

LAB – 2 B00122875 Vimal Jaswal

Hashing Investigation

You've been asked by the Garda to assist in helping to retrieve some hashed passwords. They have managed to get a dump of one of the database tables, however they still need the original passwords and have been unable to crack them themselves and have called in your help. The issue seems to be that the database is only storing the password hashes, and so far their attempts to brute force the passwords have failed.

They have tried their standard rainbow tables without success and suspect that the passwords may have been salted. A brief analysis of the hashes supports this belief and indicates that all the passwords have been hashed with the same salt. **Can you help the Garda and crack any of the salted hashed passwords?**

Some potentially useful information from the Garda case files:

- The password policy file was changed in May 2010, passwords created after this date are alphanumeric 5-7 characters in length. Passwords created before these dates are believed to have consisted of only digits and 5-7 characters in length.
- It's believed that all passwords have used the same salt, and that the value is somewhere in our data.
- The database dump was from MySQL database
- The site's domain name is www.exploringsecurity.com
- Some of the captured JavaScript code from the site, reveals the salt format as `CommonHash($salt,$pass)`

Retrieve as much information as you can from the dump below for the Garda.

Join_date	Username	Password	Role	Last_accessed	Pass_modified
2009-06-07	Sparky	2834da08d58330d8dafbb2ac1c0f85f6b3b135ef	Admin	2011-09-12	2011-05-09
2010-06-03	Mark123	92e54f10103a3c511853c7098c04141f114719c1	user	2011-01-20	2010-06-03
2009-09-02	superman	437fbc6892b38db6ac5bdbe2eab3f7bc924527d9	user	2011-09-01	2011-01-01
2010-01-11	security	fafa4483874ec051989d53e1e432ba3a6c6b9143	user	2011-10-07	2010-01-11
2009-12-03	Tomtom	06f6fe0f73c6e197ee43eff4e5f7d10fb9e438b2	user	2011-10-03	2009-12-03
2010-04-11	JillC	f44f3b09df53c1c11273def13cacd8922a86d48c	user	2011-04-19	2010-12-20

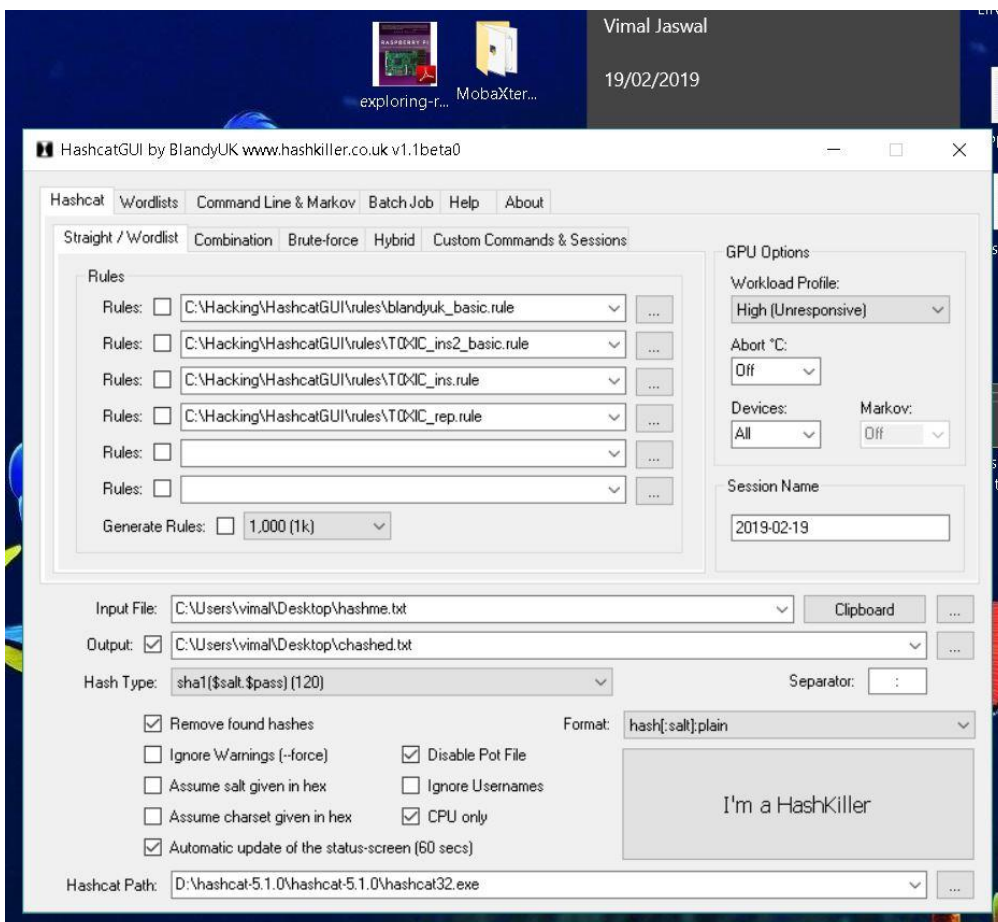
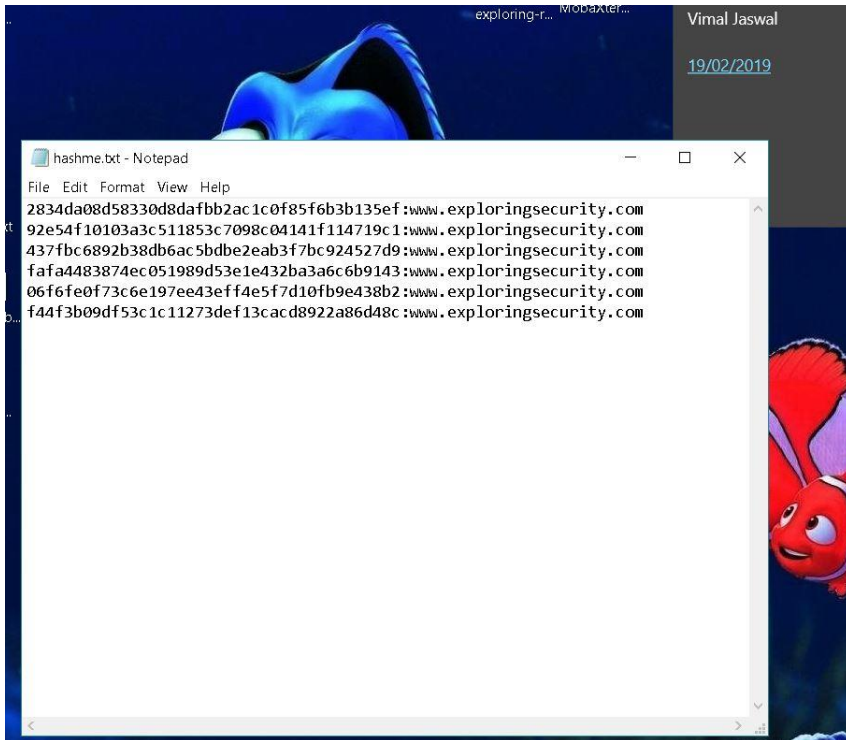
You should submit a detailed report outlining each step of your investigation including dead-ends and reasoning for each step along the way. Your report should be <1000 words. You should reference any materials, resources used separately.

