Password Strength Analyzer & Custom Wordlist Generator

Created by Sridhar S

Introduction

With the increasing reliance on digital platforms, password security has become a critical aspect of personal and organizational safety. Weak or predictable passwords are a leading cause of security breaches. This project addresses these challenges by providing a cross-platform Python application that not only evaluates password strength but also generates custom wordlists for security testing and awareness.

Abstract

The Password Strength Analyzer & Custom Wordlist Generator is a user-friendly, cross-platform desktop application built with Python and Tkinter. It enables users to assess the strength of their passwords using advanced algorithms and industry standards, providing real-time feedback and actionable suggestions for improvement. Additionally, it allows for the creation of targeted password wordlists based on personal clues, which can be used for penetration testing or educational demonstrations of password vulnerabilities. The tool is designed for security professionals, educators, and end-users to promote better password practices and awareness of potential attack vectors.

Tools Used

- **Programming Language:** Python 3.8+
- **GUI Framework:** Tkinter
- **Password Strength Library:** zxcvbn (for advanced password analysis)
- **Natural Language Processing:** nltk (for wordlist manipulation)
- **Operating Systems Supported:** Windows 10, Ubuntu 22.04
- **Other Tools:** Python venv for environment management, pip for dependency installation

---

Steps Involved in Building the Project

1. **Requirements Analysis:**
   Identified the need for a tool that combines password strength analysis with custom wordlist generation for security testing and awareness.
2. **Environment Setup:**
   Configured Python virtual environments and installed required libraries (zxcvbn, nltk, tkinter).
3. **Password Analyzer Module:**
   Developed a module integrating zxcvbn for robust password evaluation, including entropy fallback and real-time feedback mechanisms.
4. **Wordlist Generator Module:**
   Implemented logic to generate wordlists using personal information, custom words, leetspeak, case variations, year appendages, and common prefixes/suffixes.

5. **Graphical User Interface:**
   Designed a two-tab Tkinter GUI for seamless navigation between password analysis and wordlist generation, with real-time previews and progress indicators.
6. **Testing and Refinement:**
   Conducted cross-platform testing on Windows and Ubuntu, optimized performance, and enhanced user experience with tooltips and feedback.
7. **Documentation and Packaging:**
   Prepared user guides, installation scripts, and ensured the application could be easily installed and used by non-technical users.

Conclusion

The Password Strength Analyzer & Custom Wordlist Generator successfully bridges the gap between password security education and practical security testing. By combining advanced password analysis with customizable wordlist generation in an accessible GUI, the tool empowers users to understand and improve their password practices while providing security professionals with a valuable resource for penetration testing and awareness campaigns. The project demonstrates the effectiveness of open-source tools in enhancing digital security and user awareness.

Security Note:
This tool is intended for legitimate security testing and educational purposes only. Users must ensure they have proper authorization before using it to test or generate wordlists for any system.