Practica 6 - Introducción a la auditoria de contraseñas

Adrián Anchuela Villoldo – Puesto 5

Estamos empleando los archivos de hashes 5 y 14: raw-md5.hashes5.txt y raw-md5.hashes14.txt
Trabajaremos con 2 diccionarios distintos: passwords.txt y 500_passwords.txt
Mas un diccionario adicional para el ataque hibrido: hybriddic.txt

## Ataque STRAIGHT

Primero probaremos un ataque Straight sobre ambos archivos de hashes.

```
┌──(slagged㉿kali-linux-2021-3)-[~/Documents/Practica6]
└─$ hashcat -m 0 -a 0 raw-md5.hashes5.txt passwords.txt 500_passwords.txt --potfile-disable
hashcat (v6.1.1) starting ...

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 9.0.1, SLEEF, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================
* Device #1: pthread-0×000, 1421/1485 MB (512 MB allocatable), 2MCU

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

```
Session..........: hashcat
Status...........: Exhausted
Hash.Name........: MD5
Hash.Target......: raw-md5.hashes5.txt
Time.Started.....: Tue May 10 21:25:36 2022 (0 secs)
Time.Estimated ...: Tue May 10 21:25:36 2022 (0 secs)
Guess.Base.......: File (500_passwords.txt)
Guess.Queue......: 2/2 (100.00%)
Speed.#1.........:  1964.1 kH/s (0.11ms) @ Accel:1024 Loops:1 Thr:1 Vec:4
Recovered........: 26/3500000 (0.00%) Digests
Remaining........: 3499974 (100.00%) Digests
Recovered/Time ...: CUR:N/A,N/A,N/A AVG:106682,6400711,153611333 (Min,Hour,Day)
Progress.........: 502/502 (100.00%)
Rejected.........: 0/502 (0.00%)
Restore.Point....: 502/502 (100.00%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: 123456 → albert

Started: Tue May 10 21:25:31 2022
Stopped: Tue May 10 21:25:38 2022
```

```
Session..........: hashcat
Status...........: Exhausted
Hash.Name........: MD5
Hash.Target......: raw-md5.hashes14.txt
Time.Started.....: Tue May 10 21:31:19 2022 (0 secs)
Time.Estimated ...: Tue May 10 21:31:19 2022 (0 secs)
Guess.Base.......: File (500_passwords.txt)
Guess.Queue......: 2/2 (100.00%)
Speed.#1.........:  1770.5 kH/s (0.09ms) @ Accel:1024 Loops:1 Thr:1 Vec:4
Recovered........: 21/3500000 (0.00%) Digests
Remaining........: 3499979 (100.00%) Digests
Recovered/Time ...: CUR:N/A,N/A,N/A AVG:0,0,0 (Min,Hour,Day)
Progress.........: 502/502 (100.00%)
Rejected.........: 0/502 (0.00%)
Restore.Point....: 502/502 (100.00%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: 123456 → albert

Started: Tue May 10 21:31:14 2022
Stopped: Tue May 10 21:31:21 2022
```

Logrando recuperar un total de 47 contraseñas.

En un tiempo aproximado de 7 segundos por cada archivo de hashes.

Podemos mejorar el ataque Straight utilizando reglas localizadas en el sistema.
En este caso vamos a emplear la regla Combinator.rule.

```
┌──(slagged㉿kali-linux-2021-3)-[~/Documents/Practica6]
└─$ hashcat -m 0 -a 0 raw-md5.hashes5.txt passwords.txt 500_passwords.txt -r /usr/share/hashcat/rules/combinator.rule --potfile-d
isable
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 9.0.1, SLEEF, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================
* Device #1: pthread-0×000, 1421/1485 MB (512 MB allocatable), 2MCU