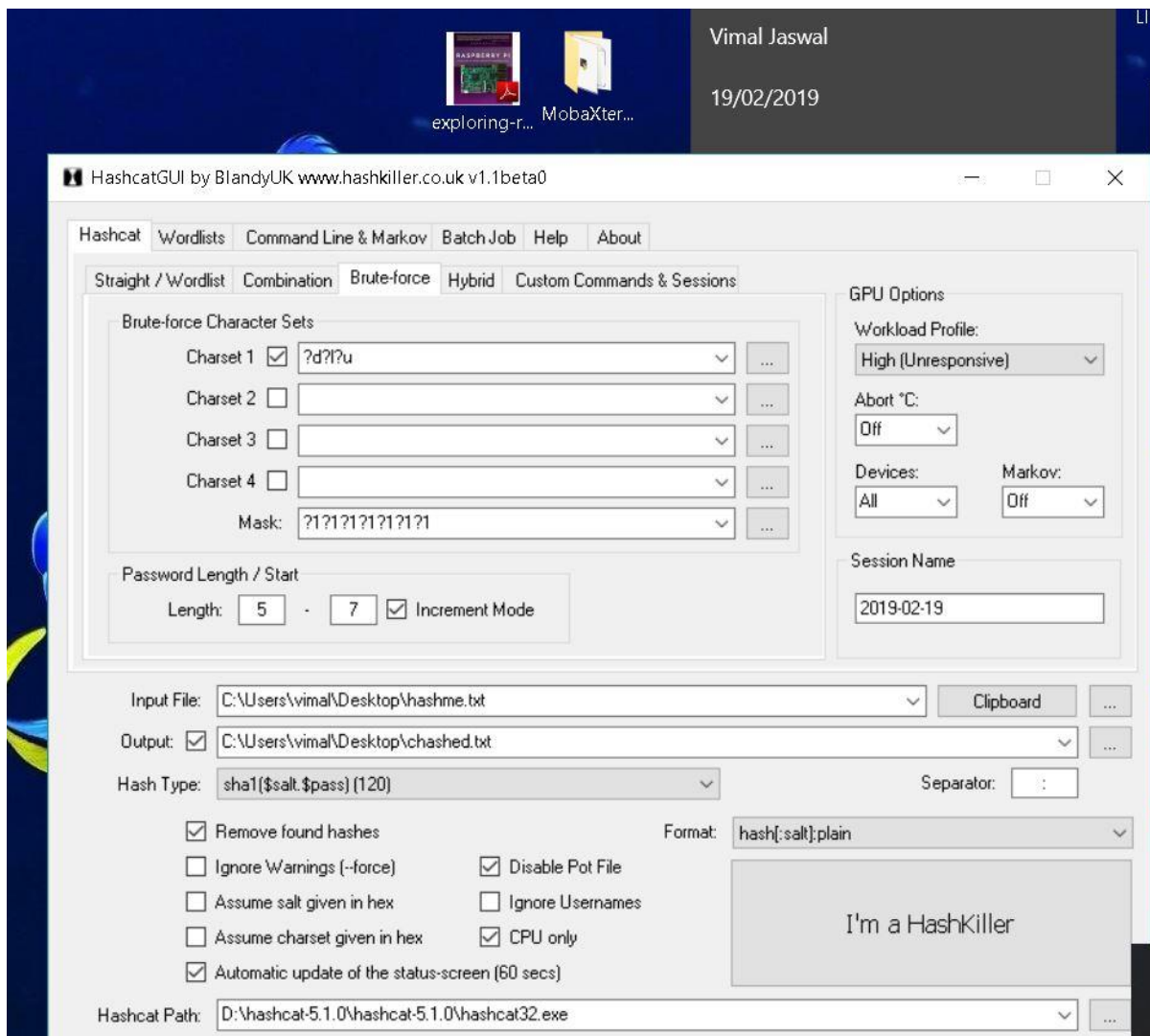
SOLUTION

Hashcat GUI and Binary both can be used to resolve hashes.

Hashcat GUI

Input file hashme.txt is used in hascat GUI with a blank text file chashed.txt for output. The input file contains hashes along with salt as shown below.



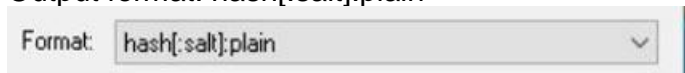


After setting input and output file paths in hashcatGUI I have set the

Hash type as----- sha1(\$salt, \$pass)



Output format: hash[:salt]:plain



I have used brute force method. Since the password may contain digits only, lowercase letters, uppercase letters or any mixed pattern as per given information

Therefore mask is set as ?d?l?u with maximum password length seven ?1?1?1?1?1?1?1

The brute force can be started from any digit but we know password length is between 5 – 7 characters so it is set as password length/start 5-7 with increment mode.

It means brute force will try to crack hash combinations from 5 characters and will run till maximum combinations of 7 characters. Disable pot file to run the software smoothly without warnings.

