Password Strength Analyzer with Custom Wordlist Generator

Introduction

This project aims to provide a simple yet effective tool to analyze the strength of user-provided passwords and generate custom wordlists based on personal data inputs. These wordlists can be used for ethical hacking and cybersecurity training purposes.

Abstract

The tool evaluates passwords using the zxcvbn library, which estimates password strength based on common patterns, dictionary words, and entropy. Additionally, it collects personal inputs such as name, date of birth, or pet names, and creates a tailored wordlist that could be used in password cracking simulations. This enhances the understanding of how predictable passwords can be and promotes the use of stronger, more secure passwords.

Tools Used

- Python
- zxcvbn-python
- argparse (optional)
- tkinter (optional)
- Basic text processing libraries

Steps Involved in Building the Project

1. Accept user input for password and personal info.
2. Analyze password using zxcvbn to determine strength.
3. Generate wordlist by combining personal data with patterns (e.g., leetspeak, years).
4. Export the generated wordlist into a .txt file.
5. (Optional) Create a GUI for easier input using tkinter.

Conclusion

The Password Strength Analyzer and Custom Wordlist Generator demonstrates how attackers may exploit weak or predictable passwords. It also emphasizes the importance of secure password practices. The project serves as an excellent educational tool for beginners in ethical hacking and cybersecurity.