Cracking Speed of Password Attack Tools/Modes

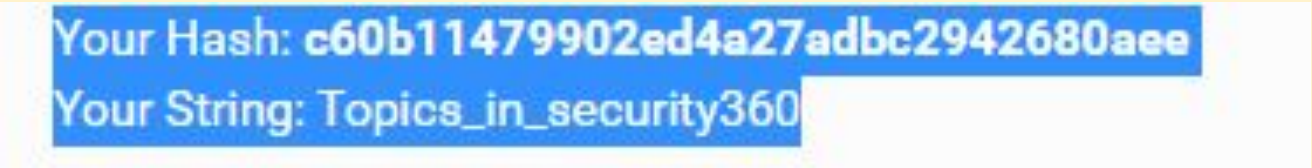
- By Jaleel Calhoun & Joshua Parrella

General Objectives

- Use multiple password attack tools & attack modes in Kali Linux
- Compare each tool’s password attack modes and speed of cracking a hash value/password
- “Hashcat” and “John the ripper”
- Hashcat: Straight, brute-force, combination attack modes
- John: Straight/Single mode

Overall Procedure (Attack Modes)

- Hash the password: “Topics_in_security360”
- Store hash value in a text file of Kali Linux
- Create an appropriate word list
- Hashcat used to crack hash value using different attack modes
- Measure time for each attack mode to crack hash

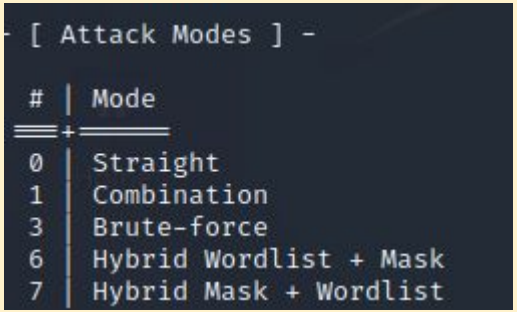


Overall Procedure (Attack Tools)

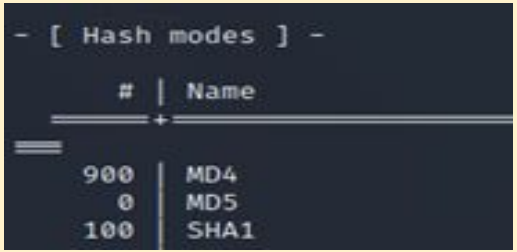
- Hash the password: “Test1”
- Store hash value in seperate text file
- Create new word list
- Hashcat used to crack hash value using (straight) attack mode
- John used to crack hash value using (straight/single) attack mode
- Measure cracking time for both attack tools

Hashcat's Formats

```
- [ Options ] -

Options Short / Long          | Type | Description
Example
==============================+======+============================================
==========================

-m, --hash-type               | Num  | Hash-type, see references below
-m 1000
-a, --attack-mode             | Num  | Attack-mode, see references below
-a 3
-V, --version                 |      | Print version
-h, --help                    |      | Print help
    --quiet                   |      | Suppress output
    --hex-charset             |      | Assume charset is given in hex
    --hex-salt                |      | Assume salt is given in hex
    --hex-wordlist            |      | Assume words in wordlist are given in hex
    --force                   |      | Ignore warnings
```



```
- [ Attack Modes ] -

 #  | Mode
====+======
 0  | Straight
 1  | Combination
 3  | Brute-force
 6  | Hybrid Wordlist + Mask
 7  | Hybrid Mask + Wordlist
```



```
- [ Hash modes ] -

      #  | Name
=========+=================================================
===

    900  | MD4
      0  | MD5
    100  | SHA1
```

Hashcat - Straight

1. Create file with hash (“hash.txt”)
2. Create text file with possible passwords (“wordlist.txt”)

Command:

```
┌──(kali㉿kali)-[~]
└─$ hashcat -a 0 -m 0 /home/kali/Desktop/hash.txt /home/kali/Desktop/wordlist.txt
hashcat (v6.1.1) starting ...
```