Now click on "I'm a hash killer" radio button. The hashcat will run it in command window with set instructions.



```
o... 2019-02-19 19:02:19 exploring-r... Vimal Jaswal TYPE ME.txt
hashcat (v5.1.0) starting...

* Device #1: Intel's OpenCL runtime (GPU only) is currently broken.
  We are waiting for updated OpenCL drivers from Intel.
  You can use --force to override, but do not report related errors.
OpenCL Platform #1: Intel(R) Corporation
=====
* Device #1: Intel(R) UHD Graphics 620, skipped.
* Device #2: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 511/511 MB allocatable, 8MCU

Hashes: 6 digests; 6 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Early-Skip
* Not-Iterated
* Single-Salt
* Brute-Force
* Raw-Hash

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Minimum salt length supported by kernel: 0
Maximum salt length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.
```

```
o... 2019-02-19 22:59:47-M... exploring-r... Mobaxter... Vimal Jaswal TYPE ME.txt
19/02/2019

C:\Windows\System32\cmd.exe - hashcat32.exe -a 3 --session=2019-02-19 -m 120 -w 3 -D 1 --status --status-timer=60 --potfile-disable --remove -...
Maximum salt length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: 2019-02-19
Status.....: Running
Hash.Type.....: sha1($salt.$pass)
Hash.Target....: C:\Users\vimal\Desktop\hashme.txt
Time.Started....: Tue Feb 19 20:03:27 2019 (6 secs)
Time.Estimated...: Tue Feb 19 20:03:41 2019 (8 secs)
Guess.Mask.....: ?1?1?1?1?1 [5]
Guess.Charset...: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 1/3 (33.33%)
Speed.#2.....: 67309.2 KH/s (5.81ms) @ Accel:1024 Loops:62 Thr:1 Vec:8
Recovered.....: 1/6 (16.67%) Digests, 0/1 (0.00%) Salts
Progress.....: 373309440/916132832 (40.75%)
Rejected.....: 0/373309440 (0.00%)
Restore.Point....: 6021120/14776336 (40.75%)
Restore.Sub.#2...: Salt:0 Amplifier:0-62 Iteration:0-62
Candidates.#2....: sPDH9 -> XZ4cf

Approaching final keyspace - workload adjusted.
```



```
2019-02-19 22:59:47-M... exploring-r... MobaXter... Vimal Jaswal 19/02/2019 TYPE ME.txt

C:\Windows\System32\cmd.exe - hashcat32.exe -a 3 --session=2019-02-19 -m 120 -w 3 -D 1 --status --status-timer=60 --potfile-disable --remove -...

Speed.#2.....: 67382.7 kH/s (5.79ms) @ Accel:1024 Loops:62 Thr:1 Vec:8
Recovered.....: 1/6 (16.67%) Digests, 0/1 (0.00%) Salts
Progress.....: 916132832/916132832 (100.00%)
Rejected.....: 0/916132832 (0.00%)
Restore.Point...: 14776336/14776336 (100.00%)
Restore.Sub.#2...: Salt:0 Amplifier:0-62 Iteration:0-62
Candidates.#2....: sRKvQ -> XQzFz
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: 2019-02-19
Status.....: Running
Hash.Type.....: sha1($salt.$pass)
Hash.Target....: C:\Users\vimal\Desktop\hashme.txt
Time.Started...: Tue Feb 19 20:03:41 2019 (46 secs)
Time.Estimated...: Tue Feb 19 20:13:29 2019 (9 mins, 2 secs)
Guess.Mask.....: ?1?1?1?1?1?1 [6]
Guess.Charset...: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 2/3 (66.67%)
Speed.#2.....: 96497.8 kH/s (80.77ms) @ Accel:1024 Loops:62 Thr:1 Vec:8
Recovered.....: 3/6 (50.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 4408606720/5680023584 (7.76%)
Rejected.....: 0/4408606720 (0.00%)
Restore.Point...: 1146880/14776336 (7.76%)
Restore.Sub.#2...: Salt:0 Amplifier:0-1024 Iteration:0-1024
Candidates.#2....: sae1GO -> 6b1vRT

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: 2019-02-19
Status.....: Running
```

```
2019-02-19 22:59:47-M... exploring-r... MobaXter... Vimal Jaswal 19/02/2019 TYPE ME.txt

C:\Windows\System32\cmd.exe - hashcat32.exe -a 3 --session=2019-02-19 -m 120 -w 3 -D 1 --status --status-timer=60 --potfile-disable --remove -...

Rejected.....: 0/4408606720 (0.00%)
Restore.Point...: 1146880/14776336 (7.76%)
Restore.Sub.#2...: Salt:0 Amplifier:0-1024 Iteration:0-1024
Candidates.#2....: sae1GO -> 6b1vRT

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: 2019-02-19
Status.....: Running
Hash.Type.....: sha1($salt.$pass)
Hash.Target....: C:\Users\vimal\Desktop\hashme.txt
Time.Started...: Tue Feb 19 20:03:41 2019 (48 secs)
Time.Estimated...: Tue Feb 19 20:13:30 2019 (9 mins, 1 sec)
Guess.Mask.....: ?1?1?1?1?1?1 [6]
Guess.Charset...: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 2/3 (66.67%)
Speed.#2.....: 96516.1 kH/s (80.82ms) @ Accel:1024 Loops:62 Thr:1 Vec:8
Recovered.....: 3/6 (50.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 4566056960/5680023584 (8.04%)
Rejected.....: 0/4566056960 (0.00%)
Restore.Point...: 1187840/14776336 (8.04%)
Restore.Sub.#2...: Salt:0 Amplifier:0-1024 Iteration:0-1024
Candidates.#2....: saMAqa -> 6bUGAM

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: 2019-02-19
Status.....: Running
Hash.Type.....: sha1($salt.$pass)
Hash.Target....: C:\Users\vimal\Desktop\hashme.txt
```

```
2019-02-19 22:59:47-M... exploring-r... MobaXter... Vimal Jaswal 19/02/2019 TYPE ME.txt

C:\Windows\System32\cmd.exe - hashcat32.exe -a 3 --session=2019-02-19 -m 120 -w 3 -D 1 --status --status-timer=60 --potfile-disable --remove -...

Guess.Charset.....: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 2/3 (66.67%)
Speed.#2.....: 94297.1 kH/s (82.06ms) @ Accel:1024 Loops:1024 Thr:1 Vec:8
Recovered.....: 3/6 (50.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 56800235584/56800235584 (100.00%)
Rejected.....: 0/56800235584 (0.00%)
Restore.Point.....: 14776336/14776336 (100.00%)
Restore.Sub.#2....: Salt:0 Amplifier:3072-3844 Iteration:0-1024
Candidates.#2.....: SjsSeXj -> XqQgXj

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: 2019-02-19
Status.....: Running
Hash.Type.....: sha1($salt.$pass)
Hash.Target.....: C:\Users\vimal\Desktop\hashme.txt
Time.Started.....: Tue Feb 19 20:13:52 2019 (54 secs)
Time.Estimated....: Wed Feb 20 06:33:17 2019 (10 hours, 18 mins)
Guess.Mask.....: ?l?l?l?l?l?l?l [7]
Guess.Charset.....: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 3/3 (100.00%)
Speed.#2.....: 94753.7 kH/s (88.41ms) @ Accel:1024 Loops:1024 Thr:1 Vec:8
Recovered.....: 4/6 (66.67%) Digests, 0/1 (0.00%) Salts
Progress.....: 5121114112/3521614606208 (0.15%)
Rejected.....: 0/5121114112 (0.00%)
Restore.Point.....: 16384/14776336 (0.11%)
Restore.Sub.#2....: Salt:0 Amplifier:148480-149504 Iteration:0-1024
Candidates.#2.....: IIMyrta -> wQsbk12

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>
```

```
2019-02-19 22:59:47-M... exploring-r... MobaXter... Vimal Jaswal 19/02/2019 TYPE ME.txt

C:\Windows\System32\cmd.exe - hashcat32.exe -a 3 --session=2019-02-19 -m 120 -w 3 -D 1 --status --status-timer=60 --potfile-disable --remove -...

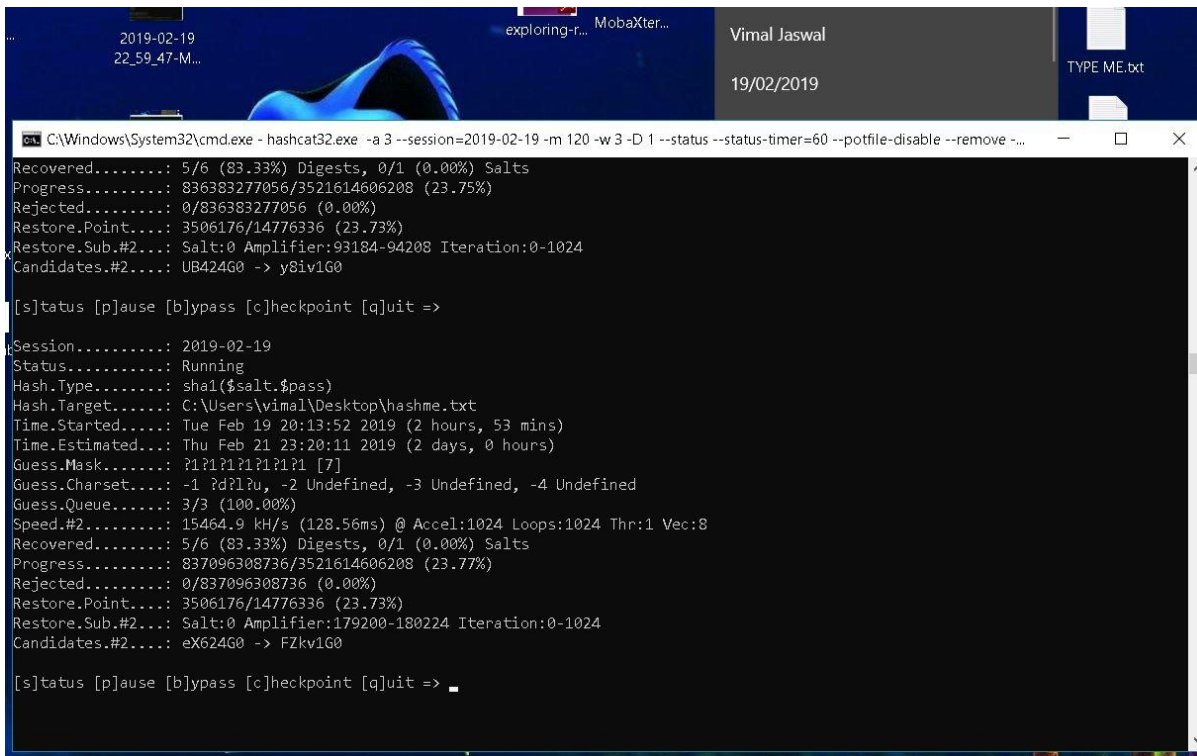
Speed.#2.....: 94038.1 kH/s (88.13ms) @ Accel:1024 Loops:1024 Thr:1 Vec:8
Recovered.....: 4/6 (66.67%) Digests, 0/1 (0.00%) Salts
Progress.....: 464308600832/3521614606208 (13.18%)
Rejected.....: 0/464308600832 (0.00%)
Restore.Point.....: 1941504/14776336 (13.14%)
Restore.Sub.#2....: Salt:0 Amplifier:193536-194560 Iteration:0-1024
Candidates.#2.....: SmTITS2 -> cOeSK27

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: 2019-02-19
Status.....: Running
Hash.Type.....: sha1($salt.$pass)
Hash.Target.....: C:\Users\vimal\Desktop\hashme.txt
Time.Started.....: Tue Feb 19 20:13:52 2019 (1 hour, 36 mins)
Time.Estimated....: Wed Feb 20 06:49:56 2019 (8 hours, 59 mins)
Guess.Mask.....: ?l?l?l?l?l?l?l [7]
Guess.Charset.....: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 3/3 (100.00%)
Speed.#2.....: 94189.9 kH/s (88.09ms) @ Accel:1024 Loops:1024 Thr:1 Vec:8
Recovered.....: 5/6 (83.33%) Digests, 0/1 (0.00%) Salts
Progress.....: 470216081408/3521614606208 (13.35%)
Rejected.....: 0/470216081408 (0.00%)
Restore.Point.....: 1966080/14776336 (13.31%)
Restore.Sub.#2....: Salt:0 Amplifier:199680-200704 Iteration:0-1024
Candidates.#2.....: qXLXRN -> jkOLOKU

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: 2019-02-19
```



