Password Strength Analyzer with Custom Wordlist Generator

Name: Athul P

Internship: Cybersecurity Research Intern – Elevate Labs

Duration: July 2025

Introduction

In today's Cybersecurity landscape, weak and predictable passwords remain one of the most exploited vulnerabilities. This project, "Password Strength Analyzer with Custom Word list Generator," is designed to assist both users and Cybersecurity analysts in evaluating password strength and generating targeted word lists for password auditing and penetration testing.

Abstract

This Python-based tool performs two core functions:
1. Password Strength Analysis: Uses the zxcvbn-python algorithm to estimate how long it would take an attacker to crack a password.
2. Custom Wordlist Generation: Based on user inputs (like name, year, etc.), it generates a .txt wordlist using common real-world patterns such as leetspeak and date combinations.
It is designed as a command-line tool and outputs a text file compatible with password auditing tools. This tool helps simulate realistic password cracking scenarios while promoting stronger password practices.

Tools Used

- Language: Python 3
- Libraries:
  - zxcvbn-python – For password strength estimation
  - argparse, itertools, datetime, string – For CLI handling and wordlist logic

Steps Involved

1. Installed Python 3 and required libraries using pip.
2. Built the CLI structure with two commands: analyze and generate.
3. Implemented password analysis using the zxcvbn algorithm.
4. Developed logic for generating wordlist permutations:
   - Leetspeak substitutions

- Capitalization variations
- Year additions (e.g., 2001, 2025)
- Word merges (e.g., athul2001)

5. Saved the wordlist to a .txt file for use in tools like Hydra or John the Ripper.
6. Verified outputs using multiple passwords and keyword combinations.

Conclusion

This project successfully demonstrates the creation of a practical CLI cybersecurity utility. It supports both defensive (awareness) and offensive (testing) learning. It’s modular, extendable, and usable in training labs and beginner pentesting environments. A GUI version or real-time password leak check could be future enhancements.