

Descifrar archivo rar con John The Ripper.

Tenemos un archivo .rar cifrado con clave, por lo que no podemos acceder a su contenido. Vamos a averiguar su contraseña para poder acceder a él.

1. Ejecutamos el comando 'rar2john' sobre el archivo .rar. Esta es una herramienta que incluye john the ripper, que permite obtener el hash de la clave de un archivo .rar cifrado. En la misma linea, redirigimos el hash obtenido a un archivo .txt para almacenarlo y acceder a él posteriormente. El comando se nos queda asi:

```
rar2john MATERIAL1.rar > rar_hash.txt
```

```
(victor@victor)-[~/JohnTheRipper_Víctor_Cordeiro]
$ ls
MATERIAL1.rar

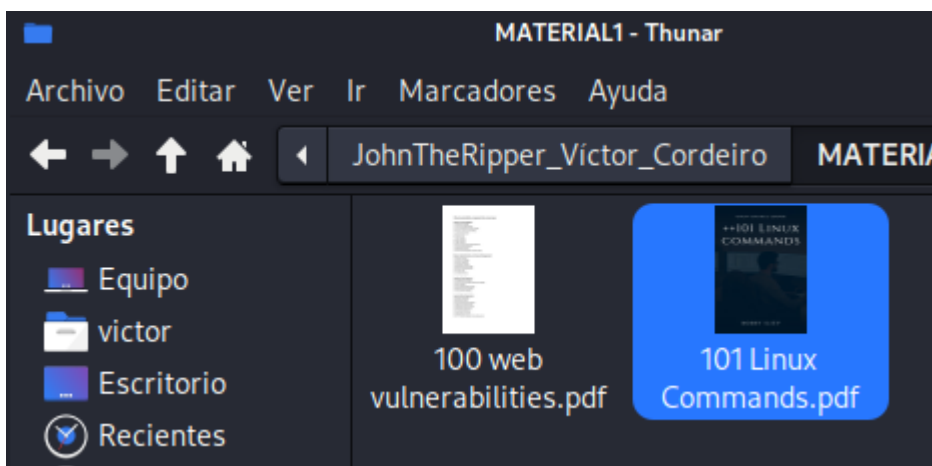
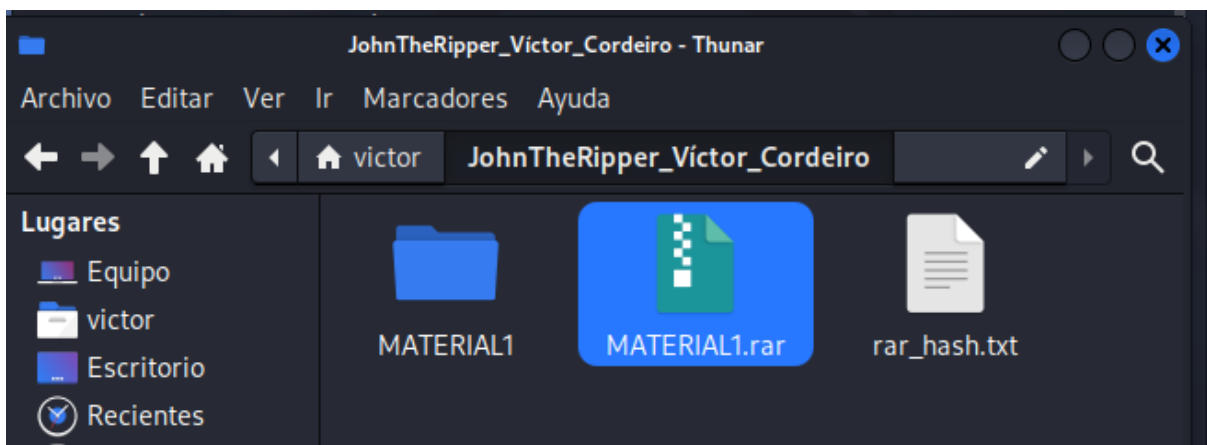
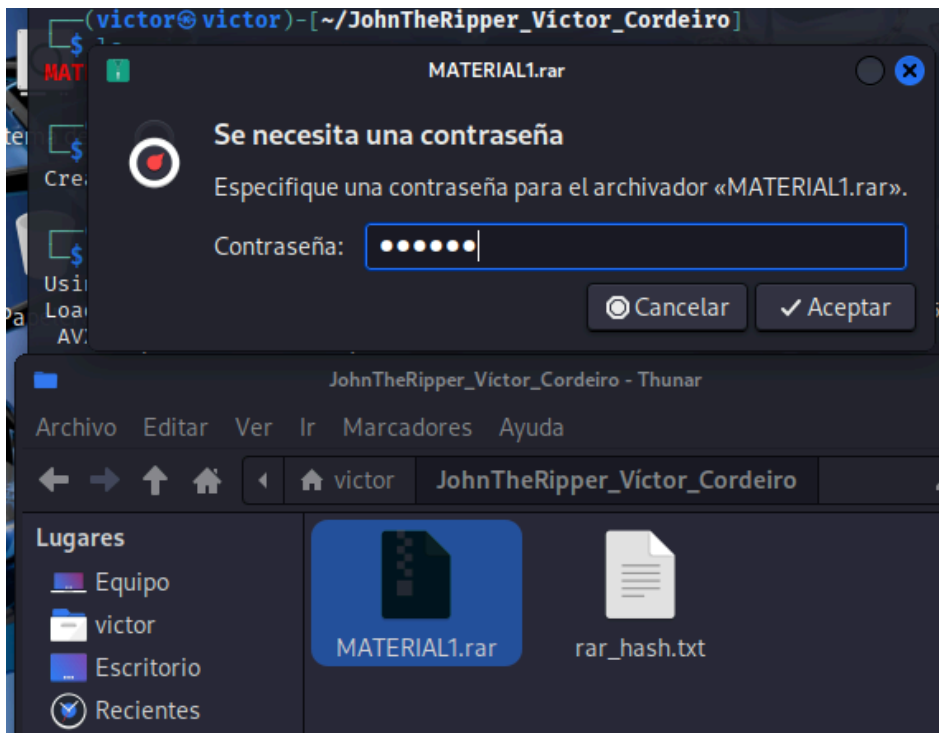
(victor@victor)-[~/JohnTheRipper_Víctor_Cordeiro]
$ rar2john MATERIAL1.rar > rar_hash.txt
Created directory: /home/victor/.john

(victor@victor)-[~/JohnTheRipper_Víctor_Cordeiro]
$ cat rar_hash.txt
MATERIAL1.rar:$rar5$16$d962f3d72cdc47869669f06dea33284c$15$5638237a55705909fc
04be465494b8a6$8$e68f482404ec56d5
MATERIAL1.rar:$rar5$16$d962f3d72cdc47869669f06dea33284c$15$95e6dcaec229de0acf
14714f76352731$8$e68f482404ec56d5
```

