



Proyecto III

HASHCAT

Criptografía y Seguridad 2021-1

Profesor: Manuel Díaz Díaz
Ayudante: Gerardo Rubén López Hernández
Ayudante: Jesús Lara Arellano
Laboratorista: José Canek García Aguilar

Licenciatura en Ciencias de la Computación Facultad de Ciencias, UNAM

Alumnos:
Jorge Iván Pérez Pérez 314211349
Dafne Michel Miranda Salazar 314212597

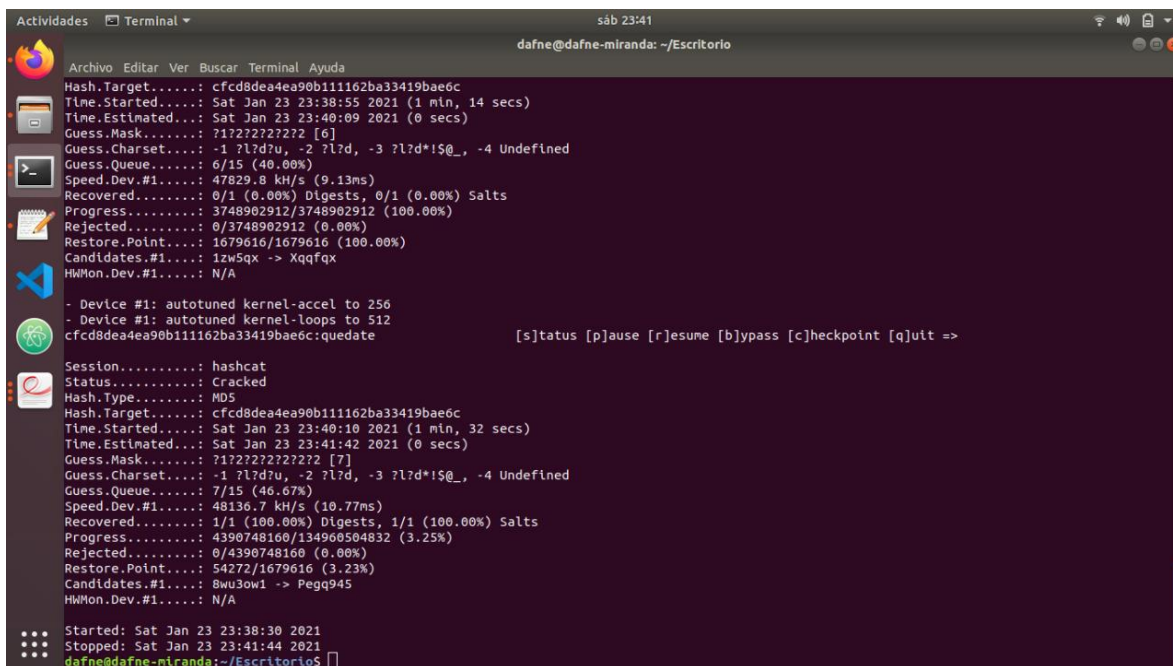
Se utilizo la herramienta HASHCAT para poder recuperar el valor original de los siguientes hashes md5:

- cfcd8dea4ea90b111162ba33419bae6c
- 9cfefed8fb9497baa5cd519d7d2bb5d7
- 202447d5d44ce12531f7207cb33b6bf7
- 7cf41ff971d626b865524717448c298a
- 047fb90408a79f189d51cbcea168b1a5

OBSERVACION: Por alguna razón en una de las computadoras de los integrantes del equipo no fue posible ejecutar la herramienta ya que salían errores como *device #1 unstable openc1 driver detected*, fue probado tanto en Ubuntu como en Windows sin éxito.

