Rajat Sethi

CPSC 4240

Milestone 1

Idea: Advanced Password Strength Tester

Basic Goals:

The Advanced Password Strength Tester (APST) will be a specialized program that will put a password under intense standards. A password should not be found in common wordlists (like rockyou.txt), brute-forcible, or easily guessable. The tester will provide a brief analysis of how strong the password is and what improvements can be made.

Components:

1. Perform a linear search through several wordlists using "John the Ripper."
2. Record how long each search took (if applicable).
3. Perform a brute-force check (stops after a certain amount of time).
4. Record how long the brute-force took (if applicable).
5. Check if password is easily guessable (i.e., username and password are the same).
6. (Possible) A few other tests if I find anything else important.
7. Weigh the severity of each test and determine the password's strength level.
8. Print results and suggestions to user.
9. (Possible) Add flags and options for limited searches.

Implementation:

- The project itself should be a bash script working with custom C++ code.
- The bash script should download dependencies like John the Ripper (if not installed already).
- The C++ code will keep track of the data, time, and other calculations.
- The C++ code will also print out any suggestions that the user should make.
- The project can be pulled from a GitHub Repository.