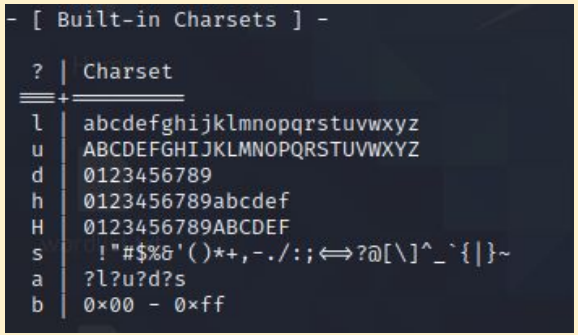
Output:

Time = 37s

```
c60b11479902ed4a27adbc2942680aee:Topics_in_security360

Session..........: hashcat
Status...........: Cracked
Hash.Name........: MD5
Hash.Target......: c60b11479902ed4a27adbc2942680aee
Time.Started.....: Tue Dec  1 16:43:46 2020 (0 secs)
Time.Estimated...: Tue Dec  1 16:43:46 2020 (0 secs)
Guess.Base.......: File (/home/kali/Desktop/wordlist.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      176 H/s (0.01ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 16/16 (100.00%)
Rejected.........: 0/16 (0.00%)
Restore.Point....: 0/16 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: Apple000 → security360

Started: Tue Dec  1 16:43:14 2020
Stopped: Tue Dec  1 16:43:47 2020
```

Hashcat - Mask Attack (Brute-Force)

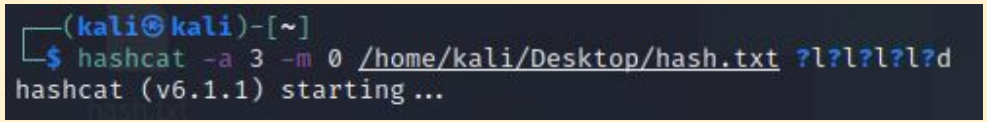
1. Create file containing hash/hashes → (“hash.txt”)
2. Determine Charset using length of password



Ex: password = test1

Charset = ?l?l?l?l?d

3. Execute command using determined charset



Hashcat - Mask Attack

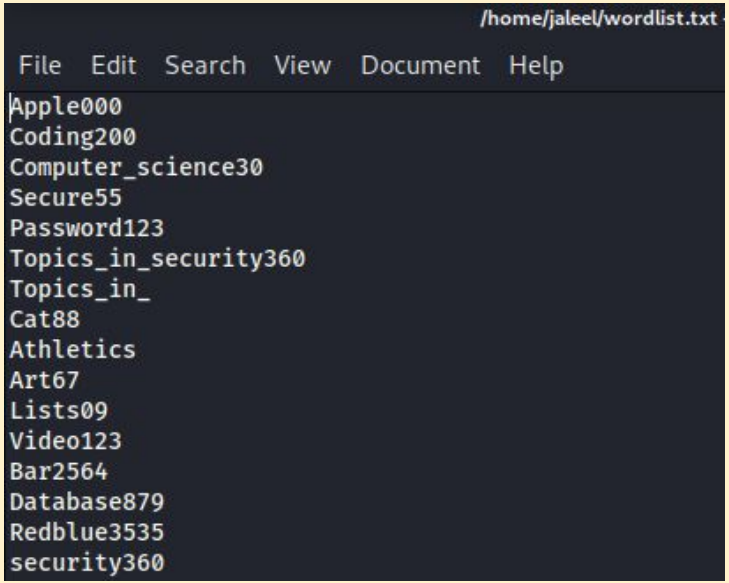
Output:

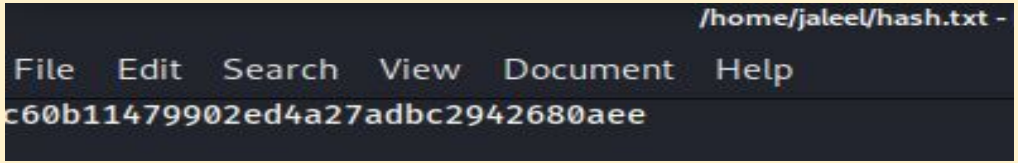
```
Session..........: hashcat
Status...........: Exhausted
Hash.Name........: MD5
Hash.Target......: /home/kali/Desktop/hash.txt
Time.Started.....: Tue Dec  1 20:03:47 2020 (1 sec)
Time.Estimated...: Tue Dec  1 20:03:48 2020 (0 secs)
Guess.Mask.......: ?l?l?l?l?d [5]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 13075.8 kH/s (0.81ms) @ Accel:1024 Loops:26 Thr:1 Vec:8
Recovered........: 2/3 (66.67%) Digests
Progress.........: 4569760/4569760 (100.00%)
Rejected.........: 0/4569760 (0.00%)
Restore.Point....: 175760/175760 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-26 Iteration:0-26
Candidates.#1....: sskv5 → xqxv5

Started: Tue Dec  1 20:03:45 2020
Stopped: Tue Dec  1 20:03:48 2020
```

