Encrypted Keylogger Project Report

1. Introduction

The Encrypted Keylogger project is a demonstration of how keylogging, encryption, and data exfiltration can be integrated in a controlled environment. The primary aim is to simulate how sensitive data can be captured, encrypted for security, and transmitted to a remote server for storage. This helps in understanding both offensive and defensive aspects of cybersecurity.

2. Abstract

This project logs keystrokes from the user's keyboard, encrypts them using the Fernet symmetric encryption method, and sends the encrypted logs to a simulated remote server built with Flask. The server receives these logs via a POST request and stores them in a designated folder. A kill switch (`Esc` key) is implemented to safely terminate the logger, and `F12` triggers encryption and upload of logs.

3. Tools Used

- Python 3
- pynput (for capturing keystrokes)
- cryptography (for Fernet encryption)
- Flask (to simulate a remote server)
- requests (for sending HTTP POST data)

4. Steps Involved in Building the Project

1. Implemented a keylogger using the pynput library.
2. Integrated Fernet encryption to secure logged data.
3. Created a Flask server to receive encrypted logs.
4. Added functionality to send encrypted logs via HTTP POST.
5. Incorporated a kill-switch and log-upload triggers using keyboard events.

5. Conclusion

The project demonstrates the integration of keystroke logging, encryption, and server communication in a secure, ethical setting. It provides insights into data security, system vulnerabilities, and ethical hacking practices, while emphasizing responsible usage for learning and cybersecurity awareness.