Password Strength Analyzer with Custom Wordlist Generator

Cybersecurity Project Report

september 9,2025

Introduction

This project develops a cybersecurity tool for password analysis and custom wordlist generation. Implemented in Python with a Kali Linux-themed interface, it helps users evaluate password strength and create targeted wordlists for security testing purposes.

Abstract

The tool combines password entropy analysis with personalized wordlist generation capabilities. It features both GUI and CLI interfaces, making it suitable for various cybersecurity scenarios. The application assesses password strength using mathematical entropy calculations while generating custom wordlists based on personal information with common password patterns.

Tools Used

- **Programming Language**: Python 3
- **GUI Framework**: Tkinter
- **Platform**: Kali Linux
- **Key Libraries**: math, datetime, os, argparse

Steps in Building the Project

1. Environment Setup

Verified Python 3 and Tkinter functionality on Kali Linux. Established proper display environment for GUI applications.

2. Core Functionality Development

- **Password Analyzer**: Implemented entropy calculation based on character set diversity
- **Wordlist Generator**: Created pattern-based generation with leetspeak substitutions
- **Common Patterns**: Added year appending (1970-current) and special character variations

3. User Interface Implementation

- Developed tabbed interface for dual functionality
- Applied Kali Linux color scheme for authentic appearance
- Added real-time feedback and export capabilities

4. Testing and Validation

- Verified password strength analysis with various inputs
- Tested wordlist generation with multiple data combinations
- Validated file export functionality

Key Features

1. **Password Analysis**: Entropy-based security evaluation with detailed feedback
2. **Wordlist Generation**: Creates personalized wordlists using common patterns
3. **Dual Interface**: Both GUI and command-line access
4. **Export Functionality**: Saves wordlists in TXT format for security tools

Conclusion

The project successfully demonstrates practical password security principles and offensive security techniques. The tool provides valuable insights into password vulnerability while offering practical wordlist generation for security assessments. Its implementation on Kali Linux ensures compatibility with standard penetration testing environments, making it suitable for educational purposes and authorized security testing.

This tool is intended for educational purposes and authorized security testing only. Always ensure proper authorization before using security assessment tools.