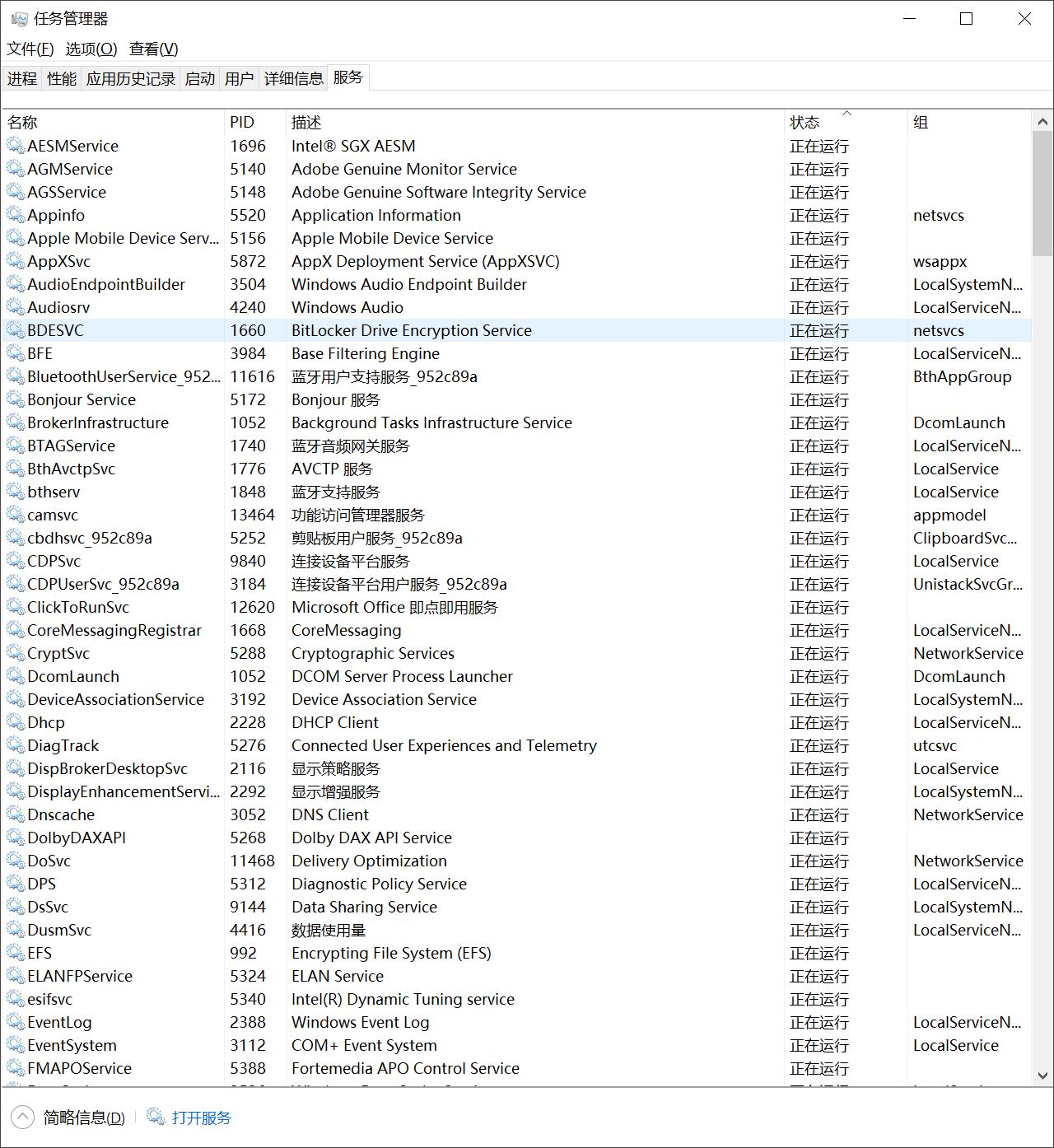


图2 通过任务管理器查看正在运行的服务



图3 随机选择了一个正在运行的服务通过属性查看数字签名

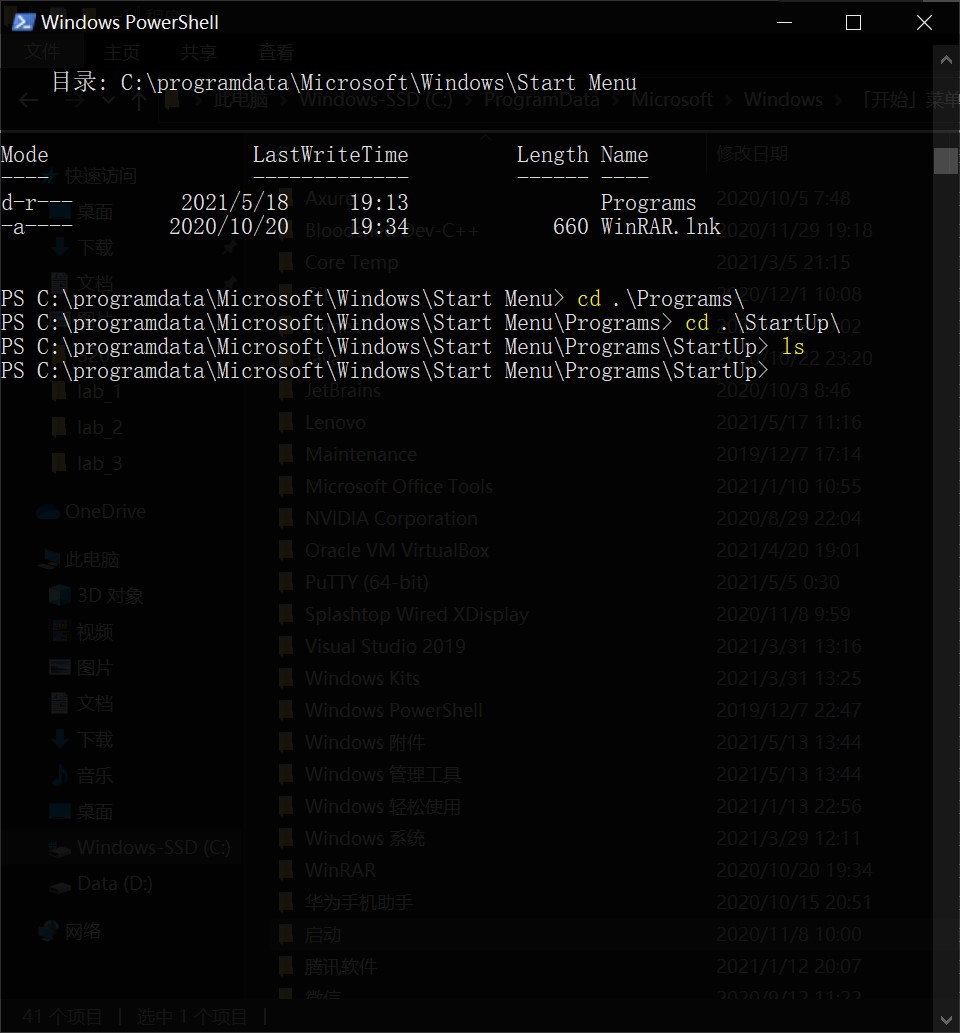