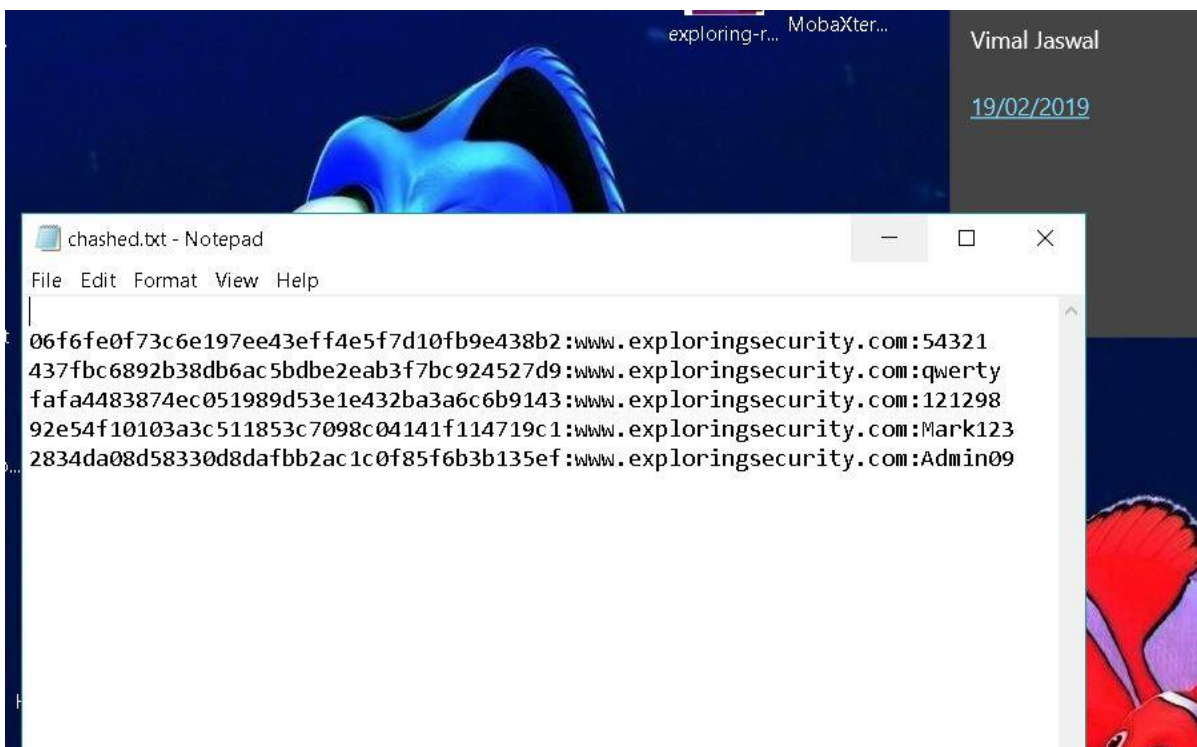
```
C:\Windows\System32\cmd.exe - hashcat32.exe -a 3 --session=2019-02-19 -m 120 -w 3 -D 1 --status --status-timer=60 --potfile-disable --remove -...
Recovered.....: 5/6 (83.33%) Digests, 0/1 (0.00%) Salts
Progress.....: 836383277056/3521614606208 (23.75%)
Rejected.....: 0/836383277056 (0.00%)
Restore.Point....: 3506176/14776336 (23.73%)
Restore.Sub.#2...: Salt:0 Amplifier:93184-94208 Iteration:0-1024
Candidates.#2....: UB424G0 -> y8iv1G0

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: 2019-02-19
Status.....: Running
Hash.Type.....: sha1($salt.$pass)
Hash.Target....: C:\Users\vimal\Desktop\hashme.txt
Time.Started....: Tue Feb 19 20:13:52 2019 (2 hours, 53 mins)
Time.Estimated...: Thu Feb 21 23:20:11 2019 (2 days, 0 hours)
Guess.Mask.....: ?1?1?1?1?1?1 [7]
Guess.Charset...: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue....: 3/3 (100.00%)
Speed.#2.....: 15464.9 kH/s (128.56ms) @ Accel:1024 Loops:1024 Thr:1 Vec:8
Recovered.....: 5/6 (83.33%) Digests, 0/1 (0.00%) Salts
Progress.....: 837096308736/3521614606208 (23.77%)
Rejected.....: 0/837096308736 (0.00%)
Restore.Point....: 3506176/14776336 (23.73%)
Restore.Sub.#2...: Salt:0 Amplifier:179200-180224 Iteration:0-1024
Candidates.#2....: eX624G0 -> FZkv1G0

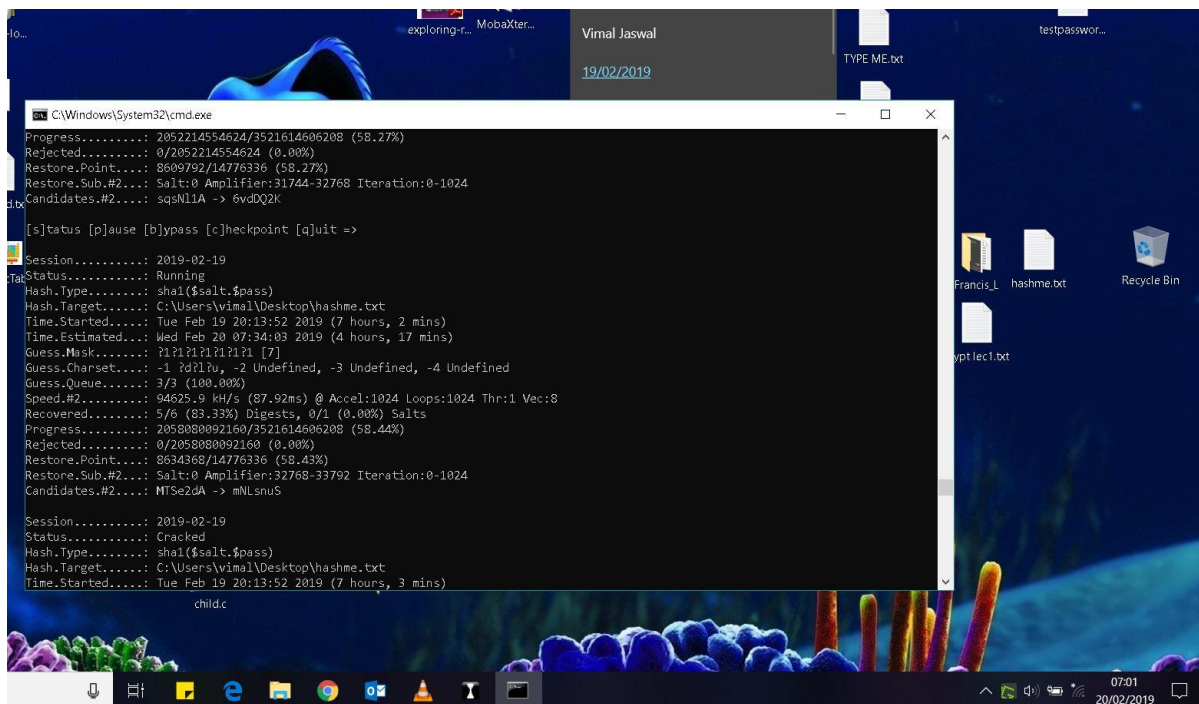
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => .
```

