Title: Password Strength Analyzer with Custom Wordlist Generator

1. Introduction

With the increasing use of online services, securing user accounts with strong passwords has become critical. Weak passwords are easy targets for brute-force and dictionary attacks. This project aims to develop a tool that not only evaluates password strength but also generates custom wordlists for security testing and analysis.

2. Abstract

This Python-based GUI tool allows users to input a password, analyze its strength using the zxcvbn library, and generate a custom wordlist based on personal details like name, pet name, year of birth, and hobby. It includes leetspeak variations, appends numbers, and creates useful combinations for use in penetration testing or security awareness. The final product is a user-friendly
`.exe` application built using PyInstaller.

3. Tools Used

- Python 3
- Tkinter (for GUI)
- zxcvbn (password strength estimator)
- PyInstaller (for generating .exe file)
- Basic string manipulation and file handling

4. Steps Involved in Building the Project

- Designed GUI using Tkinter for user input and interaction.
- Integrated zxcvbn to assess password strength and provide feedback.
- Collected user inputs (name, pet, year, hobby) for wordlist generation.
- Programmatically created multiple wordlist combinations (e.g., appending numbers, leetspeak).

- Saved the generated wordlist in `.txt` format.
- Converted the Python script to a standalone `.exe` using PyInstaller.

5. Conclusion

The tool is helpful for understanding password strength and generating personalized wordlists for ethical hacking and security testing. It provides an easy-to-use interface and demonstrates key cybersecurity principles such as password entropy and attack simulation through wordlists.