Digital Forensics – Spring 19
Project 1 – Password Cracking

Overview

This project is meant to introduce you to password cracking concepts.

Option 1

Write a basic password cracking program using Python. Your program should support brute force and dictionary cracking methods.

- You may only import 'hashlib', 'sys' and 'time' libraries
- This project will be restricted to unsalted md5 hashes
- For a dictionary method, your program should prompt the user for a dictionary file and the md5 hash to be cracked
- For both the brute force and dictionary methods, your program should output to screen the secret password, the time it took to crack the password and the number of passwords attempted

Dictionary method - I will test your program using a common dictionary list and random md5 hash of one of the words in the list.
Brute Force method – given the processing time required to brute force complex passwords, I will test your code on passwords shorter than 6 characters.

Extra grading consideration will be given to students who implement functionality to crack complex passwords (upper case, lower case, special characters, and mangling).

The following items must be submitted to receive full credit for this project:
1) A brief explanation of your approach to this project
2) Commented code (.py file)

Option 2

Submit a 3-5 page paper on one of the following topics:
- Compare various password cracking tools and techniques. For example, John the Ripper, Cain, Hashcat, Brute Force, Dictionary, Rainbow Tables.
- Recent security breaches related to compromised passwords and the associated security practices

Digital Forensics – Spring 19
Project 1 – Password Cracking

This project is due No Later Than midnight, February 12th.
Submit your project via Canvas.