RECUPERACIÓN DE HASHES

- cfcd8dea4ea90b111162ba33419bae6c -> **quedate**



```
Actividades Terminal sáb 23:41
dafne@dafne-miranda: ~/Escritorio

Hash.Target.....: cfcd8dea4ea90b111162ba33419bae6c
Time.Started.....: Sat Jan 23 23:38:55 2021 (1 min, 14 secs)
Time.Estimated....: Sat Jan 23 23:40:09 2021 (0 secs)
Guess.Mask.....: 717272727272 [6]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 6/15 (40.00%)
Speed.Dev.#1.....: 47829.8 kH/s (9.13ms)
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 3748902912/3748902912 (100.00%)
Rejected.....: 0/3748902912 (0.00%)
Restore.Point....: 1679616/1679616 (100.00%)
Candidates.#1....: 1zw5qx -> Xqqfqx
HWMon.Dev.#1....: N/A

- Device #1: autotuned kernel-accel to 256
- Device #1: autotuned kernel-loops to 512
cfcd8dea4ea90b111162ba33419bae6c:quedate [s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: MD5
Hash.Target.....: cfcd8dea4ea90b111162ba33419bae6c
Time.Started.....: Sat Jan 23 23:40:10 2021 (1 min, 32 secs)
Time.Estimated....: Sat Jan 23 23:41:42 2021 (0 secs)
Guess.Mask.....: 717272727272 [7]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 7/15 (46.67%)
Speed.Dev.#1.....: 48136.7 kH/s (10.77ms)
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 4390748160/134960504832 (3.25%)
Rejected.....: 0/4390748160 (0.00%)
Restore.Point....: 54272/1679616 (3.23%)
Candidates.#1....: 8wu3ow1 -> Pegq945
HWMon.Dev.#1....: N/A

Started: Sat Jan 23 23:38:30 2021
Stopped: Sat Jan 23 23:41:44 2021
dafne@dafne-miranda:~/Escritorio$
```

- 9cfefed8fb9497baa5cd519d7d2bb5d7 -> en

```

Actividades Terminal sáb 23:49
dafne@dafne-miranda: ~/Escritorio

Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 62/62 (100.00%)
Rejected.....: 0/62 (0.00%)
Restore.Point...: 1/1 (100.00%)
Candidates.#1...: 6 -> X
HWMon.Dev.#1...: N/A

- Device #1: autotuned kernel-accel to 1024
- Device #1: autotuned kernel-loops to 31
[s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit => The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

9cfefed8fb9497baa5cd519d7d2bb5d7:en

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: MD5
Hash.Target.....: 9cfefed8fb9497baa5cd519d7d2bb5d7
Time.Started....: Sat Jan 23 23:48:59 2021 (0 secs)
Time.Estimated...: Sat Jan 23 23:48:59 2021 (0 secs)
Guess.Mask.....: ?1?2 [2]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 2/15 (13.33%)
Speed.Dev.#1....: 10488 H/s (0.04ms)
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 1116/2232 (50.00%)
Rejected.....: 0/1116 (0.00%)
Restore.Point...: 0/36 (0.00%)
Candidates.#1...: sa -> 7q
HWMon.Dev.#1...: N/A

Started: Sat Jan 23 23:48:53 2021
Stopped: Sat Jan 23 23:49:01 2021
dafne@dafne-miranda:~/Escritorio$

```

- 202447d5d44ce12531f7207cb33b6bf7 -> casa

```

Actividades Terminal sáb 23:50
dafne@dafne-miranda: ~/Escritorio

Hash.Target.....: 202447d5d44ce12531f7207cb33b6bf7
Time.Started....: Sat Jan 23 23:50:21 2021 (0 secs)
Time.Estimated...: Sat Jan 23 23:50:21 2021 (0 secs)
Guess.Mask.....: ?1?2?2 [3]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 3/15 (20.00%)
Speed.Dev.#1....: 807.0 kH/s (0.73ms)
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 80352/80352 (100.00%)
Rejected.....: 0/80352 (0.00%)
Restore.Point...: 1296/1296 (100.00%)
Candidates.#1...: 6ar -> Xqx
HWMon.Dev.#1...: N/A

- Device #1: autotuned kernel-accel to 1024
- Device #1: autotuned kernel-loops to 31
202447d5d44ce12531f7207cb33b6bf7:casa [s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: MD5
Hash.Target.....: 202447d5d44ce12531f7207cb33b6bf7
Time.Started....: Sat Jan 23 23:50:21 2021 (0 secs)
Time.Estimated...: Sat Jan 23 23:50:21 2021 (0 secs)
Guess.Mask.....: ?1?2?2?2 [4]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 4/15 (26.67%)
Speed.Dev.#1....: 3707.5 kH/s (2.28ms)
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 380928/2892672 (13.17%)
Rejected.....: 0/380928 (0.00%)
Restore.Point...: 4006/46656 (8.78%)
Candidates.#1...: skue -> 7sok
HWMon.Dev.#1...: N/A

Started: Sat Jan 23 23:50:19 2021
Stopped: Sat Jan 23 23:50:23 2021
dafne@dafne-miranda:~/Escritorio$

