Project: Password Strength Analyzer with Custom Wordlist Generator

Introduction

In cybersecurity, password security is a critical factor in protecting digital identities. Weak passwords can be easily cracked by attackers using dictionary and brute-force attacks. This project aims to analyze password strength and generate custom wordlists that help simulate real-world password cracking scenarios for ethical hacking and security assessments.

Abstract

The Password Strength Analyzer evaluates passwords using the zxcvbn library, providing estimates for cracking times and strength scores. The tool also generates custom wordlists based on personal user data like names, hobbies, or years, including leetspeak variations. Such tools are useful for penetration testers to assess password vulnerabilities and educate users about strong password practices.

Tools Used

- python
- zxcvbn library
- argparse
- itertools

Steps Involved

1. Accept password from user via command line.
2. Analyze password strength using zxcvbn.
3. Accept personal words to generate a wordlist.
4. Create leetspeak variations and combine with years.
5. Export custom wordlist to a text file.

Conclusion

The Password Strength Analyzer and Wordlist Generator provides insights into how easily a password might be cracked and emphasizes the importance of strong, unique passwords. It also equips ethical hackers with targeted wordlists for controlled penetration testing, promoting better cybersecurity practices.