**Lab #5.1 - Introduction to Password Cracking using Hashcat**

**0. Lab Objectives**

At the end of this lab exercise, you should be able to:

* Be familiar with the concept of password cracking
* Apply Hashcat for password cracking purposes
* Understand the importance of having strong passwords

1. Run the hashcat benchmark (eg hashcat -b -m 0), and complete the following:

The purpose is to find out the speed of hashcat for each of the specified hash functions. That is, we want to see how many hashes it can run per second.

Your Device: cpu-penryn-AMD Ryzen 7 7435HS, 2193/4450 MB (1024 MB allocatable), 4MCU

Hash rate for MD5: 169.3 MH/s (10.75ms)

Hash rate for SHA-1: 91087.0 kH/s (4.49ms)

Hash rate for SHA-256: 37033.8 kH/s (55.32ms)

1. We have hashed a SHA-256 value of the following and put it into a file named file.txt:

106a5842fc5fce6f663176285ed1516dbb1e3d15c05abab12fdca46d60b539b7

By adding a word of “help” in a word file of words.txt, prove that the following cracks the hash (where file.txt contains the hashed value):

hashcat -m 1400 file.txt words.txt

|  |
| --- |
|  |

1. The following is an MD5 hash, for “help”:

657f8b8da628ef83cf69101b6817150a

Prove that the following can crack the hash (where file.txt contains the hashed value):

|  |  |
| --- | --- |
| What is the command? | hashcat -m 0 file1.txt words.txt |
|  | |

1. Suppose the following cities have been hashed by MD5. Crack them and write down what the cities are.

d177b4d1d9e6b6fa86521e4b3d00b029 dea56e47f1c62c30b83b70eb281a6c39 b90bbd2b879d5c0167b28d02c017771a 22638a3131d0f0a7346b178fd29f939c

The command(s) I used was/were:

hashcat -a 0 -m 0 file2.txt /usr/share/wordlists/rockyou.txt

Cities:

1) liverpool

2) barcelona

3) bangkok

4) shanghai

1. Rather than use a dictionary, we can use a brute force a hashed password using a lowercase character set:

hashcat -a 3 -m 0 file.txt ?l?l?l?l?l?l?l?l

The above command is known as *filter* style.

Using this style of command, crack the following 4-lower-case-letter word followed by 4 digits that have been hashed by SHA-1 algorithm:

0323658974aa5427d485a179cb0ddf90a8c4cfc1

The command I used was:

hashcat -a 3 -m 100 file5.txt ?l?l?l?l?d?d?d?d

The word is: year2024

Using this style of command, crack the following 8-lower-case-letter word that have been hashed by SHA-256 algorithm:

5489eb1d2a0285016de38986b21749ed5beee9ac3f5097b9a95854dd146b1b07

The command I used was: hashcat -a 0 -m 1400 file6.txt /usr/share/wordlists/rockyou.txt

The word is: accident