

DESCIFRAR CONTRASEÑAS CON JOHN THE RIPPER

Objetivo General.- Descifrar las contraseñas de archivos comprimidos con winrar y Microsoft Office uso del programa **JOHN THE RIPPER** que trae Kali Linux.

Pasos:

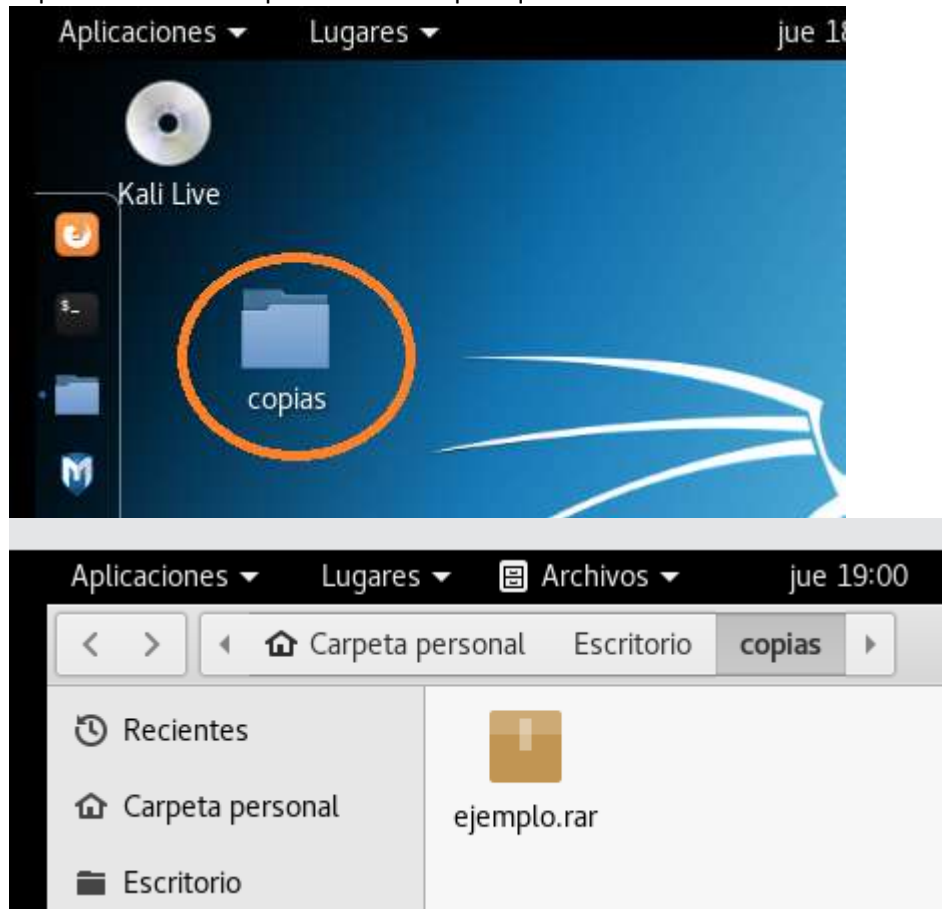
- Descifrar contraseña de archivo rar
 - o Obtener código hash del archivo rar
 - o Descifrar contraseña con **john the ripper** (con el diccionario rockyou)
- Descifrar contraseña de Microsoft Word
 - o Obtener código hash del archivo docx ()
 - o Descifrar contraseña con **john the ripper** (con el diccionario rockyou)

