CMPUT 333, Assignment 1, Winter 2021

(sliding part - 25%)

University of Alberta / Department of Computing Science

Instructor: Ioanis Nikolaidis (nikolaidis@ualberta.ca)

(password cracking)

Part 4 (25%)

You are given hashed passwords. Each group is given a set of five Unix password hashes. You are to determine the passwords for the hashes assigned to *your group*.

The following "hints" must be exploited to reduce the search space. For each group:

1. one Unix password is a Spanish word,
2. one Unix password is a mangled Oilers player name (from the early 90s roster),
3. one Unix password is an English word with two of its letters in leet,
4. one Unix password is a hexadecimal number.

The mangling of the Oilers player name is performed by introducing a connector (can be $, %, *, or _) between first and last name. Each component of the name (first name and last name) are transformed separately with respect to character capitalization. There are three options for each name component capitalization: all letters in lower case, all letters in upper case, first letter upper case with the rest lower case. The capitalization strategy for the first component (first name) can be different from the capitalization strategy applied to the second component (last name).

The leet-transformed English word is a word in which exactly two characters (two *different* characters) have been transformed to leet equivalent.

Tools

The highly recommended tool for the job is "John-the-Ripper" (https://www.openwall.com/john/) but because of some extensions (and lots of user-contributed code) you are probably better served by the community version of the same tool maintained at a github repository (https://github.com/magnumripper/john).

In order to receive full marks, you need to provide the passwords you found but you must *also* provide:

1. the process and tools you used to collect relevant information (e.g., player names, etc.),
2. the mangling rules you used in each case to control the search carried out by John-the-Ripper,
3. the time it took you (even if approximate) for each password to be cracked.

Brute force cracking can work well in some cases, but it does not result in full marks. You must focus the search space as much as possible. Also, ensure that you indicate exactly which version of John-the-Ripper you used and

any exceptional compilation flags you may have used.

Deliverables

Only one of the group members need to submit on behalf of the entire group (in the event of more than one submission, the last one will be considered). Your report should include answers to the questions and should cite any resources that you used to answer the questions. By default it is assumed that all group members equally contribute to the assignment. If you need to deviate from this model of cooperation, explain why and indicate who was responsible for what. There is no restriction to the language you can use for programming as long as you can provide the instructions of how to compile and run your code in CS undergraduate lab machines (and specifically the *ucXX.cs.ualberta.ca* hosts). Your report (in plaintext, markdown, or pdf format) to address the questions raised in this assignment should be submitted as a single file accompanying your results, source code, etc.

(This is the sliding part of Assignment 1 and will be submitted separately from the non-sliding part by the deadline for the non-sliding part of Assignment 2.)

Monday, January 25, 2021