You can see the hashes cracked or recovered in chashed.txt output file. Below screenshot shows 5 resolved password. These five hashes has been recovered within three hours of time. The remaining one hash require long time time to run as per estimated time. You can pause and run the hashcat as per your convenience.



```
chashed.txt - Notepad
File Edit Format View Help

06f6fe0f73c6e197ee43eff4e5f7d10fb9e438b2:www.exploringsecurity.com:54321
437fbc6892b38db6ac5bdb2eab3f7bc924527d9:www.exploringsecurity.com:qwerty
fafa4483874ec051989d53e1e432ba3a6c6b9143:www.exploringsecurity.com:121298
92e54f10103a3c511853c7098c04141f114719c1:www.exploringsecurity.com:Mark123
2834da08d58330d8dafbb2ac1c0f85f6b3b135ef:www.exploringsecurity.com:Admin09
```

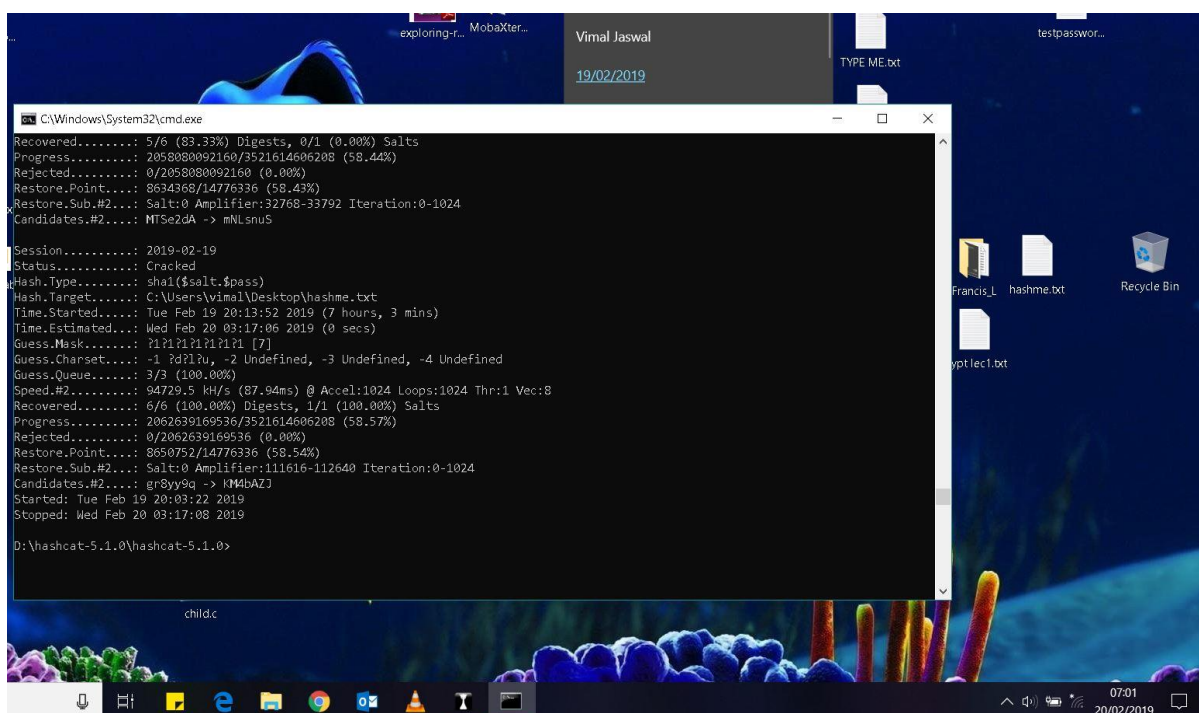
```
C:\Windows\System32\cmd.exe
Progress.....: 2052214554624/3521614606208 (58.27%)
Rejected.....: 0/2052214554624 (0.00%)
Restore.Point...: 8609792/14776336 (58.27%)
Restore.Sub.#2...: Salt:0 Amplifier:31744-32768 Iteration:0-1024
Candidates.#2....: sqsN11A -> 6vdDQ2K

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: 2019-02-19
Status.....: Running
Hash.Type.....: sha1($salt,$pass)
Hash.Target.....: C:\Users\vimal\Desktop\hashme.txt
Time.Started....: Tue Feb 19 20:13:52 2019 (7 hours, 2 mins)
Time.Estimated...: Wed Feb 20 07:34:03 2019 (4 hours, 17 mins)
Guess.Mask.....: ?1?1?1?1?1?1 [7]
Guess.Charset....: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 3/3 (100.00%)
Speed.#2.....: 94625.9 KH/s (87.92ms) @ Accel:1024 Loops:1024 Thr:1 Vec:8
Recovered.....: 5/6 (83.33%) Digests: 0/1 (0.00%) Salts
Progress.....: 2058080092160/3521614606208 (58.44%)
Rejected.....: 0/2058080092160 (0.00%)
Restore.Point...: 8634368/14776336 (58.43%)
Restore.Sub.#2...: Salt:0 Amplifier:32768-33792 Iteration:0-1024
Candidates.#2....: MTSe2dA -> mNLSnuS

Session.....: 2019-02-19
Status.....: Cracked
Hash.Type.....: sha1($salt,$pass)
Hash.Target.....: C:\Users\vimal\Desktop\hashme.txt
Time.Started....: Tue Feb 19 20:13:52 2019 (7 hours, 3 mins)

child.c
```



