⍰ Keylogger with Encrypted Data Exfiltration (PoC)

⍰ Introduction

This project demonstrates a PoC keylogger built with Python, which captures keystrokes, encrypts them, and simulates data exfiltration by writing encrypted data to a local file.

⍰ Components

- keylogger.py – Captures and logs keystrokes.
- encryptor.py – Encrypts logs using Fernet (AES).
- exfiltrate.py – Simulates sending logs to a remote server.
- decryptor.py – Decrypts the encoded logs.

⍰ How to Run

1. Install Required Libraries:

```
pip install pynput cryptography
```

2. Run keylogger:

```
python keylogger.py (Press ESC to stop)
```

3. View encrypted logs in: logs/exfiltrated_data.txt

4. Decrypt logs using:

```
python decryptor.py
```

⍰ Log Files

- logs/keystrokes.log – Temporarily stores raw keystrokes.
- logs/exfiltrated_data.txt – Stores encrypted logs.

⍰ Disclaimer

This tool is for educational use only. Unauthorized keylogging is illegal and unethical.