PassDefender ToolKit: Password Strength Analyzer & Custom Wordlist Generator

Abstract **-Navya Nandika A**

PassDefender ToolKit is a cybersecurity application for analyzing password strength and generating custom wordlists for security audits and penetration testing. Built using Python and tkinter, it leverages the zxcvbn library for advanced password analysis and uses combinatorial techniques (case, leetspeak, permutations) for wordlist generation. Its dark-themed GUI provides real-time feedback and interactive previews for both educational and professional use.

Introduction

Passwords are a frequent vulnerability in cybersecurity. Users often choose weak, guessable passwords, while security pros need targeted wordlists for ethical hacking. PassDefender ToolKit bridges this gap with real-time strength analysis and custom wordlist generation, enhancing both awareness and practical assessment.

Objectives:

- Give users actionable password feedback using entropy/scoring
- Enable custom wordlist generation from personal info
- Use advanced patterns: leetspeak, case, permutations
- GUI for usability and clarity
- Export lists for tools like hashcat or John the Ripper

Tools Used

Component	Technology	Purpose
GUI Framework	tkinter	Cross-platform interface
Password Analysis	zxcvbn	Entropy & pattern detection
Core Language	Python 3.x	Logic and algorithms
Wordlist Generation	itertools	Combos and transformations
Data Export	file I/O	.txt output for cracking tools

Dependencies: pip install zxcvbn

Steps Involved in Building the Project

Phase 1: Password Analyzer

- Integrated zxcvbn for entropy and issue scoring
- Added length, common-word, character-type checks
- Scoring (0-4), feedback, crack-time estimates
- Show/hide password toggle in GUI

Phase 2: Wordlist Generator

- User fields: Name, Pet/Nickname, Birth Year, Place, Number
- Generation patterns: base, suffix, special chars, case, leet, reverse, combos
- Real-time, scrollable preview of all combinations
- Export and save using file dialog

Phase 3: UI/UX Design

- Dark theme (purple, neon green, blue)
- Monospace fonts for hacker/terminal effect
- Two main frames: Password, Wordlist
- Scrollable preview area
- Error handling with friendly notifications

Phase 4: Testing & Refinement

- Tested analyzer with various passwords and edge cases
- Checked wordlist output accuracy/compatibility
- Verified export to .txt and tool compatibility
- UI optimized for short/wide screen and visibility

Conclusion

PassDefender ToolKit combines password analysis and custom wordlist automation in one educational, hacker-friendly GUI. Designed for both cybersecurity students and professionals, it enables better security practices and supports ethical testing workflows.

Possible Future Enhancements:

- NLTK integration for word variations
- CLI mode for batch jobs
- Custom dictionary merging
- User-defined rules & Password breach database lookup