🛡️ **Pinnacle Labs Cybersecurity Internship – Task 2 Report**

Intern Name: Abin Shaji Thomas
Institution: Karunya Institute of Technology and Sciences, Coimbatore
Track: Cybersecurity
Project Title: Stealth Keylogger with Encrypted Email Reporting
Task Number: 2
Submission Date: 27 May 2025

Project Overview

This project focuses on the development of a **Python-based stealth keylogger** capable of logging keystrokes and securely emailing the collected logs at regular intervals. It is designed with ethical usage in mind and built to simulate real-world cyber investigation tools.

The objective of this task was to explore the offensive side of cybersecurity by understanding how keylogging works, how such tools are deployed, and more importantly, how to protect systems against them.

Objectives

- Capture and store every keystroke typed on the system.
- Stealthily run in the background without user detection.
- Automatically send the logged keystrokes to a predefined email address in .txt format.
- Secure the credentials using a .env file to avoid hardcoding.
- Learn the potential risks and reinforce the importance of endpoint security.

Technologies Used

Component	Technology
Programming Language	Python 3.12
Email Service	Gmail (App Password Authentication)
Keystroke Capture	pynput Library
Mail Sending	smtplib, email.message
Environment Management	python-dotenv

Component	Technology
Execution OS	Windows 10/11

Implementation Details

- The **pynput** library was used to monitor and log all keystrokes to a temporary .txt file.
- The **mail.py** module securely reads credentials from the .env file and uses smtplib to send the logs.
- A scheduler sends the log file as an email attachment at a fixed time interval.
- The script runs in the background without opening any windows or prompts, ensuring stealth operation.
- The code was thoroughly tested and debugged in **Visual Studio Code**.

Security Measures

- All email credentials are stored in a separate .env file to ensure they are not exposed in the codebase.
- Used **Google App Passwords** to safely authenticate email-sending logic.
- Implemented structured error handling to catch failed email delivery attempts.
- The keylogger is only for **educational and awareness** purposes. It is not intended for unauthorized surveillance.

Testing Summary

Test Scenario	Result
Script runs without user detection	✅ Success
Keystrokes logged accurately	✅ Success
Email with attachment sent correctly	✅ Success
.env credentials not exposed	✅ Verified
Script safely terminable via VS Code	✅ Tested

Learning Outcome

This task helped me deeply understand the **mechanics of keyloggers**, how cybercriminals exploit them, and more importantly, how to **prevent and detect** such threats. It also gave me practical experience in:

- Stealth script execution
- Email automation and security
- Managing credentials securely
- Ethical hacking boundaries and defense strategies

This project enhanced both my technical skills and cybersecurity mindset.

Declaration

This project was developed independently by **Abin Shaji Thomas** as part of the Pinnacle Labs Cybersecurity Internship. It is intended **strictly for educational use** to promote awareness about system security and ethical hacking.