Lab #6.2 - Pasword Cracking with Hashcat Activities

0. Lab Objectives

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

- Carry out password cracking in more complex situations using Hashcat

1. Scenario 1

Suppose that you have been able to locate a set of passwords. It appears that they are all in the format: “DIGITECH-SUT-“ followed by 4 digits. You job is to crack them.

9200a1ca87d0989be58eb01347f0c3cc
c5cc1686176878a460c39d1412517401
c395f4f189de723e9bcd3a2d16c0d636
6de30cff92c2ea8f0797f02ac8599ec1
f696c1f409eb002b22f3b3aa099e65d7
e7b9b01b1c83c685431dd7104b0e93af
0fdaf89b29c3c9a65196354710637a43
a3c0e1dc7c6d8d190f9b81991a7b9bd8
424a20217ac7cc7318792810d6e6bfa6
afe0daf86231e852377a69dc67dc0590

1.1 Write a short explanation to show the steps you take to crack the above hashes.

ใช้การ Brute Force Attack **ด้วย** -a 3 **โดยใช้** Filter style **ของ** hashcat
โดยในโจทย์มี DIGITECH-SUT- **ให้แล้ว โดยเพิ่ม** Filter “ ?d “ **ทั้งหมด** 4 **ตัว** DIGITECH-SUT-?d?d?d?d **และกำหนดให้เป็น** MD5 **คือ** -m 0
จะได้เลขทั้งหมดมาตามข้างล่าง

0fdaf89b29c3c9a65196354710637a43:DIGITECH-SUT-4999
c395f4f189de723e9bcd3a2d16c0d636:DIGITECH-SUT-0367
c5cc1686176878a460c39d1412517401:DIGITECH-SUT-0099
f696c1f409eb002b22f3b3aa099e65d7:DIGITECH-SUT-1234
afe0daf86231e852377a69dc67dc0590:DIGITECH-SUT-9988
9200a1ca87d0989be58eb01347f0c3cc:DIGITECH-SUT-0001
424a20217ac7cc7318792810d6e6bfa6:DIGITECH-SUT-9111
e7b9b01b1c83c685431dd7104b0e93af:DIGITECH-SUT-1843
6de30cff92c2ea8f0797f02ac8599ec1:DIGITECH-SUT-0754
a3c0e1dc7c6d8d190f9b81991a7b9bd8:DIGITECH-SUT-8972

1.2 What is the command you need to crack the above hashes?

hashcat -a 3 -m 0 hash DIGITECH-SUT-?d?d?d?d

1.3 What are the values of the cracked passwords?

Hash Value	Cracked Password
9200a1ca87d0989be58eb01347f0c3cc	DIGITECH-SUT-0001
c5cc1686176878a460c39d1412517401	DIGITECH-SUT-0099
c395f4f189de723e9bcd3a2d16c0d636	DIGITECH-SUT-0367
6de30cff92c2ea8f0797f02ac8599ec1	DIGITECH-SUT-0754
f696c1f409eb002b22f3b3aa099e65d7	DIGITECH-SUT-1234
e7b9b01b1c83c685431dd7104b0e93af	DIGITECH-SUT-1843
0fdaf89b29c3c9a65196354710637a43	DIGITECH-SUT-4999
a3c0e1dc7c6d8d190f9b81991a7b9bd8	DIGITECH-SUT-8972
424a20217ac7cc7318792810d6e6bfa6	DIGITECH-SUT-9111
afe0daf86231e852377a69dc67dc0590	DIGITECH-SUT-9988

2. Scenario 2

Suppose that you have been able to locate a set of passwords. After having cracked a few passwords, it appears that they overlap with the passwords in the Rockyou breach. There are only a few left to be cracked. Can you crack them?

a11c8694ddaa49e036807888e4f739e0
4a2c8813df066aba95359d5cb99a7dac
6b12ba85cf7c36202bf75ba53cd75d7f
0b2db70c8a0ed91a6968fc95c21e2556
078767cdd05b7e91b7375a76cf66736f

2.1 What is the directory for the rockyou wordlist or password dictionary?

/usr/share/wordlists/rockyou.txt.gz

2.2 What is the type of hash function (hashing algorithm) you are trying to crack?

MD5

2.3 What is the attack mode (-a) you use to crack the passwords?

Dictionary “-a 0”

2.4 What is the command line you use to crack the passwords?

```
hashcat -a 0 -m 0 hashall2.txt /usr/share/wordlists/rockyou.txt.gz
```

2.5 What are the values of the cracked passwords?

Hash Value	Cracked Password
a11c8694ddaa49e036807888e4f739e0	red05
4a2c8813df066aba95359d5cb99a7dac	blue27
6b12ba85cf7c36202bf75ba53cd75d7f	yellow22
0b2db70c8a0ed91a6968fc95c21e2556	green9
078767cdd05b7e91b7375a76cf66736f	purple101

3. Scenario 3

Suppose that you have been able to locate a set of passwords, which incidentally belong to hackers. Somehow you have found out that these hackers really like Doraemon. Can you crack the followings?

E7BF35DA90A7C6D80B19BF4287F9588384553C680E541AD13C8B08073E45066B
00FBF54A345E5874A00F97D86DB2A052850AB3891233BB257CE170D698058D1A
79A7404869FCCF1D762793A1D50A54D273569A98033293EE3C8F1A8C2917FA63
9F499D515065BE9B32D7C5A12286BF537A7A999D9E45C44FD6F0EDE6F8CB5BBE
CB94D795781F8E86FB34E995DD2D6F253E05A19EB1F1BA6F6896E6CF79D24AD5
DB5BEA376A0DC01A0DC3D3389ED02651EB2AD23D4789C44560D60985974D296A

3.1 What is the type of hash function (hashing algorithm) you are trying to crack?

SHA-256

3.2 Write a short explanation to show the steps you take to crack the above hashes.

ใน Hash ข้างต้น นำไปใส่ในไฟล์ text ชื่อ Do
แล้วทำการ Crack โดยใช้ Dictionary -a 0 และใช้ hashing algorithm “ SHA-256”
โดยใช้ Dictionary ของ Hashcat ชื่อ Rockyou.txt.gz
แต่พบว่าไม่สามารถ Hash ได้ทั้งหมด จึงดูข้อความพบว่า Hacker ผู้นี้ชอบ Doraemon
จึงดูว่าตัวละครหลักมีใครบ้าง และ Hash ที่เหลือออกมา โดยใช้
hashcat -a 3 -m 1400 Do2 Doremi
hashcat -a 3 -m 1400 Do2 Suneo
hashcat -a 3 -m 1400 Do2 Giant

3.3 What is the command you need to crack the above hashes?

hashcat -a 0 -m 1400 Do /usr/share/wordlists/rockyou.txt.gz

3.4 What are the values of the cracked passwords?

Hash Value	Password
E7BF35DA90A7C6D80B19BF4287F9588384553C680E541AD13C8B08073E45066B	Doraemon
00FBF54A345E5874A00F97D86DB2A052850AB3891233BB257CE170D698058D1A	Nobita
79A7404869FCCF1D762793A1D50A54D273569A98033293EE3C8F1A8C2917FA63	Shizuka
9F499D515065BE9B32D7C5A12286BF537A7A999D9E45C44FD6F0EDE6F8CB5BBE	Suneo
CB94D795781F8E86FB34E995DD2D6F253E05A19EB1F1BA6F6896E6CF79D24AD5	Doremi
DB5BEA376A0DC01A0DC3D3389ED02651EB2AD23D4789C44560D60985974D296A	Giant