Time: 3s

Hashcat - Combination

1. Stored hash value in text file “hash.txt” (cat > hash.txt)
2. Created/used wordlist “wordlist.txt” (cat > wordlist.txt)





Hashcat - Combination

3. command/statement

```
jaleel@kali:~$ hashcat -a 1 -m 0 /home/jaleel/hash.txt /home/jaleel/wordlist.txt /home/jaleel/w
ordlist.txt
hashcat (v6.0.0) starting ...
```

4. Obtain result/measure cracking time

```
c60b11479902ed4a27adbc2942680aee:Topics_in_security360

Session..........: hashcat
Status...........: Cracked
Hash.Name........: MD5
Hash.Target......: c60b11479902ed4a27adbc2942680aee
Time.Started.....: Mon Nov 16 17:38:43 2020 (0 secs)
Time.Estimated...: Mon Nov 16 17:38:43 2020 (0 secs)
Guess.Base.......: File (/home/jaleel/wordlist.txt), Left Side
Guess.Mod........: File (/home/jaleel/wordlist.txt), Right Side
Speed.#1.........:    99869 H/s (0.11ms) @ Accel:1024 Loops:15 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 225/225 (100.00%)
Rejected.........: 0/225 (0.00%)
Restore.Point....: 0/15 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-15 Iteration:0-15
Candidates.#1....: Apple000Apple000 → security360security360

Started: Mon Nov 16 17:38:41 2020
Stopped: Mon Nov 16 17:38:45 2020
```

John the Ripper - Single/Straight

- Wordlist used/created
- Command and results

```
jaleel@kali:~$ sudo john --format=raw-md5 /home/jaleel/passwords.txt /home/jaleel/hash2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
test1            (?)
1g 0:00:00:00 DONE 2/3 (2020-11-17 18:54) 20.00g/s 53760p/s 53760c/s 53760C/s ncc1701d..nermal
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
jaleel@kali:~$
```

/home/jaleel/p

File Edit Search View Document Help

```
oranges123
test1
fishing898
unit9000
department5677
location065
running123
blue55
digital3d
project2
red59
flower000
cracking345
hack09
password98
resting77
computer94
hardware32
software01
information2
yellow9
new555
racing101
filming123
tech202
```

Hashcat - Straight

- Statement/command
- Results

```
jaleel@kali:~$ hashcat -a 0 -m 0 /home/jaleel/hash2.txt /home/jaleel/passwords.txt
hashcat (v6.0.0) starting...
```

```
5a105e8b9d40e1329780d62ea2265d8a:test1

Session..........: hashcat
Status...........: Cracked
Hash.Name........: MD5
Hash.Target......: 5a105e8b9d40e1329780d62ea2265d8a
Time.Started.....: Wed Nov 18 11:27:26 2020 (0 secs)
Time.Estimated...: Wed Nov 18 11:27:26 2020 (0 secs)
Guess.Base.......: File (/home/jaleel/passwords.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      628 H/s (0.04ms) @ Accel:1024 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 27/27 (100.00%)
Rejected.........: 0/27 (0.00%)
Restore.Point....: 0/27 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: oranges123 →

Started: Wed Nov 18 11:27:20 2020
Stopped: Wed Nov 18 11:27:27 2020
jaleel@kali:~$
```

Overview

Compare attack mode

Attack Mode	Seconds
Straight	37s
Brute-force(mask)	3s
Combination	4s

Compare Attack tools

Attack Tool	Seconds
John	1s
Hashcat	7s