■ Password Strength Analyzer & Custom Wordlist Generator

Abstract

This project focuses on building a security tool that can both evaluate the strength of user passwords and generate custom attack-specific wordlists. The primary aim was to improve awareness of password security while understanding how attackers may attempt to crack weak or predictable passwords. The project uses Python libraries such as zxcvbn for strength analysis and custom algorithms to expand potential wordlists based on user data.

Introduction

Passwords are the first line of defense in digital security, yet weak or guessable passwords remain one of the most common causes of account compromises. This project addresses the problem by creating a tool that not only evaluates password strength but also simulates how attackers generate custom wordlists. By doing so, the project helps raise awareness of best practices in creating stronger passwords and demonstrates the importance of defensive security.

Tools Used

The following tools and technologies were used: - **Python**: Core language for development. - **zxcvbn**: Password strength estimation library. - **NLTK**: Natural language toolkit for tokenizing user hints (optional). - **argparse**: Command-line argument handling. - **Tkinter**: GUI implementation for non-CLI users.

Steps Involved in Building the Project

1. **Requirement Analysis:** Defined project objectives to analyze password strength and generate custom wordlists.
2. **Implementation of Strength Analyzer:** Integrated zxcvbn and custom entropy-based calculations.
3. **Wordlist Generator:** Built logic to expand user-provided hints into attack-specific wordlists using leetspeak, case variants, dates, years, and suffixes.
4. **CLI and GUI Interface:** Designed a dual interface so users can choose between command-line or graphical interaction.
5. **Testing & Export:** Generated wordlists and validated strength analysis across sample passwords.

Conclusion

The project successfully demonstrated the process of analyzing password strength and creating targeted wordlists. This exercise highlights the importance of using strong, unpredictable passwords and shows how personal information can make passwords vulnerable to attacks. The tool can be used in cybersecurity training and awareness programs, ensuring users adopt safer password practices.