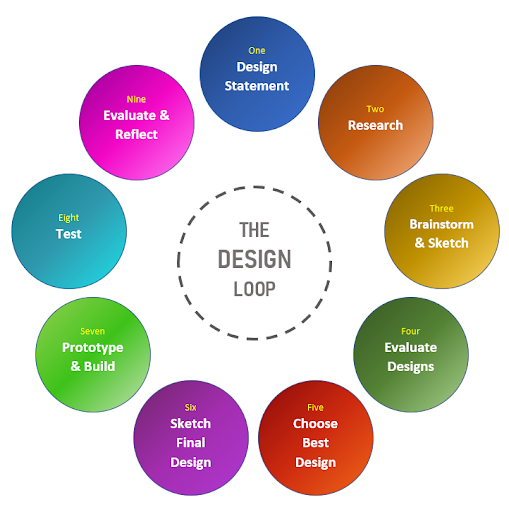
Alt 3 Project

Password Cracker



Design Statement

My Model is a password cracker, password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system. A common approach is to try guesses repeatedly for the password and check them against an available cryptographic hash of the password which is what I will be getting my program/model to do. The user enters multiple different passwords and the computer will attempt to crack/find/de-hash that password and send it back to the user to confirm that it's right.

Overview

I choose this topic because I find cryptography and ethical hacking (whitehat or blackhat) very interesting and I would love to learn more about it and see how it works and what makes people want to get into it.

I wanted to choose a project that not everyone else would be doing something that’s slightly difficult but not too difficult.

The main reason I choose this topic is because this is what I plan on doing in the future, I plan to study Digital forensics and computer security and I wanted to get a feel for what I will be potentially doing in the future.

Research on my idea

I got my research idea from my own personal interest in ethical hacking

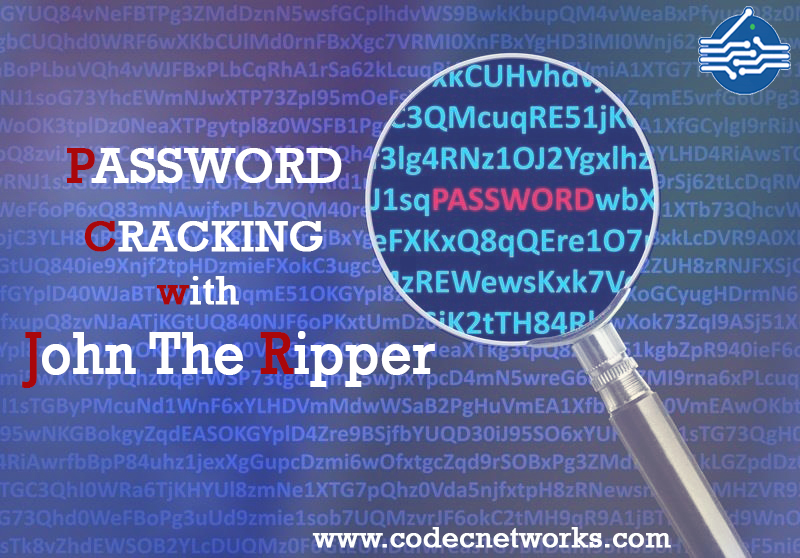
The password cracker is just one of many things that hackers would use

