

# Cracking de Hashes OSCP

---

## INDICE:

- Análisis online
  - Tipos de Encriptados:
  - HASHCAT
  - JOHN THE RIPPER
  - Formato MD5
  - Hashes NTLM
  - pdf2john - PDF con contraseña
  - Cracking KeePass
  - Cracking ssh key
  - AS-REP roasting HASH
- 

## [+] Análisis online:

[https://hashes.com/en/tools/hash\\_identifier](https://hashes.com/en/tools/hash_identifier)

<https://www.dcode.fr/hash-identifier>

## [+] Tipos de Encriptados:

```
https://hashcat.net/wiki/doku.php?id=example_hashes // m parameter
https://mattw.io/hashID/types // hashid match
```

```
hashcat -m 0 -a 0 -D2 example0.hash example.dict (m = 0 es MD5) (a = 0 es Fuerza bruta)
```

```
hashcat -m 0 -a 0 -D2 example0.hash example.dict -r custom.rule
```

```
hashcat -m 0 'hash$' /home/kali/rockyou.txt // MD5 raw
```

```
hashcat -m 1800 'hash$' /home/kali/rockyou.txt // sha512crypt
```

```
hashcat -m 1600 'hash$' /home/kali/rockyou.txt // MD5(APR)
```

```
hashcat -m 1500 'hash$' /home/kali/rockyou.txt // DES(Unix), Traditional DES, DEScrypt
```

```
hashcat -m 1000 'hash$' /home/kali/rockyou.txt // NTLM
```

```
hashcat -m 500 'hash$' /home/kali/rockyou.txt // MD5crypt, MD5 (Unix)
```

```
hashcat -m 400 'hash$' /home/kali/rockyou.txt // Wordpress
```

## [+] HASHCAT :

```
cat users
```

```
File: users
```

```
1 admin:$2a$07$neV5T/BLEDiMQUs.gM1p4uYl8xl8kvNUo4/8Aja2sAWHAQLWqufye
2 matthew:$2a$07$q.m8WQP8niXODv55lJVov0mxGtg6K/YPHbD48/JQsdGLuImeVo.Em
```

-Identificar el tipo de hash:

MANERA 1:

```
$ hash-identifier
```

```
HASH: ab48fn84jrf94jfm4939jd939d939kd03
```

```
(Dara posible tipo de hash)
```

MANERA 2:

(para ver los ejemplos)

```
hashcat --example-hashes
```

-Podemos filtrar por nuestro tipo de hash y ver las lineas por encima:

```
``
```

```
>hashcat --example-hashes | grep '$2a$'
```

```
>hashcat --example-hashes | grep '$2a'
```

```
> cat users
```

```
File: users
```

```
1 admin:$2a$07$neV5T/BLEDiMQUs.gM1p4uYl8xl8kvNUo4/8Aja2sAWHAQLWqufye
2 matthew:$2a$07$q.m8WQP8niXODv55lJVov0mxGtg6K/YPHbD48/JQsdGLuImeVo.Em
```

```
> hashcat --example-hashes | grep '$2a$'
```

```
> hashcat --example-hashes | grep '$2a'
```

```
Example.Hash.....: $2a$05$MBCzKhG1KhezLh.@LRa@Kuw12nLJtpHy6DIaU.JAnqJUDYspHC.Ou
Example.Hash.....: $2a$05$/VT2Xs2dMd8GJKfrXhjYP.DkTj0VrY12yDN7/6I8ZV0q/1lEohLru
Example.Hash.....: $2a$05$Uo385Fa0g86uUXHwZxB90.qMMdRFExaXePGka4WGFv.86I45AEjm0
Example.Hash.....: $2a$12$KhivLhCuLhSyMB0xLxCyLu78x4z2X/EJdZNfS3Gy36fvRt56P2jbs
```

#Para ver las 15 lineas por encima:

```
>hashcat --example-hashes | grep '$2a$' -B 15
```

```
Hash mode #3200
Name.....: bcrypt $2*$, Blowfish (Unix)
Category.....: Operating System
Slow.Hash.....: Yes
Password.Len.Min....: 0
Password.Len.Max....: 72
Salt.Type.....: Embedded
Salt.Len.Min.....: 0
Salt.Len.Max.....: 256
Kernel.Type(s).....: pure
Example.Hash.Format.: plain
Example.Hash.....: $2a$05$MBTzKhG1KhezLh.0LRa0Kuw12nLJtpHy6DIaU.JAnqJUDYspHC.0u
--
```

EJECUCIÓN: <-----

MANERA 1:

```
#Para ver las 15 lineas por encima:
> hashcat -a 0 -m 3200 users /usr/share/wordlists/rockyou.txt -0 --username
```

MANERA 2:

```
#Para ver las 15 lineas por encima:
> hashcat -a 3 -m 1000 hashes.txt /usr/share/wordlists/rockyou.txt --force
```

## [+] JOHN THE RIPPER

-Cracking de hash con John:

(Copio el nombre y el hash a un archivo para tratar de crackearlo con john)

```
nano hash.txt
hagrid98:$ P$BY.....Htc.
```

```
john hash --wordlist=/usr/share/wordlists/rockyou.txt
```

## [+] Formato MD5:

```
john --format=Raw-MD5 --wordlists=/usr/share/wordlists/rockyou.txt hash.txt
john --format=Raw-MD5 --wordlists=/usr/share/wordlists/rockyou.txt hash.txt --rules
```

(Si la primera no muestra nada usar el parámetro --rules , para que use mayusculas y minusculas)

---

## [+] Hashes NTLM:

-MANERA 1 :

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c:::
bob:1009:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

(Copiaremos los hashes en nuestra makina kali, para ahora tratar de descifrarlos)

```
nano hashes.txt
(pego los hashes)
```

-Ahora con john haremos:

```
john --format=NT hashes.txt
password1 (bob)
password (Administrator)
```

-MANERA 2 :

\*\* NTLM

-Podemos usar hashcat con código 1000

```
hashcat -m 1000 nelly.hash rockyou.txt -r best64.rule --force
```

\*\* Net-NTLMv2

-Podemos usar hashcat con código 5600

```
hashcat -m 5600 paul.hash rockyou.txt --force
```

---

## [+] pdf2john - PDF con contraseña:

-Para obtenerla, primero obtenemos el hash del PDF:

```
perl /usr/share/john/pdf2john.pl Infrastructure.pdf | tee pdf_hash
```



```
impacket-GetNPUsers -dc-ip 192.168.50.70 -request -outputfile hashes.asreproast  
corp.com/pete
```

-Entonces obtenemos el siguiente hash

*krb5asrep\$23*

**dave@.CORP.COM**:b24a619cfa585dc1894fd6924162b099\$1be2e632a9446d1447b5ea80b73907  
5ad214a578f03773a7908f337aa705bcb711f8bce2ca751a876a7564bdbd4a926c10da32b01ec750  
cf35a2c37abde02f28b7aa363ffa1d18c9dd0262e43ab6a5447db24f71256120f94c24b17b1df465be  
ed362fcb14a539b4e9678029f3b3556413208e8d644fed540d453e1af6f20ab909fd3d9d35ea8b179  
58b56fd8658b147186042faaa686931b2b75716502775d1a18c11bd4c50df9c2a6b5a7ce2804df3c  
71c7dbbd7af7adf3092baa56ea865dd6e6fbc8311f940cd78609f1a6b0cd3fd150ba402f14fccd90757  
300452ce77e45757dc22

-Para descifrar podemos usar hashcat con código ~ 18200

```
sudo hashcat -m 18200 hashes.asreproast rockyou.txt -r best64.rule --force
```