Exercise 02

# Overview

This exercise provides hands-on experience with Cryptography to perform brute force password attacks using ‘John The Riper’ tool

# Learning Objectives

* Understand basics of password management in Unix/Linux based systems
* Understand brute force attacks on password.
* Ability to apply basic regular expression understanding to provide appropriate patterns to John The Ripper tool

# Reading Material

1. <https://www.openwall.com/john/doc/RULES.shtml>
2. <https://miloserdov.org/?p=5477>
3. <https://en.wikipedia.org/wiki/Passwd>

# Prerequisites and environment familiarity

Student should be familiar with Linux and command line terminal usage.

Student should be familiar with use of /etc/shadow file structure

You will given access to Kali Linux VM where the tool JTR (john) is installed. Information about the IP address of this VM and login process will be provided by Sachin Phogat (TA for this course).

# Description

The assignment is to carry out a password cracking exercise using open source software “John The Ripper” (<https://www.openwall.com/john/>) on a given system. You will be provided 20 entries of /etc/shadow file corresponding to usernames cruser<NN>, where NN can have value between 11 to 99 (including both). The passwords based on dictionary words consisting your first name or last name and these names will be given to you in a file. You need to use this list of names as the dictionary to launch the dictionary base attack. Both the files “shadow” and “usernames” (to be used as dictionary words) will be available in home directory /home/cmscuser on this VM machine.

To facilitate cracking, the passwords are constructed in one of the following ways and have minimum length of 8 and max length of 12.

1. Name itself e.g. if the dictionary word is “ramrustagi”, then password can be “ramrustagi”
2. Name suffixed with some digits (123…). For example, if name is “Ram”, then password could be “RamNNNNN”, where N can be between 1 to 9 such as “Ram12345” or “Ram11111”.
3. Name suffixed or prefixed intermingled with digits. For example, if the name is “Ram”, then password can be “NNRaNmNN”, where N can be between 1 to 9.
4. Letters of name (if length is less than 8, then appended with some number of digits to make it at least 8 characters) shuffled randomly, with at least two letters capitalized.

Your assignment is as follows:

1. Run the John The Ripper (JTR) tool with appropriate options for constructing the proper rule to launch the dictionary attack.
2. After you discover the password, verify by login to that user account with the password. After login to that user account, create a file named “password” in the home directory of the user which contains the password.

## Explanation and Hints

1. First run the tool *john* with just simple dictionary words as it is.
2. Run the tool *john* with a rule that adds digits at the end of the word.
3. Either create all possible shuffle of the given word(s) and run the tool with these words with capitalization
4. Run the brute force check for all possible combinations of all alphabets of max length 12.

# Assessment and Rubric

Please do submit the following

1. The commands that you used to invoke the password cracker ( 2 marks)
2. List of username and corresponding password (cracked by you) along with the time taken by the tool to discover each password. Tool can report that information when password is cracked. The marks allotment is as follows.
   1. 2 marks for first 2 password
   2. 2 marks for next 3 passwords
   3. 2 marks for 2 more passwords
3. Challenges faced and how did you address these (2 marks)

# Note

Any plagiarism activity will result in penalties of being awarded 0 marks.

<end of Exercise 02>