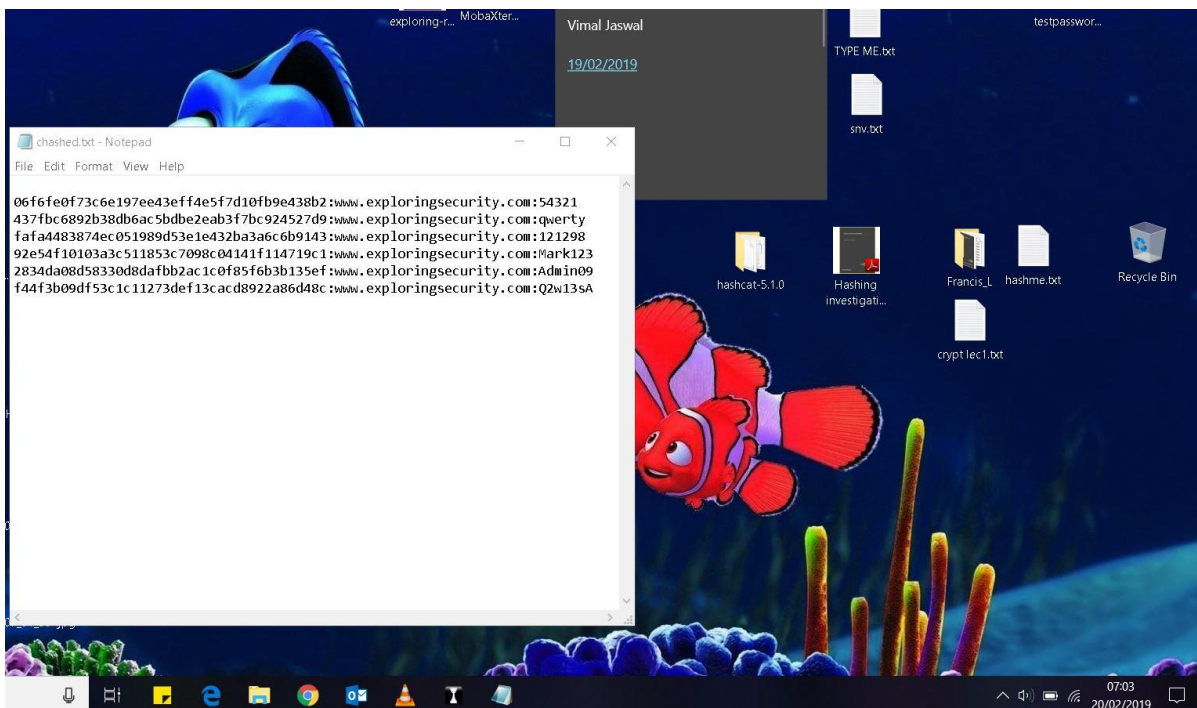
```
C:\Windows\System32\cmd.exe
Recovered.....: 5/6 (83.33%) Digests: 0/1 (0.00%) Salts
Progress.....: 2058080092160/3521614606208 (58.44%)
Rejected.....: 0/2058080092160 (0.00%)
Restore.Point...: 8634368/14776336 (58.43%)
Restore.Sub.#2...: Salt:0 Amplifier:32768-33792 Iteration:0-1024
Candidates.#2....: MTSe2dA -> mNLSnuS

Session.....: 2019-02-19
Status.....: Cracked
Hash.Type.....: sha1($salt,$pass)
Hash.Target.....: C:\Users\vimal\Desktop\hashme.txt
Time.Started....: Tue Feb 19 20:13:52 2019 (7 hours, 3 mins)
Time.Estimated...: Wed Feb 20 03:17:06 2019 (0 secs)
Guess.Mask.....: ?1?1?1?1?1?1 [7]
Guess.Charset....: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 3/3 (100.00%)
Speed.#2.....: 94729.5 KH/s (87.94ms) @ Accel:1024 Loops:1024 Thr:1 Vec:8
Recovered.....: 6/6 (100.00%) Digests: 1/1 (100.00%) Salts
Progress.....: 2062639169536/3521614606208 (58.57%)
Rejected.....: 0/2062639169536 (0.00%)
Restore.Point...: 8650752/14776336 (58.54%)
Restore.Sub.#2...: Salt:0 Amplifier:111616-112640 Iteration:0-1024
Candidates.#2....: gr8yy9q -> KM4bAZJ
Started: Tue Feb 19 20:03:22 2019
Stopped: Wed Feb 20 03:17:08 2019

D:\hashcat-5.1.0\hashcat-5.1.0>

child.c
```

It took 7 hours and 3 mins of time to crack all the hashes and results are available in chashed.txt file.



HASHCAT Through Command Line of Windows.

To run hashcat from command line we have to specify path for hascat32 or 64 bit.exe executable

and using the commands from hashcat `-help` we can specify the type of hash we want to recover like md5 or sha1 etc. `-m` is used to specify hash type.

