Password Strength Analyzer + Custom Wordlist Generator

CLI Mode — Summary Report

Overview:

The Command-Line Interface (CLI) mode provides a structured way to use the Password Strength Analyzer and Custom Wordlist Generator from a terminal environment. It enables password analysis, custom wordlist generation, and interactive prompts through various command-line arguments. This mode is ideal for security learners, professionals, and automation workflows.

Key Features of CLI Mode:

• Password strength analysis using zxcvbn or fallback entropy calculation. • Wordlist generation with support for name, pet, and year inputs. • Ability to export generated wordlists to text files. • Includes options for interactive operation and help guidance. • No GUI dependencies, making it ideal for headless systems or remote terminals.

CLI Usage Examples:

```
# Analyze password strength
python pwtool.py --analyze "P@ssw0rd2021!"

# Generate a custom wordlist
python pwtool.py --generate --name "Alice" --pet "Rex" --birth "1990" --years 2005-2024 -o mylist.txt

# Launch interactive mode
python pwtool.py --interactive

# Show help information
python pwtool.py --help
```

Advantages of CLI Mode:

• Lightweight and efficient — no graphical environment needed. • Scriptable for automation or batch execution. • Easily integrated into penetration testing pipelines or cybersecurity training labs. • Full control of input parameters and output customization.

Conclusion:

The CLI mode of the Password Strength Analyzer offers a practical and flexible way to perform security testing, training, and password auditing. It is suitable for cybersecurity professionals who prefer terminal-based workflows.