Crack de Hash

Herramientas

- **Identificadores de Hashes:** hash-identifier (Kali), Hash-identifier online
- **hashcat**

```
sudo apt install hashcat
```

  - Lista de tipos de hashes

- **John the Ripper**

Empezando con el cracking

1. **48bb6e862e54f2a795ffc4e541caed4d** --> easy (MD5)

   ```
   hashcat -a 0 -m 0 hash1.txt /usr/share/wordlists/rockyou.txt
   ```

2. **CBFDAC6008F9CAB4083784CBD1874F76618D2A97** --> password123 (SHA-1)

   ```
   hashcat -a 0 -m 100 hash2.txt /usr/share/wordlists/rockyou.txt
   ```

3. **1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032** --> letmein (SHA-256)

   ```
   hashcat -a 0 -m 1470 hash3.txt /usr/share/wordlists/rockyou.txt --show
   ```

4. **$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom** --> bleh(bcrypt $2*$, Blowfish (Unix))

   Para este caso, sabemos que **hashcat** se tardaría DEMASIADO en encontrar la contraseña asociada al hash con el formato de **bcrypt**. Para eso usamos el **hint** de TryHackMe en donde nos da la pista de filtrar solamente las contraselas que contengan 4 letras minusculas.

   Por lo que usamos un código para filtrar el diccionario de RockYou (**yo usé Python**):

   ```
   # Filtrar palabras de 4 caracteres minúsculas de rockyou.txt
   input_file = "/usr/share/wordlists/rockyou.txt"
   output_file = "wordlist_4_caracteres.txt"

   with open(input_file, "r", encoding="latin-1") as infile, open(output_file,
   "w", encoding="latin-1") as outfile:
       for line in infile:
           word = line.strip()  # Eliminar saltos de línea y espacios
           if len(word) == 4 and word.islower() and word.isalpha():  # 4
   caracteres, solo letras minúsculas
   ```

```
            outfile.write(word + "\n")

print(f"Filtrado completo. Se guardaron las palabras en '{output_file}'.")
```

Una vez hecho eso, usamos el siguiente comando:

```
hashcat -a 0 -m 3200 hash4.txt wordlist_4_caracteres.txt -w 3
```

5. **279412f945939ba78ce0758d3fd83daa** --> Eternity22 (MD4)

```
hashcat -a 0 -m 900 hash5.txt /usr/share/wordlists/rockyou.txt -r
/usr/share/hashcat/rules/best64.rule
```

Nota: Se usaron las 64 reglas que se encuentran en: *`/usr/share/hashcat/rules/best64.rule`*

Nota: Por defecto existe un hashcat.dotfile en *`/home/kali/.local/share/hashcat/hashcat.potfile`* en donde almacena los hashes antes buscados. Por lo que no es necesario hacer *bruteforce* y basta con agregar el parametro ***--show***

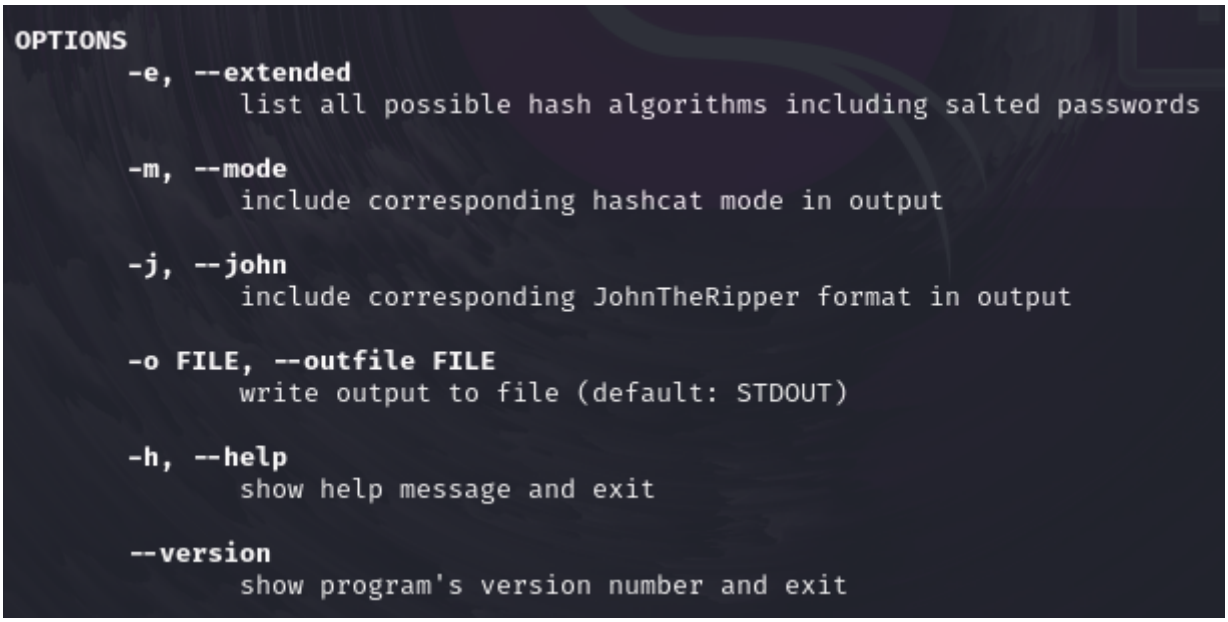
Ejemplo del output de **hashcat**:

```
48bb6e862e54f2a795ffc4e541caed4d:easy # <-- Contraseña crackeada aqui

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 48bb6e862e54f2a795ffc4e541caed4d
Time.Started.....: Thu Aug 14 19:27:06 2025 (1 sec)
Time.Estimated...: Thu Aug 14 19:27:07 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   669.9 kH/s (0.22ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 174080/14344385 (1.21%)
Rejected.........: 0/174080 (0.00%)
Restore.Point....: 172032/14344385 (1.20%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: florida69 -> berisha
Hardware.Mon.#1..: Util: 26%

Started: Thu Aug 14 19:26:13 2025
Stopped: Thu Aug 14 19:27:08 2025
```

HashCat Options



Podemos ahorrarnos el paso de buscar en Internet el número de hash correspondiente en la opción **-m** y simplemente usar el comando `hashid -m [hash]`. De esta forma, la misma herramienta nos proporciona el equivalente del hash en hashcat. O en su defecto `-j` para John The Ripper (otra herramienta similar a hashcat).

Nivel 2

1. **F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85** --> paule (SHA2-256)

   ```
   hashcat -a 0 -m 1400 2hash1.txt /usr/share/wordlists/rockyou.txt -w 3 -r /usr/share/hashcat/rules/best64.rule
   ```

2. **1DFECA0C002AE40B8619ECF94819CC1B** --> n63umy8lkf4i (NTLM)

   ```
   hashcat -a 0 -m 1000 2hash2.txt /usr/share/wordlists/rockyou.txt -w 3 -S
   ```

3. **6aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02** --> (sha512crypt 6, SHA512 (Unix))

   HINT: La contraseña tiene 6 letras.

   ```
   hashcat -a 0 -m 1800 2hash3.txt /usr/share/wordlists/rockyou.txt hashcat -a 0 -m 1800 "\$6\$aReallyHardSalt\$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02." /usr/share/wordlists/rockyou.txt
   ```

4. **e5d8870e5bdd26602cab8dbe07a942c8669e56d6** --> 481616481616 (HMAC-SHA1 (key = $salt))

   ```
   hashcat -a 0 -m 160 2hash4.txt /usr/share/wordlists/rockyou.txt
   ```