```

- 7cf41ff971d626b865524717448c298a -> por

```

Actividades Terminal sáb 23:51
dafne@dafne-miranda: ~/Escritorio

Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 2232/2232 (100.00%)
Rejected.....: 0/2232 (0.00%)
Restore.Point....: 36/36 (100.00%)
Candidates.#1....: 6a -> Xq
HWMon.Dev.#1....: N/A

- Device #1: autotuned kernel-accel to 1024
- Device #1: autotuned kernel-loops to 31
[s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit => The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keypace - workload adjusted.

7cf41ff971d626b865524717448c298a:por

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: MD5
Hash.Target.....: 7cf41ff971d626b865524717448c298a
Time.Started....: Sat Jan 23 23:51:14 2021 (0 secs)
Time.Estimated...: Sat Jan 23 23:51:14 2021 (0 secs)
Guess.Mask.....: ?1?2?2 [3]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 3/15 (20.00%)
Speed.Dev.#1....: 395.7 kH/s (0.72ms)
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 40176/80352 (50.00%)
Rejected.....: 0/40176 (0.00%)
Restore.Point....: 0/1296 (0.00%)
Candidates.#1....: sar -> 7qx
HWMon.Dev.#1....: N/A

Started: Sat Jan 23 23:51:12 2021
Stopped: Sat Jan 23 23:51:16 2021
dafne@dafne-miranda:~/Escritorio$

```

- 047fb90408a79f189d51cbcea168b1a5 -> favor

```

Actividades Terminal sáb 23:51
dafne@dafne-miranda: ~/Escritorio

Hash.Target.....: 047fb90408a79f189d51cbcea168b1a5
Time.Started....: Sat Jan 23 23:51:52 2021 (0 secs)
Time.Estimated...: Sat Jan 23 23:51:52 2021 (0 secs)
Guess.Mask.....: ?1?2?2?2 [4]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 4/15 (26.67%)
Speed.Dev.#1....: 18128.6 kH/s (2.32ms)
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 2892672/2892672 (100.00%)
Rejected.....: 0/2892672 (0.00%)
Restore.Point....: 46656/46656 (100.00%)
Candidates.#1....: 67kx -> Xqxv
HWMon.Dev.#1....: N/A

- Device #1: autotuned kernel-accel to 1024
- Device #1: autotuned kernel-loops to 31
047fb90408a79f189d51cbcea168b1a5:favor [s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: MD5
Hash.Target.....: 047fb90408a79f189d51cbcea168b1a5
Time.Started....: Sat Jan 23 23:51:52 2021 (0 secs)
Time.Estimated...: Sat Jan 23 23:51:52 2021 (0 secs)
Guess.Mask.....: ?1?2?2?2?2 [5]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 5/15 (33.33%)
Speed.Dev.#1....: 26974.3 kH/s (2.42ms)
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 5967872/104136192 (5.73%)
Rejected.....: 0/5967872 (0.00%)
Restore.Point....: 94208/1679616 (5.61%)
Candidates.#1....: sfjal -> 7c722
HWMon.Dev.#1....: N/A

Started: Sat Jan 23 23:51:48 2021
Stopped: Sat Jan 23 23:51:54 2021
dafne@dafne-miranda:~/Escritorio$

```