CS5352: Computer Security **Instructor: Dr. Deepak Tosh**
Spring 2020 **Due Date:** 02/14/2020, Midnight

ASSIGNMENT# 1

INTRODUCTION:

The purpose of this assignment is to become familiar with Message digests, the concept of hashing a password, salting technique, and cracking passwords with a brute force or dictionary approach.

In this assignment, you will write programs (recommended to execute the programs in **Linux/Unix based Operating Systems**) that will crack as many of the passwords as you can. You will also write a report. This assignment includes a sample password files for each type of password file, dictionary file, and an excel file for the last question.

Problem# 1: [30 Pts]

The password file (**shadowfile.txt**) was generated with creation of 200 users with password taken from random English dictionary words and some commonly used passwords. I downloaded a dictionary file from the Internet, named **commonPasswdFile.txt**, containing about 100,000 entries. You should be able to find this file by searching the Internet. I have created 200 users (crack01—crack200) on an Ubuntu Linux machine and the shadow file is the one that is given here. The password file contains for each user: username, salt, hashed password, and some more details. The tasks to do are:

a. List all the attributes that are stored for an individual user in a shadow file.
b. Now write your own Python program that uses the **commonPasswdFile.txt** and compute the necessary hash of the passwords to compare them with the passwords stored in shadow file.
c. The program should output all the **username:password** combinations after successful crack. Please list them in the report too.
d. To verify the passwords, you can access http://129.108.7.182:4000/ and provide the following entries: (1) UTEP Miner ID; (2) username (for example "crack01"); (3) password that you found. (**Note**: In order to access this server, you have to be in UTEP campus or VPN to campus network.)
    i. List the passwords you have successfully cracked out 200 in your report.
e. The report must include answers to (a), (b), (c), and one sample snapshot of you successfully cracking the password.

Note: To make your testing easier, I am providing the password for 1 user here.
Testing Sample: Username: crack01 and password: 123456

Problem# 2a: [30 Pts]

In this part, imagine you have 500 password hashes from a password database of a web service (extracted to the file "*UnsaltedPassTable.txt*"). It is known that the users are not really familiar with password security and create their passwords in the following ways:

1. An English word as the password (e.g. "secret")

2. A string of up to 8-digits as password (e.g. “87654321”)
3. An English word followed by some digits, but together no more than 10 characters (e.g. password89)
4. Concatenate two English words together (e.g. “secretpassword”)

When choosing English words, users only use the words from the provided dictionary of 10,000 most common English words (“*words.txt*”).

**Hint: Users are not really inclined to use very short words.

Testing Sample: Username: user1 and password: revenge234

Problem# 2b: [40 Pts]

Imagine, you got access to another password table from the same web server, but this contains usernames and password of 100 VIP users (extracted to the file “*SaltedPassTable.txt*”). The website has SALTED the password hashes to provide better security, however the users still created their passwords based on same way as discussed above. There are only 100 password hashes in this table, and the salt values are provided alongside the hashes.

The goals in the above two problems is to

1. Find all the cracked passwords.
2. Report the time taken to crack for all the users and provide your remarks on why they are different.

Testing Sample: Username: user1 and password: 16083058

Homework Download

You can download the necessary files from the following Google Drive link:
https://drive.google.com/drive/folders/1Xk0AoUf_V_mdt22YvcIMJ9YiZqWPUmpx?usp=sharing

Inside the drive, there are 3 directories for each problem. Under Problem-1 directory, there are two files named **shadowfile.txt** and **commonPasswdFile.txt** which you will be using to solve the Problem# 1. Under Problem-2, I have provided 3 files. (1) “*words.txt*” which contains 10,000 English words that people use to create their passwords. (2) *“UnsaltedPassTable.txt”* contains the password hashes you need to crack for Part 2a, with “{username}:{hash}” on each line. For example, if the username is “john” and password hash is 7e23..2b41, then that line will be:

john:7e238a22c982f0d9de093fc7bca92b41

(3) “*SaltedPassTable.txt*” contains the password hashes for Part 2b. It has username, salt, and hashed password on each line, separated by “:”. Using the same username and password as above, with a salt value 67ef98c0, the corresponding line in the password table is:

john: 67ef98c0:55457bde7a1a4816ba636d09017ff30a

Grading:

The assignment will be graded on programs correctness, programs readability, verification of the username you succeeded to log into the server, and report.

Submission:

Please submit your reports in PDF format and codes in ZIP file on **BLACKBOARD only**. Make sure to answer the questions in order and CLEARLY STATE YOUR ASSUMPTIONS, if you are unsure about something.

If you have any questions, comments, concerns, doubts, or confusions, please stop by my office to clarify. You can also email me on dktosh@utep.edu. I will be very happy to help.