DESARROLLO DE LA PRÁCTICA

1) Descifrar contraseña de archivo rar

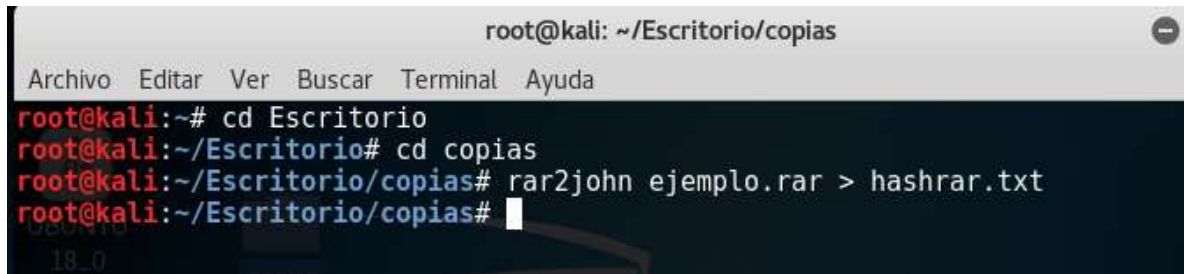
Obtener código hash del archivo rar

- o En el sistema operativo Windows comprimirémos un archivo con el programa winrar, al cual le llamaremos **ejemplo.rar** a la hora de comprimir este archivo le daremos una contraseña.
- o En kali Linux copiaremos el archivo ejemplo.rar a una carpeta, en este ejemplo copiaremos a una carpeta llamada copias que estará en el escritorio de Linux.

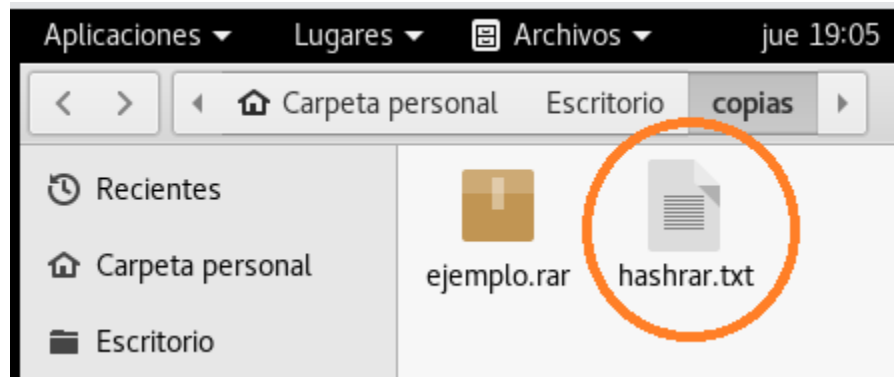


- o Obtener código hash del archivo ejemplo.rar

- Abrir una terminal de Linux
- Ubicarse en la dirección /escritorio/copias
- Escribir la instrucción: `rar2john ejemplo.rar > hashrar.txt`
Esta instrucción copia el código hash del archivo ejemplo.rar al archivo hashrar.txt



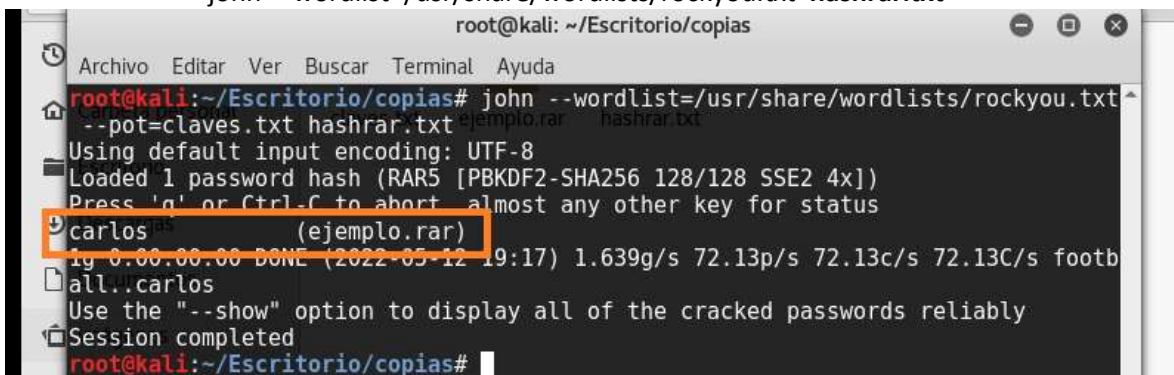
```
root@kali: ~/Escritorio/copias
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# cd Escritorio
root@kali:~/Escritorio# cd copias
root@kali:~/Escritorio/copias# rar2john ejemplo.rar > hashrar.txt
root@kali:~/Escritorio/copias#
```



- **Descifrar contraseña con john the ripper (con el diccionario rockyou)**
Rockyou.txt es un diccionario de datos con miles de posibles contraseñas.
Este archivo se encuentra en `/usr/share/wordlists/rockyou.txt`
Posiblemente este archivo este comprimido, el cual habrá que descomprimirlo.