2. Ahora ejecutamos el comando john sobre el archivo que almacena nuestro hash. La herramienta descifra la clave, y tardara en función de la complejidad de la clave y nuestro poder de procesamiento.

```
(victor@victor)-[~/JohnTheRipper_Víctor_Cordeiro]
$ john rar_hash.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (RAR5 [PBKDF2-SHA256 256/256
AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1a2b3c (MATERIAL1.rar)
1a2b3c (MATERIAL1.rar)
2g 0:00:00:10 DONE 2/3 (2025-10-06 18:10) 0.1821g/s 1318p/s 1318c/s 2636C/s r
angers..88888888
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

3. Ahora conocemos la contraseña que protege el archivo. rar, '1a2b3c'. Si la introducimos al intentar descomprimir el archivo nos da acceso, comprobando así que es la correcta.



Descifrar el hash de una contraseña con John The Ripper.

En este caso conocemos el hash de una clave, y vamos a descifrarlo usando un diccionario de claves, en concreto el que creamos en otra actividad con crunch.

1. Primero creamos un archivo .txt que contenga el hash que queremos descifrar.

```
(victor@victor)-[~/hashTest]
$ echo 7fe254f10c1a44e1984f57afe5deea35d725d192 > passwordHash.txt

(victor@victor)-[~/hashTest]
$ cat passwordHash.txt
7fe254f10c1a44e1984f57afe5deea35d725d192
```

2. Una vez hecho esto, usamos el comando john con la opción - - wordlist, con la que le indicamos a la herramienta que trabaje con un diccionario. Indicamos la ruta del diccionario y seguido la ruta del archivo con el hash que queremos descifrar

```
john --wordlist=../dictionary.txt passwordHash.txt
```

```
(victor@victor)-[~/hashTest]
$ john --wordlist=../dictionary.txt passwordHash.txt
Warning: detected hash type "Raw-SHA1", but the string is also recognized as
"Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type
instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as
"Raw-SHA1-Linkedin"
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type
instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as
"ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as
"has-160"
Use the "--format=has-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
aa2a33 (?)
1g 0:00:00:00 DONE (2025-10-06 18:43) 100.0g/s 90400p/s 90400c/s 90400C/s aa2
a3c..aa2ba1
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```

Finalmente obtenemos la clave correspondiente a este hash:

aa2a23