Task # 2 Key Logging Simulation

Contents

Keystroke Logging Simulation

1. Introduction

Keylogging is the process of recording keystrokes entered by a user via a keyboard. Although keyloggers are commonly linked with malicious cyberattacks, understanding their working mechanism is important for cybersecurity professionals in order to detect, prevent, and mitigate such threats. This project focuses on simulating a **basic keylogger in a controlled and ethical environment** for learning and awareness purposes only.

---

2. Objective of the Project

The main objectives of this project are:

- To understand how keystroke logging works at a basic level
- To simulate keystroke capture using a simple script
- To log captured input locally into a file
- To analyze the potential security and privacy risks of keylogging attacks
- To promote defensive and ethical cybersecurity practices

---

3. Scope and Ethical Considerations

This project was conducted strictly under the following conditions:

- The simulation was performed on the author's **personal local machine**
- Only **user-consented input** was captured
- No background, hidden, or system-wide keylogging was implemented
- No real credentials, passwords, or sensitive data were collected

Ethical Statement:

This project was performed solely for educational purposes in a controlled environment with full user consent. No malicious activity was involved.

---

4. Tools and Technologies Used

- **Programming Language:** Python
- **Operating Environment:** Local machine
- **File System:** Local text file for logging

---

5. Methodology

The project follows a simple and transparent methodology:

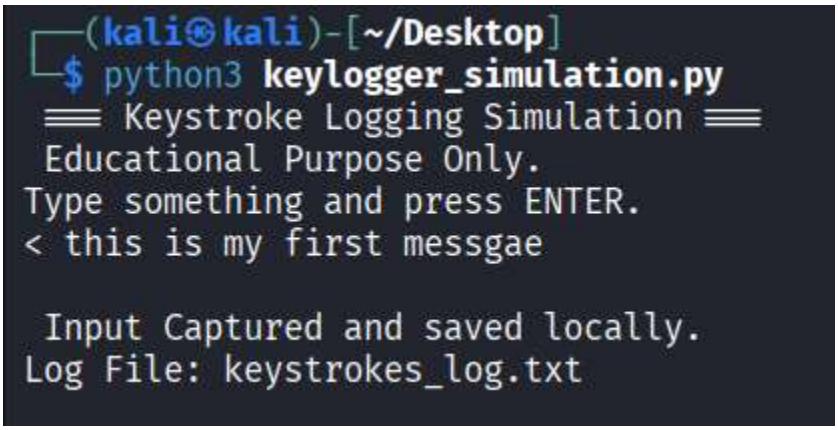
1. Display a clear message informing the user about the simulation
2. Accept keyboard input from the user
3. Capture the entered text using a Python script
4. Store the captured input into a local text file
5. Review the log file to understand how keystroke data can be recorded

---

6. Code Implementation:

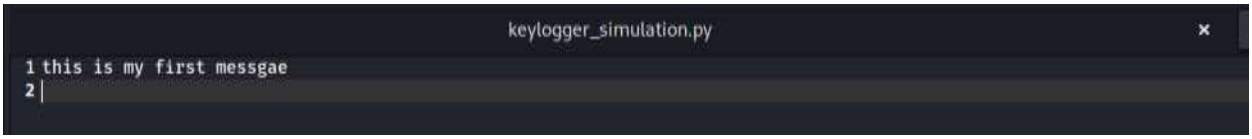
```python
#Keystroke Logging Simulation
#Purpose: Security awareness & learning
#Environment: Local Machine, user consent

log_file="keystrokes_log.txt"
print(" ≡≡≡ Keystroke Logging Simulation ≡≡≡")
print("Type something and press ENTER.")
user_input=input("< ")
with open(log_file,"a") as file:
    file.write(user_input + "\n")

print("\n Input Captured and saved locally.")
print(f"Log File: {log_file}")

```

7. Sample Output



---

8. Log File Output



---

6. Implementation Overview

A Python script was developed to simulate keystroke logging. The script uses Python's built-in input() function to capture user keystrokes entered intentionally during a typing prompt. The captured input is then written to a local text file using file-handling techniques.

This approach demonstrates the **core principle behind keylogging** without implementing any malicious or hidden behavior.

---

7. Observations and Results

- User input was successfully captured when typed into the program
- The input was stored line-by-line in a local log file
- The logging process occurred transparently with user awareness

These observations confirm that keystroke data can be captured at the software level before encryption or network transmission.

8. Risk Analysis

If keylogging techniques are misused, they can pose serious security risks:

- Theft of usernames and passwords
- Exposure of banking and financial information
- Violation of user privacy
- Identity theft and account compromise
- Corporate data leakage

Keyloggers are especially dangerous because they can capture sensitive data **before encryption is applied**.

---

9. Defensive Measures and Prevention

To protect against malicious keylogging attacks, the following measures are recommended:

- Use updated antivirus and endpoint protection solutions
- Apply the principle of least privilege
- Enable multi-factor authentication (MFA)
- Use secure and trusted software only
- Monitor system processes and application behavior
- Keep operating systems and applications up to date

---

10. Conclusion

This project successfully demonstrates a basic keystroke logging simulation in a safe and controlled environment. By understanding how keystrokes can be captured and logged, security professionals can better assess the risks associated with keylogging attacks and implement effective defensive strategies. The project reinforces the importance of ethical cybersecurity practices and user awareness.

---

11. Learning Outcomes

- Understanding of basic keylogging concepts
- Practical experience with Python input and file handling
- Awareness of real-world cybersecurity threats
- Ability to analyze and explain security risks and defenses

Project Type: Educational / Security Awareness
Author: Muhammad Anus Naseer Taimoori
Date: 9th January 2026