Here the hash type is sha1 as length of hash is greater than 32 and the password is hashed with salt.

```
120 | sha1($salt.$pass) | Raw Hash, Salted and/or Iterated
```

`-a 3` represents the attack method is and 3 is for bruteforce method.

```
-1, --custom-charset1 | CS | User-defined charset ?l |
-1 ?l?d?u
```

`-1` is used to specify the password charset lowercase alphabets `?l`, digits `?d`, uppercase alphabets `?u`.

The input file name containing hashes along with predicted salts is used along with the mask specifying assumed length of password. In our case we already know its between 5-7 characters.

For mask of 5 characters:

```
hashcat-5.1.0
File Home Share View
Pin to Quick access Copy Paste Cut Copy path Move Copy Delete Rename New New item Easy access Properties Edit Select all Select none Invert selection
Select C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17134.590]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\vimal\Desktop\hashcat-5.1.0>hashcat64.exe -m 120 -a 3 -1 ?d hash.txt ?1?1?1?1?1
hashcat (v5.1.0) starting...

* Device #1: Intel's OpenCL runtime (GPU only) is currently broken.
  We are waiting for updated OpenCL drivers from Intel.
  You can use --force to override, but do not report related errors.
No devices found/left.

Started: Tue Feb 19 13:31:46 2019
Stopped: Tue Feb 19 13:31:46 2019

C:\Users\vimal\Desktop\hashcat-5.1.0>hashcat64.exe -m 120 --force -a 3 -1 ?d hash.txt ?1?1?1?1?1
hashcat (v5.1.0) starting...

OpenCL Platform #1: Intel(R) Corporation
=====
* Device #1: Intel(R) UHD Graphics 620, 2047/3219 MB allocatable, 24MCU
* Device #2: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, skipped.

Hashes: 4 digests; 4 unique digests, 4 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Early-Skip
* Not-Iterated
* Brute-Force

hashcat.dictstat2 05/02/2019 19:08 DICTSTAT2 File 1 KB
hashcat.hcstat2 02/12/2018 11:01 HCSTAT2 File 235 KB
```

```
hashcat-5.1.0
File Home Share View
Pin to Quick access Copy Paste Cut Copy path Move Copy Delete Rename New New item Easy access Properties Edit Select all Select none Invert selection
Select C:\Windows\System32\cmd.exe
Approaching final key space - workload adjusted.

06f6fe0f73c6e197ee43eff4e5f7d10fb9e438b2:www.exploringsecurity.com:54321

Session.....: hashcat
Status.....: Exhausted
Hash.Type.....: sha1($salt.$pass)
Hash.Target.....: hash.txt
Time.Started.....: Tue Feb 19 13:32:10 2019 (0 secs)
Time.Estimated...: Tue Feb 19 13:32:10 2019 (0 secs)
Guess.Mask.....: ?1?1?1?1?1 [5]
Guess.Charset....: -1 ?d, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 9178.6 kH/s (0.94ms) @ Accel:16 Loops:10 Thr:256 Vec:1
Recovered.....: 1/4 (25.00%) Digests, 1/4 (25.00%) Salts
Progress.....: 400000/400000 (100.00%)
Rejected.....: 0/400000 (0.00%)
Restore.Point....: 10000/10000 (100.00%)
Restore.Sub.#1...: Salt:3 Amplifier:0-10 Iteration:0-10
Candidates.#1...: 12345 -> 67646

Started: Tue Feb 19 13:32:07 2019
Stopped: Tue Feb 19 13:32:12 2019

C:\Users\vimal\Desktop\hashcat-5.1.0>
```

For mask of 6 characters

```
C:\Windows\System32\cmd.exe - hashcat64.exe -m 120 --force -a 3 -1 ?d?l?u hash.txt ?1?1?1?1?1?1

C:\Users\vimal\Desktop\hashcat-5.1.0>hashcat64.exe -m 120 --force -a 3 -1 ?d?l?u hash.txt ?1?1?1?1?1?1
hashcat (v5.1.0) starting...

OpenCL Platform #1: Intel(R) Corporation
=====
* Device #1: Intel(R) UHD Graphics 620, 2047/3219 MB allocatable, 24MCU
* Device #2: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, skipped.

Hashes: 6 digests; 6 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Early-Skip
* Not-Iterated
* Single-Salt
* Brute-Force
* Raw-Hash

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Minimum salt length supported by kernel: 0
Maximum salt length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
```

```
C:\Windows\System32\cmd.exe - hashcat64.exe -m 120 --force -a 3 -1 ?d?l?u hash.txt ?1?1?1?1?1?1

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

INFO: Removed 1 hash found in potfile.

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: hashcat
Status.....: Running
Hash.Type.....: sha1($salt.$pass)
Hash.Target.....: hash.txt
Time.Started....: Tue Feb 19 13:40:23 2019 (4 secs)
Time.Estimated...: Tue Feb 19 13:50:08 2019 (9 mins, 41 secs)
Guess.Mask.....: ?1?1?1?1?1?1 [6]
Guess.Charset....: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 97106.4 kH/s (6.73ms) @ Accel:16 Loops:8 Thr:256 Vec:1
Recovered.....: 1/6 (16.67%) Digests, 0/1 (0.00%) Salts
Progress.....: 367263744/56800235584 (0.65%)
Rejected.....: 0/367263744 (0.00%)
Restore.Point....: 0/14776336 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:3736-3744 Iteration:0-8
Candidates.#1....: gJnler -> 9Vz8he

437fbc6892b38db6ac5bdbe2eab3f7bc924527d9:www.exploringsecurity.com:qwerty
fafa4483874ec051989d53e1e432ba3a6c6b9143:www.exploringsecurity.com:121298
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>
```

Connect

Benji Rpi

C:\Windows\System32\cmd.exe - hashcat64.exe -m 120 --force -a 3 -1 ?d?l?u hash.txt ?1?1?1?1?1?

```

Progress.....: 367263744/56800235584 (0.65%)
Rejected.....: 0/367263744 (0.00%)
Restore.Point...: 0/14776336 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:3736-3744 Iteration:0-8
Candidates.#1...: gJnien -> 9Vz8he

437fbc6892b38db6ac5bdbe2eab3f7bc924527d9: www.exploringsecurity.com:qwerty
fafa4483874ec051989d53e1e432ba3a6c6b9143: www.exploringsecurity.com:121298
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: hashcat
Status.....: Running
Hash.Type.....: shal($salt.$pass)
Hash.Target....: hash.txt
Time.Started...: Tue Feb 19 13:40:23 2019 (2 mins, 59 secs)
Time.Estimated...: Tue Feb 19 13:50:46 2019 (7 mins, 24 secs)
Guess.Mask.....: ?1?1?1?1?1?1 [6]
Guess.Charset...: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 90228.3 kH/s (7.09ms) @ Accel:16 Loops:8 Thr:256 Vec:1
Recovered.....: 3/6 (50.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 16715612160/56800235584 (29.43%)
Rejected.....: 0/16715612160 (0.00%)
Restore.Point...: 4325376/14776336 (29.27%)
Restore.Sub.#1...: Salt:0 Amplifier:904-912 Iteration:0-8
Candidates.#1...: AAT161 -> PHIdxl

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>
  
