Course Name:	**Information and Cyber Security Laboratory**	**Semester:**	**VII**
Date of Performance:	**01 / 10 / 2025**	**Batch No:**	**B - 1**
Faculty Name:	**Prof. Makrand Kulkarni**	**Roll No:**	**16014022050**
Faculty Sign & Date:		**Grade/Marks:**	**___ / 25**

Experiment No: 7

Title: To perform 'Keylogger' using VS code

Aim and Objective of the Experiment:

To perform 'Keylogger' using VS code.

COs to be achieved:

CO3: Comprehend concept of cyber-crime, threats, security, cyber offenses and methods used in cybercrime.

Books/Journals/Websites referred:

Using Microsoft Store install the following :

1. VS Code IDE Tool
2. Python 3.13

Tools required:

VS code IDE tool and Python code

Theory:

A **keylogger** is either **software-based** or **hardware-based**. Its main job is to secretly monitor and log keystrokes without the user's knowledge. The collected data is then stored locally or transmitted to a remote attacker.

Types of Keyloggers:

1. **Software Keyloggers**
   - Installed on the target computer, often disguised as legitimate software or hidden inside malware.
   - Operate at different levels:
     - **API-based** → Capture keystrokes by monitoring keyboard APIs.
     - **Kernel-based** → Installed in the operating system kernel for deeper control.
     - **Form grabbers** → Capture text entered into web forms before it's encrypted.
   - Can also take screenshots and record application usage.

2. **Hardware Keyloggers**
    - Physical devices placed between the keyboard and the computer (like USB devices).
    - Small and hidden, making them hard to detect.
    - They store keystrokes in internal memory, which can later be retrieved by the attacker.
    - Example: USB keylogger, wireless keyboard sniffer.

Not all keyloggers are illegal. They can be used for:

- **Parental control**: Monitoring children's online activities.
- **Employee monitoring**: Ensuring workplace productivity (with permission).
- **Law enforcement**: Tracking suspects in cybercrime investigations.
- **Personal backup**: Some people use them to keep track of what they type.

Implementation details:

1. Using Microsoft Store install the following:
    - VS Code IDE Tool
    - Python 3.13
2. Open 'Keylogger' folder in VS code IDE tool.
3. Go to 'View' tab and open the 'Terminal'
4. Open 'README.md' file
5. To Set Up Virtual Environment copy : python -m venv env and paste in terminal and press Enter key
6. To install the required dependencies: copy: pip install -r requirements.txt and paste in terminal and press Enter key.
7. To start logging keystrokes, run: python keylogger.py and paste in terminal and press Enter key.
8. It will open GUI. Press START key on GUI.
9. Write text on any of the .doc or .txt file and then press STOP key of GUI.
10. Check the output on : out----'key_log.txt'
11. Take the screenshots of each step and share in the writeup.

Output / Screenshots:

Create a Python virtual environment:

```
PS C:\Users\Admin\Desktop\keylogger> python -m venv env
>>
PS C:\Users\Admin\Desktop\keylogger>
```

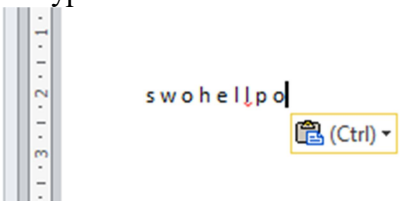
Installing Requirements:

```
PS C:\Users\Admin\Desktop\keylogger> pip install -r requirements.txt
>>
Requirement already satisfied: pynput in c:\users\admin\appdata\local\programs\python\python37\lib\site-packages (from -r requirements.txt (l
ine 1)) (1.8.1)
Requirement already satisfied: six in c:\users\admin\appdata\local\programs\python\python37\lib\site-packages (from pynput->-r requirements.t
xt (line 1)) (1.16.0)
You are using pip version 10.0.1, however version 24.0 is available.
You should consider upgrading via the 'python -m pip install --upgrade pip' command.
PS C:\Users\Admin\Desktop\keylogger>
```

