Password Strength Analyzer & Custom Wordlist Generator

Introduction

This project focuses on building a lightweight and portable password strength analyzer combined with a custom wordlist generator. Designed especially for Kali Linux, it avoids external libraries and emphasizes user-driven wordlist creation for use in penetration testing.

Abstract

The tool evaluates the strength of a password using basic heuristics like length and complexity (uppercase, lowercase, digits, symbols). It also takes personal user input like names, dates, and pet names to generate a custom wordlist with variations such as leetspeak and year-based combinations. This allows security professionals to simulate real-world password guessing scenarios effectively.

Tools Used

- Python 3
- Built-in libraries: argparse, datetime, re
- Kali Linux environment
- No external Python libraries required

Steps Involved in Building the Project

1. Created a Python script using built-in modules only.

2. Developed a simple password strength checker (based on length and complexity).

3. Implemented custom wordlist generation using user inputs like name, pet, and date.

4. Generated leetspeak variations and year combinations.

5. Exported the wordlist in a .txt format.

6. Built a CLI interface for easy usage on terminal-based systems.

Conclusion

This project delivers a handy and efficient tool for beginners and cybersecurity enthusiasts to assess password strength and create targeted wordlists. Its lightweight design and CLI interface make it perfect for Kali Linux environments, especially in training or Capture The Flag (CTF) competitions.