```

Notepad+... Postman

2019-02-19 13:32:49-h...

```
C:\Windows\System32\cmd.exe
Restore.Point....: 14745600/14776336 (99.79%)
Restore.Sub.#1...: Salt:0 Amplifier:3840-3844 Iteration:0-8
Candidates.#1....: ZfMBwV -> XqbyWf

Session.....: hashcat
Status.....: Exhausted
Hash.Type.....: sha1($salt.$pass)
Hash.Target....: hash.txt
Time.Started...: Tue Feb 19 13:40:23 2019 (16 mins, 34 secs)
Time.Estimated...: Tue Feb 19 13:56:57 2019 (0 secs)
Guess.Mask.....: ?1?1?1?1?1?1 [6]
Guess.Charset...: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 5140.7 kH/s (2.15ms) @ Accel:16 Loops:8 Thr:256 Vec:1
Recovered.....: 3/6 (50.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 56800235584/56800235584 (100.00%)
Rejected.....: 0/56800235584 (0.00%)
Restore.Point....: 14776336/14776336 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:3840-3844 Iteration:0-8
Candidates.#1....: ZfdrPx -> XqQgXj

Started: Tue Feb 19 13:40:20 2019
Stopped: Tue Feb 19 13:56:58 2019

C:\Users\vimal\Desktop\hashcat-5.1.0>
```

For mask of 7 characters


```
Connect
C:\Windows\System32\cmd.exe - hashcat64.exe -m 120 --force -a 3 -1 ?d?l?u hash.txt ?1?1?1?1?1?1?1?1
Started: Tue Feb 19 13:40:20 2019
Stopped: Tue Feb 19 13:56:58 2019

C:\Users\vimal\Desktop\hashcat-5.1.0>hashcat64.exe -m 120 --force -a 3 -1 ?d?l?u hash.txt ?1?1?1?1?1?1?1?1
hashcat (v5.1.0) starting...

OpenCL Platform #1: Intel(R) Corporation
=====
* Device #1: Intel(R) UHD Graphics 620, 2047/3219 MB allocatable, 24MCU
* Device #2: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, skipped.

Hashes: 6 digests; 6 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Early-Skip
* Not-Iterated
* Single-Salt
* Brute-Force
* Raw-Hash

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Minimum salt length supported by kernel: 0
Maximum salt length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
```

```
Connect
C:\Windows\System32\cmd.exe - hashcat64.exe -m 120 --force -a 3 -1 ?d?l?u hash.txt ?1?1?1?1?1?1?1?1
* Not-Iterated
* Single-Salt
* Brute-Force
* Raw-Hash

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Minimum salt length supported by kernel: 0
Maximum salt length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

INFO: Removed 3 hashes found in potfile.

92e54f10103a3c511853c7098c04141f114719c1:www.exploringsecurity.com:Mark123
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => _
```

C:\Windows\System32\cmd.exe - hashcat64.exe -m 120 --force -a 3 -1 ?d?l?u hash.txt ?1?1?1?1?1?1

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

INFO: Removed 3 hashes found in potfile.

92e54f10103a3c511853c7098c04141f114719c1:www.exploringsecurity.com:Mark123
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: hashcat
Status.....: Running
Hash.Type.....: sha1(\$salt.\$pass)
Hash.Target.....: hash.txt
Time.Started....: Tue Feb 19 14:12:29 2019 (38 secs)
Time.Estimated...: Wed Feb 20 00:22:24 2019 (10 hours, 9 mins)
Guess.Mask.....: ?1?1?1?1?1?1 [7]
Guess.Charset....: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 96229.6 kH/s (6.74ms) @ Accel:16 Loops:8 Thr:256 Vec:1
Recovered.....: 4/6 (66.67%) Digests, 0/1 (0.00%) Salts
Progress.....: 3675783168/3521614606208 (0.10%)
Rejected.....: 0/3675783168 (0.00%)
Restore.Point....: 0/14776336 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:37384-37392 Iteration:0-8
Candidates.#1....: Uoueran -> aPTjq88

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

The screenshot shows a Windows 10 desktop with a blue background featuring a cartoon clownfish. A Windows Defender Firewall notification is visible in the top-left corner, indicating that Windows Defender Firewall is turned on and blocking an incoming connection from 'C:\Windows\System32\cmd.exe'. The notification includes buttons for 'Allow' and 'Block'. In the center of the screen, a black command prompt window is open, displaying the output of a hashcat command. The command is 'C:\Windows\System32\cmd.exe -hashcat64.exe -m 120 --force -a 3 -1 ?d?l?u hash.txt ?1?1?1?1?1?1'. The output shows progress, rejected hashes, and restored points. The desktop also has several icons: 'LINKS.docx', 'TYPE ME.txt', 'snw.txt', '5.1.0', 'Hashing investigati...', 'Notepad+...', 'Postman', and two folders named '2019-02-19' and '2019-02-19 13_32_49-h...'.

LINKS.docx

TYPE ME.txt

snw.txt

5.1.0

Hashing investigati...

Notepad+...

Postman

2019-02-19

2019-02-19 13_32_49-h...

2019-02-19 14_11_30-M...

Windows Defender Firewall

Windows Defender Firewall is turned on and blocking an incoming connection from C:\Windows\System32\cmd.exe.

Allow

Block

C:\Windows\System32\cmd.exe -hashcat64.exe -m 120 --force -a 3 -1 ?d?l?u hash.txt ?1?1?1?1?1?1

Progress.....: 10896801792/3521614606208 (0.31%)

Rejected.....: 0/10896801792 (0.00%)

Restore.Point....: 0/14776336 (0.00%)

Restore.Sub.#1...: Salt:0 Amplifier:110848-110856 Iteration:0-8

Candidates.#1....: Wk7eran -> Xk7jq88

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session.....: hashcat

Status.....: Running

Hash.Type.....: sha1(\$salt.\$pass)

Hash.Target.....: hash.txt

Time.Started....: Tue Feb 19 14:12:29 2019 (17 mins, 53 secs)

Time.Estimated...: Wed Feb 20 00:40:35 2019 (10 hours, 10 mins)

Guess.Mask.....: ?1?1?1?1?1?1 [7]

Guess.Charset....: -1 ?d?l?u, -2 Undefined, -3 Undefined, -4 Undefined

Guess.Queue.....: 1/1 (100.00%)

Speed.#1.....: 93437.1 KH/s (6.97ms) @ Accel:16 Loops:8 Thr:256 Vec:1

Recovered.....: 4/6 (66.67%) Digests, 0/1 (0.00%) Salts

Progress.....: 100600381440/3521614606208 (2.86%)

Rejected.....: 0/100600381440 (0.00%)

Restore.Point....: 393216/14776336 (2.66%)

Restore.Sub.#1...: Salt:0 Amplifier:70040-70048 Iteration:0-8

Candidates.#1....: DYfD0LA -> HH2Dkyn

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>