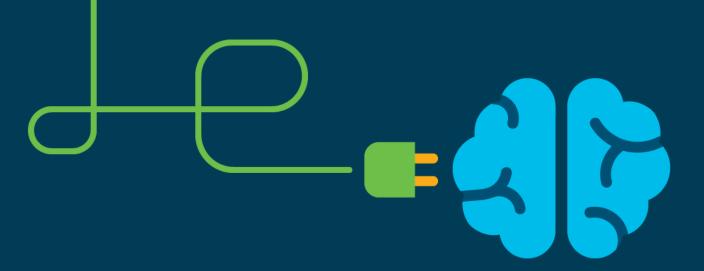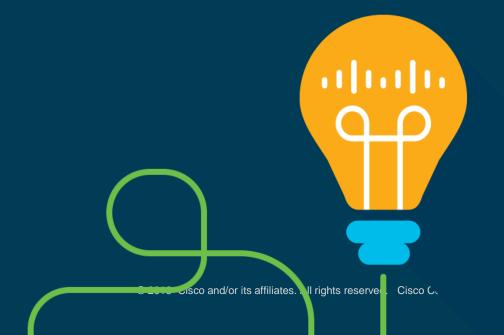# Password Cracking using Hashcat

Ismail Abdurrahman Hakim

26 February 2021

Introduction to Hash

What is Hash

Hash is the simplest type of cryptographic operation which is the result of hashing algorithm.

Hash Algorithm

Hashing algorithm:

1. NT hash

2. MD5

3. SHA 128

4. SHA 256

5. SHA 512

Hash Example

MD5

5f4dcc3b5aa765d61d8327deb882cf99

SHA-256

5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542D8

SHA-512

B109F3BBBC244EB82441917ED06D618B9008DD09B3BEFD1B5E07394C706A8BB980B1D7785
E5976EC049B46DF5F1326AF5A2EA6D103FD07C95385FFAB0CACBC86

Hash Characteristics

- Fixed Length

- One way process

- Same word always gives identical hash value

Salt

Adding random value characters to the hash.

Characteristics:

1. Often is not secret

2. Must be unique to each password

Salt Example

Password: abcde

Salt: K56Khj

Salted Password: abcdeK56Khj

MD5 Hash: 6718dc2b249d3f9cfd1d55f4774718fe

Hash Location

Linux: /etc/shadow

Windows: C:\windows\system32\config\SAM

Active Directory NTDS.dit in %SystemRoot%/NTDS

SQL database

Router

Cracking the Hash

- The most realistic way to crack the hash is by using dictionary or brute force.

- The latter is effective for relatively short plain-text/password

- Dictionary attack itself is divided into different methods

  1. "Basic" dictionary attack

  2. Rainbow attack (pre-calculated hashes)

  3. Mask attack (dictionary + rules)

Tools

Hashcat

JohnTheRipper

Online Tools

Hashcat

Hashcat Strength

- Cracking password using GPU is the trend

- Modular

The Four Arguments of Hashcat

Hashcat –m <hash-type> -a <attack-mode> <file-name> <dictionary>

The four essential arguments are

1. Hash type

2. Attack mode

3. File name (target hashes)

4. Dictionary

First Argument: Hash type

https://hashcat.net/wiki/doku.php?id=hashcat

Option = -m, hash type example

1. MD5 = 0

2. NT-Hash = 1000

3. SHA1 = 100

4. SHA-512 = 1700

5. SHA512crypt = Unix

Second Argument: Attack Mode

Option= -a , Attack mode

- 0 = Straight

- 1 = Combination

- 3 = Brute-force

- 6 = Hybrid wordlist + mask

- 7 = Hybrid mask + wordlist

Third Argument: File Name

Replace filename with list of hashes or you can input a single hash here

Fourth Argument: Dictionary

Lab purpose:

1. Rockyou

2. Using your own

Great dictionary for a real password cracking activity:

1. Rockyou

2. Geovedi Indonesian wordlist

3. Danielmiessler SecLists

Demo

Feel Free to Access File

https://github.com/devismail2y/hashcatlab

Basic Password Cracking

hashcat -m 0 -a 0 BasicPasswordCracking.txt ezwordlist.txt

Masking Attack

hashcat -m 0 -a 1 BasicPasswordCracking.txt CommonEnglishWords.txt ezwordlist.txt

Password Cracking with Rule

hashcat -m 0 -a 0 BasicPasswordCracking.txt ezwordlist.txt ==-r /usr/share/hashcat/rules/dive.rule==

Brute-Forcing

Basic:

hashcat -m 0 -a 3 BasicPasswordCracking.txt ?a?a?a?a

Increment:

hashcat -m 0 -a 3 BasicPasswordCracking.txt -i ?a?a?a?a

Terimakasih