Password Strength Analyzer and Custom Wordlist Generator

Introduction

Passwords remain the first line of defense for most digital systems. Weak or predictable passwords are one of the primary causes of security breaches. Attackers often exploit personal information such as names, dates, and common patterns to guess passwords.
This project focuses on analyzing password strength and generating customized wordlists based on user-provided data. The tool helps users understand how secure their passwords are and demonstrates how attackers may construct targeted password lists.

Abstract

This project implements a Python-based Password Strength Analyzer and Custom Wordlist Generator. The system evaluates password strength using the zxcvbn library and entropy-based calculations. It also generates attack-specific wordlists by combining personal inputs, leetspeak substitutions, separators, and year patterns. The tool supports both Command Line Interface (CLI) and Graphical User Interface (GUI) using Tkinter. The generated wordlists are exported in .txt format and are compatible with standard password auditing tools.

Tools Used

- **Python** – Core programming language
- **zxcvbn** – Password strength estimation
- **NLTK** – Tokenization and lemmatization
- **argparse** – Command-line argument handling
- **Tkinter** – Graphical user interface
- **reportlab** – PDF report generation

Steps Involved in Building the Project

1. Designed a password strength evaluation system using zxcvbn with a fallback entropy-based heuristic.
2. Implemented Shannon entropy calculation to estimate randomness.
3. Collected user-specific inputs such as names, pets, and dates.
4. Generated wordlist variations using:
    - Case transformations
    - Leetspeak substitutions
    - Year suffixes and prefixes
    - Token separators
5. Removed duplicate entries and limited output size for efficiency.
6. Added CLI support using argparse.
7. Developed a Tkinter-based GUI for ease of use.
8. Enabled exporting wordlists in .txt format for security testing.
9. Tested the tool with multiple inputs to validate correctness.

Conclusion

The Password Strength Analyzer and Custom Wordlist Generator successfully demonstrates how password security can be evaluated and how targeted wordlists are created. The project highlights the importance of strong, unpredictable passwords and shows how personal data can weaken security if misused.

This tool can be used for educational purposes, security awareness, and ethical password auditing. Future enhancements may include hash-based attacks, rule engines, and advanced mutation strategies.