Encrypted Keylogger Project Report

1. Introduction

This project is a demonstration of how keystroke logging, encryption, and network transmission can be combined to understand potential cybersecurity vulnerabilities. The keylogger silently captures all keyboard input from a user, encrypts this data using symmetric encryption (Fernet), and transmits it to a local server mimicking a remote attacker's endpoint. This is intended strictly for educational and ethical hacking simulations.

2. Abstract

The Encrypted Keylogger project showcases the process of intercepting and protecting sensitive data through encryption before it is transmitted. Built in Python, this project consists of a keylogging client that listens for keystrokes and a Flask-based server that accepts incoming logs. Encryption ensures that intercepted data remains unreadable without the secret key, simulating secure data handling. This project helps learners explore how malicious behavior works and how to prevent it through logging, monitoring, and encryption analysis.

3. Tools Used

- **Python 3.10+** – Core programming language
- **pynput** – To capture real-time keyboard input
- **cryptography (Fernet)** – For AES-based encryption
- **Flask** – To simulate a remote server
- **requests** – For sending HTTP POST requests
- **datetime & os** – For timestamping and file handling

4. Steps Involved in Building the Project

1. **Keylogger Implementation**
   Used pynput.keyboard.Listener to detect and record each keystroke.
2. **Kill Switch and Upload Trigger**
   - Pressing Esc stops the keylogger safely.
   - Pressing F12 encrypts the log file and sends it to the server.
3. **Encryption Mechanism**
   The cryptography module generates a Fernet key and uses it to encrypt the log file content.

4. **Server Creation**
   A lightweight Flask application handles POST requests at /upload and saves received files in an uploads/ directory.
5. **Testing & Execution**
   Verified the generation of keylogs.txt, its encryption to encrypted_log.txt, and successful reception at the server endpoint.

5. Conclusion

This project serves as a practical and ethical introduction to keylogging, encryption, and network communication in cybersecurity. It illustrates how attackers may leverage keyloggers and how defenders can use knowledge of such methods to enhance security systems. Although it demonstrates offensive techniques, it is crafted to highlight the importance of encryption, access control, and ethical responsibility. This project is an excellent tool for students, ethical hackers, and penetration testers to enhance their understanding of system vulnerabilities and protective mechanisms.