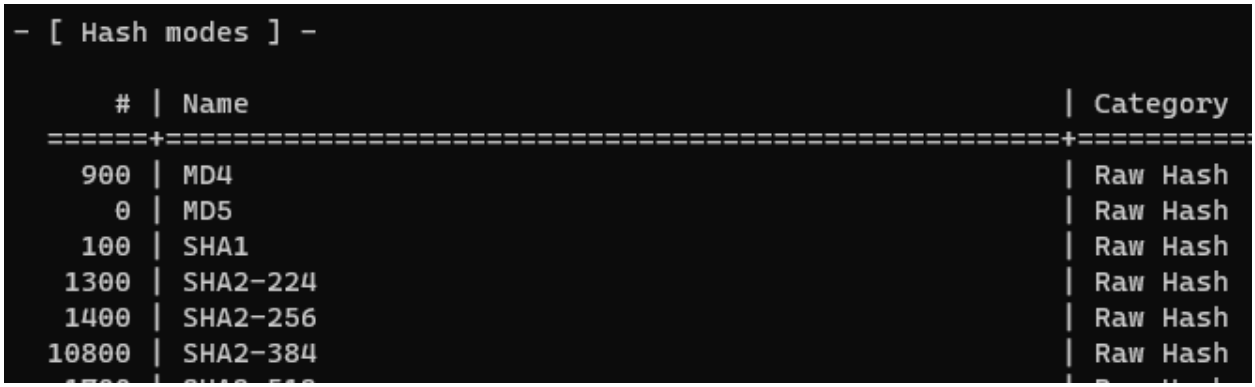
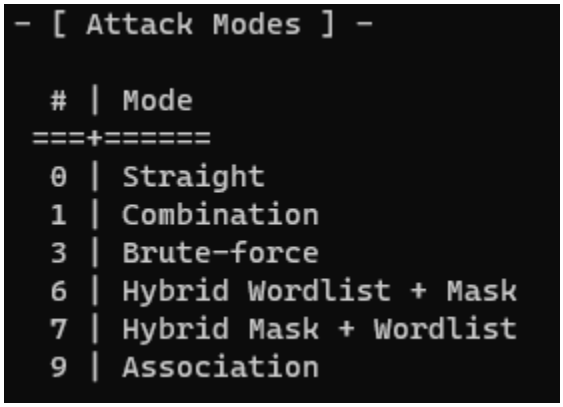
Lab Task 1: Cracking Passwords Using Hashcat on Kali Linux

Objective:
This lab task aims to familiarize yourself with the usage of Hashcat, a popular password-cracking tool, on Kali Linux. You will learn how to crack passwords using different attack modes supported by Hashcat.

Steps:

1. Create a file named hashes.txt that contains the hash (without quote, line separated) - '5f4dcc3b5aa765d61d8327deb882cf99', 'aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d'
2. Rockyou database location: /usr/share/wordlists/rockyou.txt
3. Command format: `hashcat -m [hash_type] -a [attack_mode] [hash] [dictionary]`





4. Execute a command to perform a dictionary attack.
5. Execute a command to perform a brute-force attack.

Lab Task 2: Rainbow Table Generation
Before starting task 2, install rainbowcrack from here http://project-rainbowcrack.com/

Objective:
The objective of this lab task is to understand the concept of rainbow tables and learn how to generate rainbow tables using the RainbowCrack tool on Kali Linux. You will create and use rainbow tables to efficiently crack password hashes.

Steps:

1. Ensure that RainbowCrack is installed on your system. If not, you can install it using the following command:
   `sudo apt-get install rainbowcrack`
2. First we run it with `rtgen -h` to see the options
3. Write a command to generate a rainbow table for a MD5 hash of a 4 plaintext length (containing only alphabets)
4. This rainbow table will be stored in /usr/share/rainbowcrack directory.
5. Crack this md5 hash - d6ca3fd0c3a3b462ff2b83436dda495e
6. Discuss possible solution to prevent such attacks

Tutorial: https://www.kalilinux.in/2021/03/rainbow-tables-rainbowcrack-kali-linux.html

Lab Task 3:

Repeat the same task as task 1. But, instead of using Hashcat, use John the ripper.
Do your own research and execute the necessary commands.