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

La cual nos va a permitir obtener resultados bastante mejores que sin el uso de reglas.

```
Session..........: hashcat
Status...........: Exhausted
Hash.Name........: MD5
Hash.Target......: raw-md5.hashes5.txt
Time.Started.....: Tue May 10 23:01:25 2022 (0 secs)
Time.Estimated...: Tue May 10 23:01:25 2022 (0 secs)
Guess.Base.......: File (500_passwords.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/combinator.rule)
Guess.Queue......: 2/2 (100.00%)
Speed.#1.........: 10001.5 kH/s (1.85ms) @ Accel:1024 Loops:40 Thr:1 Vec:4
Recovered........: 315/3500000 (0.01%) Digests
Remaining........: 3499685 (99.99%) Digests
Recovered/Time...: CUR:N/A,N/A,N/A AVG:239570,14374069,344974257 (Min,Hour,Day)
Progress.........: 20080/20080 (100.00%)
Rejected.........: 0/20080 (0.00%)
Restore.Point....: 502/502 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-40 Iteration:0-40
Candidates.#1....: 123456 → albert

Started: Tue May 10 23:01:20 2022
Stopped: Tue May 10 23:01:27 2022
```

```
Session..........: hashcat
Status...........: Exhausted
Hash.Name........: MD5
Hash.Target......: raw-md5.hashes14.txt
Time.Started.....: Tue May 10 23:03:54 2022 (0 secs)
Time.Estimated...: Tue May 10 23:03:54 2022 (0 secs)
Guess.Base.......: File (500_passwords.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/combinator.rule)
Guess.Queue......: 2/2 (100.00%)
Speed.#1.........:  6721.3 kH/s (2.82ms) @ Accel:1024 Loops:40 Thr:1 Vec:4
Recovered........: 305/3500000 (0.01%) Digests
Remaining........: 3499695 (99.99%) Digests
Recovered/Time...: CUR:N/A,N/A,N/A AVG:131539,7892284,189413080 (Min,Hour,Day)
Progress.........: 20080/20080 (100.00%)
Rejected.........: 0/20080 (0.00%)
Restore.Point....: 502/502 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-40 Iteration:0-40
Candidates.#1....: 123456 → albert

Started: Tue May 10 23:03:50 2022
Stopped: Tue May 10 23:03:56 2022
```

Capturando así por el mismo tipo de ataque 620 contraseñas frente a las 47 anteriores.
Con un tiempo empleado de 7 segundos por cada archivo de hashes lo cual nos da un rendimiento mucho mayor en el mismo periodo de tiempo.

## Ataque HIBRIDO

Para el ataque hibrido hemos creado un diccionario con algunas de las contraseñas más utilizadas. (password, admin, qwerty, qwaszx, dog, cat, sky, tree, house ,lock, root, user).
Para hacer que acierte lo máximo posible le añadimos “?a?a?a?a” para la mascara.

l | abcdefghijklmnopqrstuvwxyz
u | ABCDEFGHIJKLMNOPQRSTUVWXYZ
d | 0123456789
s | !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
a | ?l?u?d?s