图4 查看startup自启动文件夹

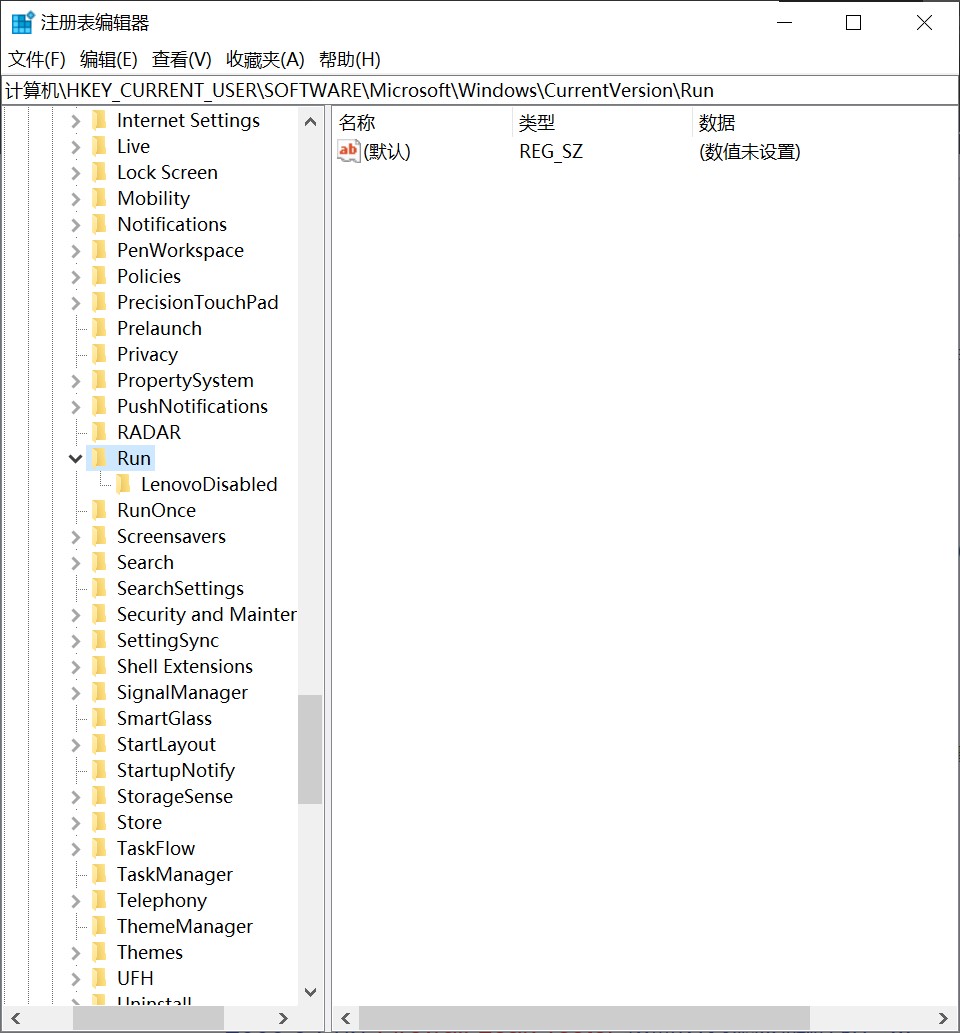


图5 在win10注册表中，没有注册键



图6 测试钩子应用（python）

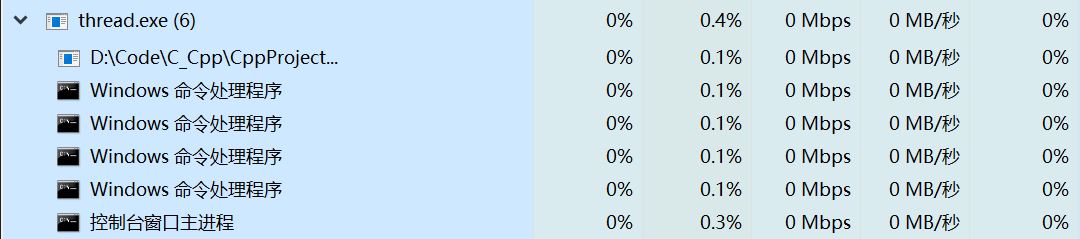


图7 运行后可在任务管理器内查看到的四个线程

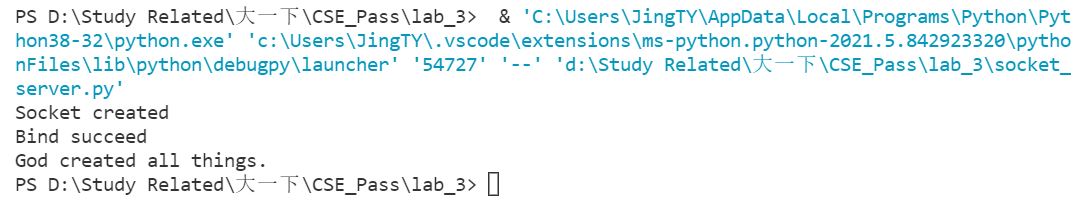


图8 启动socket服务器端

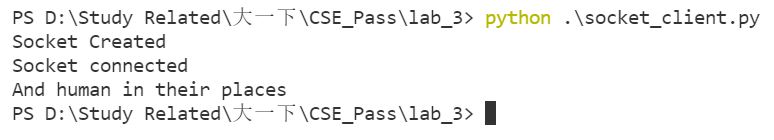


图9 启动和连接socket客户端