Titile: Password Strength Analyzer with Custom Wordlist Generator

Presented by **Hemanth S**

Introduction

In today's digital era, password security is paramount. Weak passwords remain one of the most exploited vulnerabilities in cyber attacks. This project presents a Python-based desktop tool designed to evaluate password strength and generate custom wordlists based on user data. It serves as both a personal security assistant and an educational resource for cybersecurity learners.

Abstract

The tool integrates password strength analysis using the zxcvbn library and generates personalized wordlists by applying transformation patterns such as leetspeak, common suffixes, and capitalizations. The goal is to help users understand password vulnerabilities and create better defenses. The wordlists can be exported for use in ethical hacking and penetration testing scenarios.

Tools Used

- Python
- argparse
- NLTK
- zxcvbn
- Tkinter

Steps Involved in Building the Project

a Analyze user password using zxcvbn

b Allow user inputs (name, date, pet) to generate a custom wordlist.

c Include common patterns like leetspeak, append years.

d Export in .txt format for cracking tools.

e Add GUI with Tkinter

Conclusion

This project successfully merges usability and cybersecurity insights, enabling users to evaluate and improve their password security. The customizable wordlist generation feature emphasizes how personal information can be misused in password attacks, reinforcing the need for strong, unpredictable passwords. The tool acts as both a preventive and educational resource in the field of cybersecurity.