Lo cual significa que introduciremos detrás de cada palabra de nuestro diccionario una permutación de 4 posiciones.

```
┌──(slagged㉿kali-linux-2021-3)-[~/Documents/Practica6]
└─$ hashcat -m 0 -a 6 -o atthybrid1.txt raw-md5.hashes5.txt hybriddic.txt ?a?a?a?a --potfile-disable
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 9.0.1, SLEEF, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================
* Device #1: pthread-0×000, 1421/1485 MB (512 MB allocatable), 2MCU

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

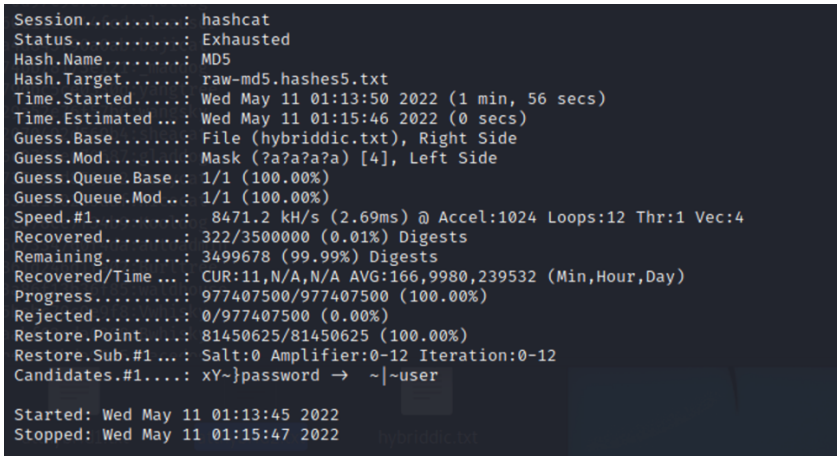
Haremos lo mismo para ambos archivos de hashes (5 y 14)

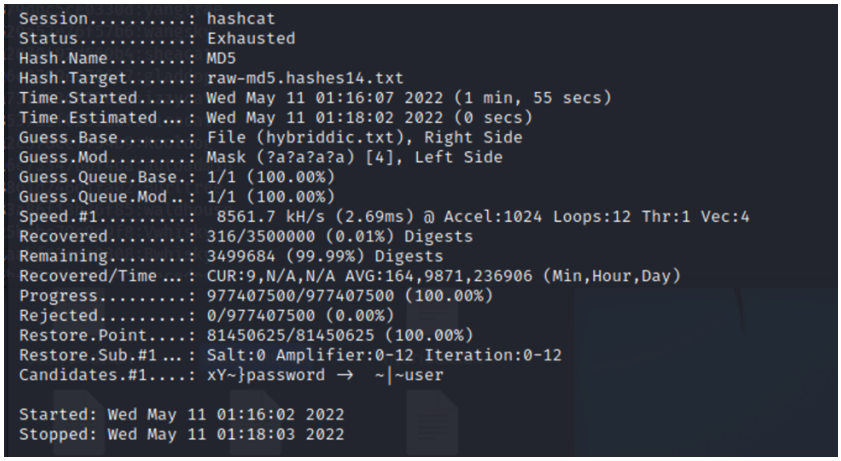
```
Session..........: hashcat
Status...........: Exhausted
Hash.Name........: MD5
Hash.Target......: raw-md5.hashes5.txt
Time.Started.....: Wed May 11 00:37:18 2022 (2 mins, 5 secs)
Time.Estimated...: Wed May 11 00:39:23 2022 (0 secs)
Guess.Base.......: File (hybriddic.txt), Left Side
Guess.Mod........: Mask (?a?a?a?a) [4], Right Side
Guess.Queue.Base.: 1/1 (100.00%)
Guess.Queue.Mod..: 1/1 (100.00%)
Speed.#1.........:  7892.0 kH/s (1.42ms) @ Accel:64 Loops:1024 Thr:1 Vec:4
Recovered........: 403/3500000 (0.01%) Digests
Remaining........: 3499597 (99.99%) Digests
Recovered/Time...: CUR:7,N/A,N/A AVG:193,11628,279077 (Min,Hour,Day)
Progress.........: 977407500/977407500 (100.00%)
Rejected.........: 0/977407500 (0.00%)
Restore.Point....: 12/12 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:81449984-81450625 Iteration:0-1024
Candidates.#1....: passwordv:~} → user ~|~

Started: Wed May 11 00:37:13 2022
Stopped: Wed May 11 00:39:24 2022
```

Hemos recuperado un total de 403 contraseñas en un total de 2 minutos 11 segundos

```
Session..........: hashcat
Status...........: Exhausted
Hash.Name........: MD5
Hash.Target......: raw-md5.hashes14.txt
Time.Started.....: Wed May 11 00:53:26 2022 (2 mins, 31 secs)
Time.Estimated...: Wed May 11 00:55:57 2022 (0 secs)
Guess.Base.......: File (hybriddic.txt), Left Side
Guess.Mod........: Mask (?a?a?a?a) [4], Right Side
Guess.Queue.Base.: 1/1 (100.00%)
Guess.Queue.Mod..: 1/1 (100.00%)
Speed.#1.........:  6606.7 kH/s (0.36ms) @ Accel:256 Loops:256 Thr:1 Vec:4
Recovered........: 400/3500000 (0.01%) Digests
Remaining........: 3499600 (99.99%) Digests
Recovered/Time...: CUR:7,N/A,N/A AVG:159,9581,229963 (Min,Hour,Day)
Progress.........: 977407500/977407500 (100.00%)
Rejected.........: 0/977407500 (0.00%)
Restore.Point....: 12/12 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:81450496-81450625 Iteration:0-256
Candidates.#1....: password@]~} → user ~|~