Escribir el código de john the ripper que descifrá la contraseña para lo cual escribiremos la siguiente instrucción:

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



```
root@kali: ~/Escritorio/copias
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~/Escritorio/copias# john --wordlist=/usr/share/wordlists/rockyou.txt
--pot=claves.txt hashrar.txt
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 128/128 SSE2 4x])
Press 'q' or Ctrl-C to abort, almost any other key for status
carlos (ejemplo.rar)
1g 0:00:00.00 DONE (2022-05-12 19:17) 1.639g/s 72.13p/s 72.13c/s 72.13C/s footb
all..carlos
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Escritorio/copias#
```

Como se ve encontró la clave del archivo el cual es “carlos”

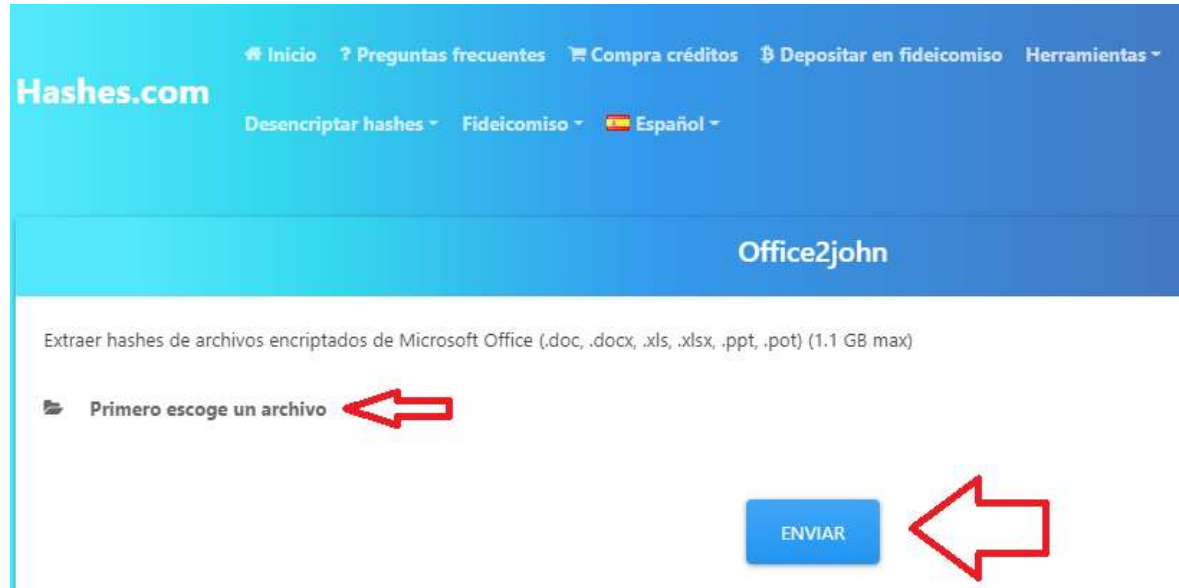
Para volver a visualizar el password puede escribir el comando:

`john --show hashrar.txt`

2) Descifrar contraseñas de documento Microsoft Word

Obtener hash del documento mediante la página:

<https://hashes.com/es/johntheripper/office2john>



Después de escoger el archivo (documento word) y presionar el botón enviar, nos enviará su código hash



Ahora ese código se debe llevar a kali Linux en un archivo de texto. (por ejemplo **dos.txt**)

En kali Linux escribir el siguiente comando:

John -wordlist:/usr/share/wordlists/rockyou.txt dos.txt

```
root@kali:~/Escritorio/bas# john --wordlist=/usr/share/wordlists/rockyou.txt dos
ús.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 128/128 SSE2 4x2 / SHA512 1
28/128 SSE2 2x AES])
Press 'q' or Ctrl-C to abort, almost any other key for status
54321 (?)
lg 0:00:00:03 DONE (2022-09-08 18:03) 0.2801g/s 147.8p/s 147.8c/s 147.8C/s frank
ie..red123 = HELVETAS_
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Escritorio/bas#
```

Para volver a visualizar el password puede escribir el comando:

```
john --show dos.txt
```

```
root@kali:~/Escritorio/bas# john --show dos.txt
?:54321
1 password hash cracked, 0 left
root@kali:~/Escritorio/bas#
```