Overview

Nearly everything in today’s world is protected by some system using a username and password. With all this information out there, criminals spend a lot of time attempting to crack the passwords and gather personal information about their victims. This information can be anything from daily schedules to social security numbers and banking information. Due to the possibility that the password can be protecting extremely sensitive information it is important for the users to use secure, or “strong”, passwords for all their accounts. In this project, we are going to assess password strength, as well as how the password encryption changes the difficulty of the cracking.

Problems

A main problem with passwords are that there are many variables that go into choosing a password. Some things such as names, important dates, and special locations are common choices. These items can usually be found in a quick Facebook search of the user. After a little work and time, an attacker can compile a list of all these items and produce a table that attempts all the different combinations of these to gain access.

Another problem with password protected accounts today is to help secure accounts administrators sometimes require users to change their passwords at set time intervals. This seems like it would be a good idea, but the user then generally chooses extremely easy passwords since they must remember a new one multiple times a year. To increase security, they have now made it easier for the attacker. Administrators have also moved to putting specific requirements on passwords, such as length and what characters are acceptable. This method also produces the same problem as above, due to users having to use passwords they are not used to.

Methods

There are multiple methods and tools online today that can be used to crack passwords. This project is going to focus on three main ways. The first way is using a third-party tool called John the Ripper, located in Kali Linux, that provides a brute force attack. Brute force attacks attempt every possible combination of characters to get to the correct password. The major drawback for this is that it can take the longest time out of all the methods. This brute force attack is much quicker than any brute force attack we could produce on our own. The second method to be used is the John the Ripper tool with whatever tool they recommend for each password. This has the advantage of being efficient and easy to use, but is not available to everyone. The final method is to conduct a dictionary attack using Python. A dictionary attack is where you have a list of common passwords and attempt each of them in the hopes that the user chose an easy password. This has the drawback of not working if the password is not in the dictionary.

Each of these methods are going to tested against three set of passwords. The first password set is going to be unencrypted. The second test will have all the passwords encrypted using MD5 encryption. The final method is to encrypt the passwords using SHA-256. The time taken to crack each password will be recorded and compared, with any test reaching 24 hours being declared a failure.