Started: Wed May 11 00:53:21 2022
Stopped: Wed May 11 00:55:58 2022
```

| Ataque hibrido a la derecha “?a?a?a?a” | |
|---|---|
| Orden | hashcat -m 0 -a 6 -o atthybrid1.txt raw-md5.hashes5.txt hybriddic.txt ?a?a?a?a |
| Contraseñas recuperadas | 803 contraseñas en un total de 6 minutos 48 segundos |
| Resumen | Se crea un diccionario de contraseñas posibles (hybriddic.txt) |
| Muestras | Password1523, lock1922, housegirl, catguTs |
| Esfuerzo | 7000 kH/s aprox |




| Ataque hibrido a la izquierda “?a?a?a?a” | |
|---|---|
| Orden | hashcat -m 0 -a 7 -o atthybrid1.txt raw-md5.hashes5.txt ?a?a?a?a hybriddic.txt |
| Contraseñas recuperadas | 638 contraseñas en un total de 4 minutos 3 segundos |
| Resumen | Se crea un diccionario de contraseñas posibles (hybriddic.txt) |
| Muestras | six@admin, cocosky, 1301house, izzycat |
| Esfuerzo | 8500 kH/s aprox |

## Ataque COMBINATION

Este ataque el cual probablemente dé el mejor resultado se basa en que cada palabra de nuestro diccionario se unirá a cada una de las palabras de este, se puede usar más de 1.
En caso de solo tener un diccionario se seleccionará dos veces el mismo.

Emplearemos la orden:

```
┌──(slagged㉿kali-linux-2021-3)-[~/Documents/Practica6]
└─$ hashcat -m 0 -a 1 -o combatt1.txt raw-md5.hashes5.txt passwords.txt 500_passwords.txt --potfile-disable
hashcat (v6.1.1) starting ...
```

Obteniendo el mejor resultado hasta ahora en un tiempo muy inferior a las anteriores.

```
Session..........: hashcat
Status...........: Exhausted
Hash.Name........: MD5
Hash.Target......: raw-md5.hashes5.txt
Time.Started.....: Wed May 11 01:50:32 2022 (1 sec)
Time.Estimated...: Wed May 11 01:50:33 2022 (0 secs)
Guess.Base.......: File (passwords.txt), Left Side
Guess.Mod........: File (500_passwords.txt), Right Side
Speed.#1.........:  1753.8 kH/s (13.13ms) @ Accel:256 Loops:251 Thr:1 Vec:4
Recovered........: 9910/3500000 (0.28%) Digests
Remaining........: 3490090 (99.72%) Digests
Recovered/Time...: CUR:N/A,N/A,N/A AVG:877159,52629579,1263109833 (Min,Hour,Day)
Progress.........: 1151086/1151086 (100.00%)
Rejected.........: 0/1151086 (0.00%)
Restore.Point....: 2293/2293 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:251-502 Iteration:0-251
Candidates.#1....: jimbo2112 → dictumalbert

Started: Wed May 11 01:50:28 2022
Stopped: Wed May 11 01:50:34 2022
```

Hemos recuperado 9910 contraseñas de un solo archivo de hashes.
En un tiempo de 6 segundos.
Con un esfuerzo de 1753 kH/s.
En las muestras podemos encontrar como se ha hecho: passworddiamond (uniendo dos posibles contraseñas de los diccionarios.)

```
Session..........: hashcat
Status...........: Exhausted
Hash.Name........: MD5
Hash.Target......: raw-md5.hashes14.txt
Time.Started.....: Wed May 11 02:14:59 2022 (1 sec)
Time.Estimated...: Wed May 11 02:15:00 2022 (0 secs)
Guess.Base.......: File (passwords.txt), Left Side
Guess.Mod........: File (500_passwords.txt), Right Side
Speed.#1.........:  2583.7 kH/s (14.58ms) @ Accel:256 Loops:251 Thr:1 Vec:4
Recovered........: 9970/3500000 (0.28%) Digests
Remaining........: 3490030 (99.72%) Digests
Recovered/Time...: CUR:N/A,N/A,N/A AVG:1300989,78059375,1873424837 (Min,Hour,Day)
Progress.........: 1151086/1151086 (100.00%)
Rejected.........: 0/1151086 (0.00%)
Restore.Point....: 2293/2293 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:251-502 Iteration:0-251
Candidates.#1....: jimbo2112 → dictumalbert

Started: Wed May 11 02:14:55 2022
Stopped: Wed May 11 02:15:01 2022
```

Juntando ambos archivos damos con la cantidad de 19880 contraseñas capturadas.

**Bibliografia:**

https://www.youtube.com/watch?v=m0AGSO1LDJs

https://www.securityartwork.es/2017/02/15/cracking-contrasenas-hashcat/#:~:text=Hashcat%20dispone%20de%20dos%20variantes,al%20inicio%20de%20cada%20termino

https://www.youtube.com/watch?v=-CQcWxrdbnc