To gain access to accounts which is something i’m particularly interested

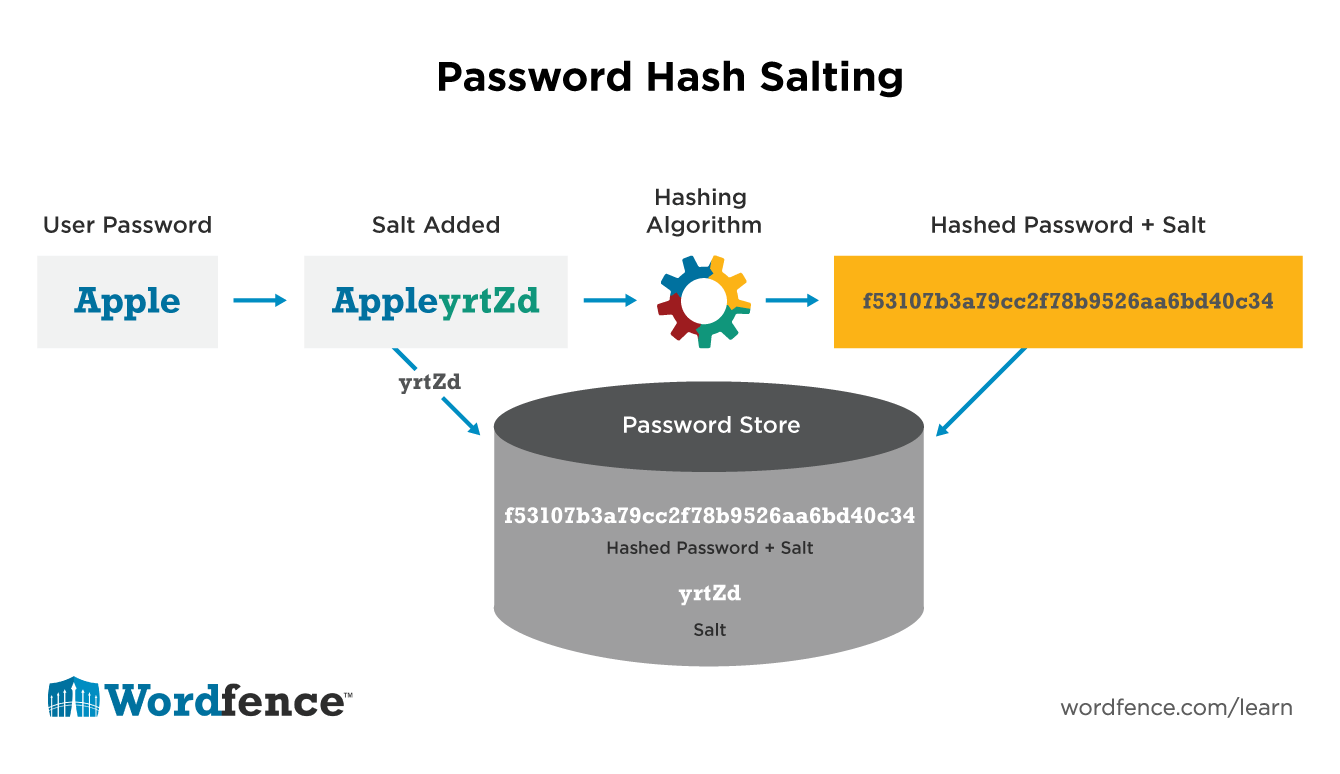
In.

Password cracking is the process of either guessing or recovering a password from stored locations or from a data transmission system. Since the introduction of a computer password, hackers have tried to crack passwords but it has only became popular and practical within the last ten years

The typical way password cracking works is to get a file containing user hashed passwords and then run a cracker against the file to try to get matches for all of the hashes, thus revealing all of the passwords in the file. While the latter part is typically uncomfortably fast, the first can be very difficult and many approaches may need to be taken to penetrate a system's security to obtain a password file. However, using simple, targeted Google searches it has become easier to gather unprotected hashes of users.



When passwords are stored on a system they are done so by first going through a hashing algorithm, then that hashed string is stored into a file. Hashing algorithms are one-way functions that turn a string of data into a fixed-length "fingerprint" that cannot be reversed. A hash for the word “computer” would be “df53ca268240ca7667c8566ee54568a,” using the popular hashing algorithm, MD5. Only cryptographic hash functions are used to implement password hashing. Some common examples are MD5, SHA-1, LM, NTLM, and Whirlpool.



Brainstorming and Sketching

For brainstorming I didn’t really know what I was going to do for my project so I just started to think of stuff that peaked my interest, I loved hacking, ethical or unethical I just had this love for it no matter what side you were on.

So I decided to base my project on it, I thought it would have been a great idea to try a password cracker, it’s not too difficult but it’s also not easy so I thought it would be the perfect fit.

I did a brief rundown of what my password cracker what it would look like and how it would work and I think that it should work well and that I wont run into too many problems on the way.

Evaluation Of Designs

The Plus and Minus points for each researched topic varied because I didn’t have many ideas that fitted the criteria for this project so I didn’t wanna do just anything that would fit the quote but something that would also peak my interest.

I had ideas such as creating a prediction model for a rookie’s future ability/worth in different kinds of sports and ideas such as Modeling a game or set of games with known expected outcomes to demonstrate how much a player stands to win/lose.

But both of these ideas were ruled out because I wanted to do something along the lines of computer security/pentesting so I decided to go with the Password Cracker.

Sketch your final Design

The design I plan to do will look similar to this but there might be some tweaks/changes in the final report.

* The user will enter the password
* The Computer will check the presented dictionary for that password
* If the password is cracked the computer will let you know