**Project Report: Keylogger**

* **Date:** August 10, 2024
* **Author(s):** [Arbaz khan]

#### **Introduction**

The Keylogger project is a simple Python-based application designed to record and log keystrokes on a computer. This type of software is typically used in security analysis, ethical hacking, or for monitoring purposes. It’s important to note that keyloggers must be used responsibly and legally, as unauthorized use can infringe on privacy rights and violate laws.

#### **Project Overview**

This Keylogger project was developed using Python and the pynput library, which facilitates the monitoring of input devices such as the keyboard. The project captures every keystroke made by the user and writes it to a file for logging purposes.

#### **Code Explanation**

1. **Importing Required Modules**:
   * The pynput.keyboard module is imported to allow for keyboard monitoring. Specifically, Key and Listener are imported from the pynput.keyboard module.
2. **Creating a List to Store Pressed Keys**:
   * An empty list named the\_keys is created to store each key pressed by the user during the runtime of the keylogger.
3. **Defining the functionPerKey Function**:
   * This function is triggered every time a key is pressed. It appends the pressed key to the the\_keys list and then calls another function, storeKeysToFile, to write the updated list of keys to a log file.
4. **Defining the storeKeysToFile Function**:
   * This function is responsible for writing the list of captured keys to a text file named keylog.txt. It opens the file in write mode ('w'), converts each key in the list to a string, and then writes it to the file, one key per line. The replace method is used to remove the quotation marks around the keys.
5. **Defining the onEachKeyRelease Function**:
   * This function is executed every time a key is released. It checks if the released key is the "Escape" key (Key.esc). If it is, the function returns False, which stops the listener and effectively ends the keylogging process.
6. **Starting the Listener**:
   * The Listener class from the pynput module is used to monitor the keyboard. The on\_press parameter is set to the functionPerKey function, and the on\_release parameter is set to the onEachKeyRelease function. The listener is started using the with statement to ensure it runs within the context, and the join method is called to keep the listener active until it is stopped.

#### **Output**

The output of the keylogger is stored in a text file named keylog.txt. This file contains a record of all the keys pressed during the execution of the program.

#### **Use Cases**

* **Security Monitoring**: Organizations might use keyloggers to monitor unauthorized use of computer systems.
* **Parental Control**: Parents can monitor their children's activities on a computer.
* **Personal Productivity**: Users might want to keep track of their typing patterns to improve productivity.

#### **Ethical Considerations**

It is essential to use keyloggers responsibly. They should only be deployed in environments where monitoring is legally permitted, such as on personal computers or within organizations where employees are aware and have consented to monitoring. Unauthorized use of keyloggers is illegal and unethical.

#### **Conclusion**

This project demonstrates how to create a basic keylogger using Python. The simplicity of the code makes it an excellent learning exercise for those interested in cybersecurity and ethical hacking. However, users must be mindful of the ethical and legal implications of deploying such a tool.

#### **Future Enhancements**

* **Encryption**: Implement encryption for the log file to protect the data.
* **Email Notifications**: Add functionality to send log files via email at regular intervals.
* **Stealth Mode**: Modify the code to run the keylogger in the background without the user’s knowledge (if legal).