Running code:

```
PS C:\Users\Admin\Desktop\keylogger> python keylogger.py
```

Text typed on word:



Keylogger Output:

keylogger.log

out > keylogger.log

```
2025-09-25 14:52:44,555 - INFO - Keylogger started.
2025-09-25 14:52:49,331 - INFO - Key pressed: [CMD]
2025-09-25 14:52:49,620 - INFO - Key pressed: s
2025-09-25 14:52:49,714 - INFO - Key released: [CMD]
2025-09-25 14:52:49,802 - INFO - Key released: s
2025-09-25 14:52:49,971 - INFO - Key pressed: w
2025-09-25 14:52:50,138 - INFO - Key released: w
2025-09-25 14:52:50,547 - INFO - Key pressed: o
2025-09-25 14:52:50,691 - INFO - Key released: o
2025-09-25 14:52:57,063 - INFO - Key pressed: h
2025-09-25 14:52:57,221 - INFO - Key released: h
2025-09-25 14:52:57,236 - INFO - Key pressed: e
2025-09-25 14:52:57,389 - INFO - Key released: e
2025-09-25 14:52:57,397 - INFO - Key pressed: l
2025-09-25 14:52:57,516 - INFO - Key released: l
2025-09-25 14:52:57,581 - INFO - Key pressed: l
2025-09-25 14:52:57,692 - INFO - Key released: l
2025-09-25 14:52:57,790 - INFO - Key pressed: p
2025-09-25 14:52:57,797 - INFO - Key pressed: o
2025-09-25 14:52:57,925 - INFO - Key released: o
2025-09-25 14:52:57,943 - INFO - Key pressed:
2025-09-25 14:52:57,948 - INFO - Key released: p
2025-09-25 14:52:58,141 - INFO - Key released:
2025-09-25 14:52:58,259 - INFO - Key pressed: [BACKSPACE]
2025-09-25 14:52:58,371 - INFO - Key released: [BACKSPACE]
2025-09-25 14:52:58,477 - INFO - Key pressed: [BACKSPACE]
2025-09-25 14:52:58,564 - INFO - Key released: [BACKSPACE]
2025-09-25 14:53:39,430 - INFO - Key pressed: [ALT]
2025-09-25 14:53:39,548 - INFO - Key pressed:
2025-09-25 14:53:39,694 - INFO - Key released: [ALT]
2025-09-25 14:53:39,772 - INFO - Key released:
2025-09-25 14:53:40,324 - INFO - Key pressed: [ALT]
```

Post Lab Subjective/Objective type Questions:

1. **What preventive measures can users take to protect themselves from keylogger attacks?**
   - Use reputable antivirus/anti-malware software and keep signatures updated.
   - Only install software from trusted sources and verify digital signatures.
   - Keep OS and applications patched and up to date.
   - Use an on-screen virtual keyboard for entering highly sensitive information (where supported).
   - Use two-factor authentication (2FA) so credentials alone are not sufficient.
   - Use a password manager (it can autofill rather than typing passwords).
   - Avoid running untrusted scripts, and use least-privilege accounts (don't run as admin/root unless necessary).
   - Monitor for unusual processes and startup entries; check installed programs regularly.
   - Employ endpoint protection solutions and application whitelisting in corporate environments.
   - Encrypt sensitive data at rest and in transit.

2. **Mention two signs that may indicate a keylogger infection on a computer.**
   - Unexplained CPU usage or unknown background processes running while you're idle.
   - Unexpected delays when typing, or text appearing in files that you didn't create; or presence of unknown files (like key_log.txt) or unknown programs starting at boot.

     (Other possible signs: frequent crashes, strange network connections from unknown processes — investigate carefully.)

Conclusion:

In this experiment we explored what a keylogger is and performed a controlled demonstration inside an isolated virtual environment. The keylogger successfully recorded typed characters into key_log.txt while the GUI was running. The lab highlighted the privacy and security risks of keyloggers and reinforced the importance of safe computing practices.

Signature of faculty in-charge with Date: