Faculty of Engineering
Cairo University

Cyber Security Project Report

Keyractor

Name	Code
Ahmed Osama Zahran	9210026
Yousef Mohamed Haggag	9211436
Abdelrahman Abdelfattah	9210587
Mohamed Adel	9211006

Under Supervision of:
Eng: Ayman Reda

Keylogger and Password Extractor

Introduction

The Keylogger and Password Extractor is a project designed to monitor and record keystrokes on a target system. Additionally, it uses pattern matching technique as regex to extract potential passwords from the logged keystrokes.

Features

a. Keylogging: The project captures keystrokes made by the user on the target system and logs them into a log file.
b. Password Extraction: The project includes a pattern matching technique that analyzes the logged keystrokes to identify potential passwords.
c. Anti-Malware: A scanner to scan for malicious patterns of a keylogger and warn the client of suspected malware.

System Requirements

-Python: Version 3.6 or higher
-Additional Python packages: pynput, pyperclip, pywin32

Usage

a. Running the Keylogger:
I. Open a command prompt or terminal and navigate to the project directory.
II. Execute the following command:
python keylogger.py

b. Monitoring Keystrokes:
The keylogger will start monitoring and logging keystrokes as soon as the program is executed. The logged keystrokes will be saved in a text file named "sus.log" in the project directory.

c. Sending the log file to the attacker:
I. use reverse SSH connection to send the log file to the attacker.
II. send background emails to the attacker with the log file as an attachment.

d. Extracting Passwords:

I. Once we have captured a sufficient amount of data in the "sus.log" file, stop the keylogger by pressing the 'Esc' key or terminating the program.

II. Execute the following command to extract potential passwords from the logged keystrokes:

python password_extractor.py

III. The potential passwords identified by the algorithm will be displayed in the console output.

Security and Legal Considerations

I. Ethical Usage: It is crucial to use this project responsibly and legally. We ensured that we had the proper authorization to monitor keystrokes and only use it on systems we own or have explicit permission to access.

II. Privacy and Data Protection: Respecting privacy rights and handling any collected data in compliance with applicable laws and regulations.

III. Antivirus Considerations: Some antivirus programs may flag keyloggers as malicious software. So, we aim (dreams may come true¯_(ツ)_/¯) to bypass at least windows defender.

Conclusion

The Keylogger and Password Extractor project provides a powerful tool for monitoring and extracting potential passwords from logged keystrokes. By following this documentation, you can install, configure, and utilize the project effectively while maintaining ethical and legal standards. Remember to always use this tool responsibly and respect privacy rights.