

[redeszone.net](https://www.redeszone.net)

# John The Ripper: Crackea contraseñas de usuarios en Linux

5-6 minutos

---

Para aquellos que aún no lo conozcan, **John the Ripper es una herramienta de crackeo de contraseñas** escrita en C y muy utilizada por los analistas de seguridad para comprobar la robustez de una clave frente a ataques de fuerza bruta.

En este artículo vamos a ver cómo puede utilizar un administrador de sistemas John the Ripper para comprobar la seguridad de la clave del equipo. De esta forma comprobaremos si somos vulnerables a un ataque de fuerza bruta o diccionario por parte de un pirata informático que busca obtener acceso remoto (o local) al mismo.

## Cómo instalar John the Ripper en Ubuntu

Lo primero que debemos hacer es instalar la herramienta en nuestro sistema. John the Ripper está incluida en los principales repositorios de Linux, por lo que para instalarla (por ejemplo en un

sistema Ubuntu) simplemente debemos teclear en el terminal:

```
sudo apt install john
```

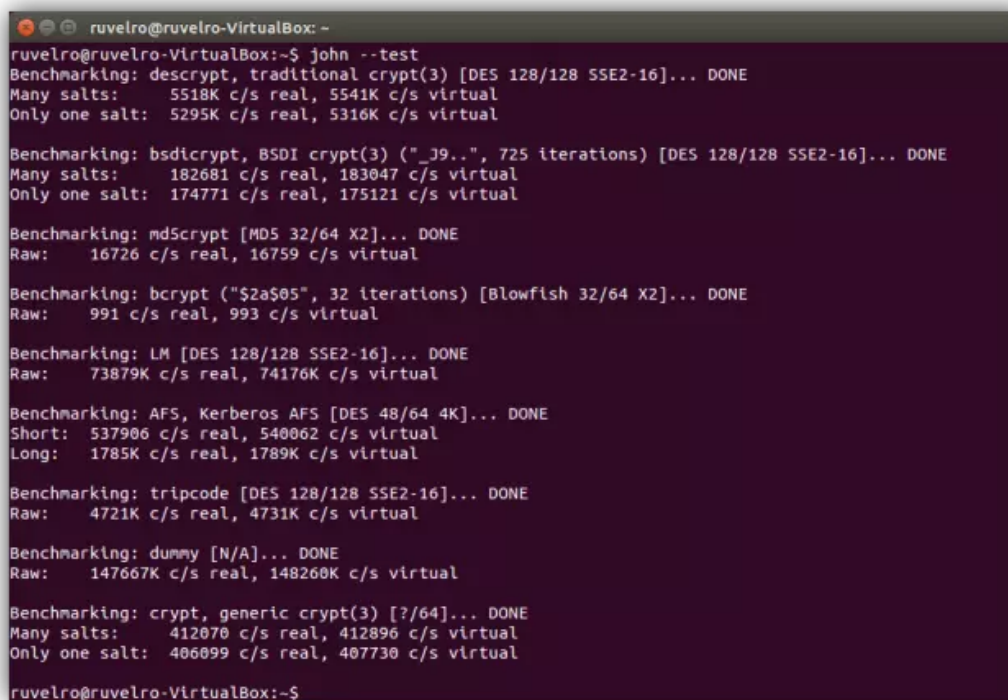
A screenshot of a terminal window titled 'ruvelro@ruvelro-VirtualBox: ~'. The user has entered the command 'sudo apt install john'. The terminal output shows the password prompt, package list reading, dependency tree creation, and state information reading. It then lists 'john-data' as an extra package to be installed along with 'john'. The output indicates that 0 packages will be updated, 2 will be installed, and 0 will be removed. It also shows the disk space requirements: 0 B/5.405 kB of files to be downloaded and 7.891 kB of additional disk space to be used. The prompt '¿Desea continuar? [S/n]' is shown at the bottom with a cursor.

Una vez instalada la herramienta ya podemos seguir con esta guía.

## Probar rendimiento de John the Ripper

Antes de empezar con el crackeo de las contraseñas podemos lanzar un sencillo test de rendimiento donde se pondrá a prueba nuestro hardware. De esta manera podremos saber la velocidad con la que la herramienta probará claves con diferentes tipos de cifrado utilizando el 100% de nuestra CPU. Para ello simplemente abrimos un terminal Linux y tecleamos:

```
john --test
```



```
ruvelro@ruvelro-VirtualBox: ~  
ruvelro@ruvelro-VirtualBox:~$ john --test  
Benchmarking: descrypt, traditional crypt(3) [DES 128/128 SSE2-16]... DONE  
Many salts: 5518K c/s real, 5541K c/s virtual  
Only one salt: 5295K c/s real, 5316K c/s virtual  
  
Benchmarking: bsdicrypt, BSDI crypt(3) ("_J9..", 725 iterations) [DES 128/128 SSE2-16]... DONE  
Many salts: 182681 c/s real, 183047 c/s virtual  
Only one salt: 174771 c/s real, 175121 c/s virtual  
  
Benchmarking: md5crypt [MD5 32/64 X2]... DONE  
Raw: 16726 c/s real, 16759 c/s virtual  
  
Benchmarking: bcrypt ("S2a$05", 32 iterations) [Blowfish 32/64 X2]... DONE  
Raw: 991 c/s real, 993 c/s virtual  
  
Benchmarking: LM [DES 128/128 SSE2-16]... DONE  
Raw: 73879K c/s real, 74176K c/s virtual  
  
Benchmarking: AFS, Kerberos AFS [DES 48/64 4K]... DONE  
Short: 537906 c/s real, 540062 c/s virtual  
Long: 1785K c/s real, 1789K c/s virtual  
  
Benchmarking: tripcode [DES 128/128 SSE2-16]... DONE  
Raw: 4721K c/s real, 4731K c/s virtual  
  
Benchmarking: dummy [N/A]... DONE  
Raw: 147667K c/s real, 148260K c/s virtual  
  
Benchmarking: crypt, generic crypt(3) [?/64]... DONE  
Many salts: 412070 c/s real, 412896 c/s virtual  
Only one salt: 406099 c/s real, 407730 c/s virtual  
ruvelro@ruvelro-VirtualBox:~$
```

Como podemos ver, se llevan a cabo una serie de tests donde se medirá el rendimiento.

## Caso práctico 1: Crackear contraseñas de usuarios de Linux por fuerza bruta

Una vez instalada la herramienta y realizado el test de rendimiento ya podemos empezar con un caso real. Podemos optar por cargar directamente el archivo «/etc/shadow» que contiene las contraseñas de Linux y crackearlas, sin embargo, en este ejemplo

vamos a crear un documento manualmente con un usuario y una contraseña y le indicaremos a John que lo crackee. Vamos a hacer esto por tres razones:

- Para no comprometer realmente nuestro sistema.
- Para obtener los resultados lo más rápidamente posible (vamos a utilizar una clave muy simple)
- Para tener una primera toma de contacto con la herramienta y familiarizarnos con ella.

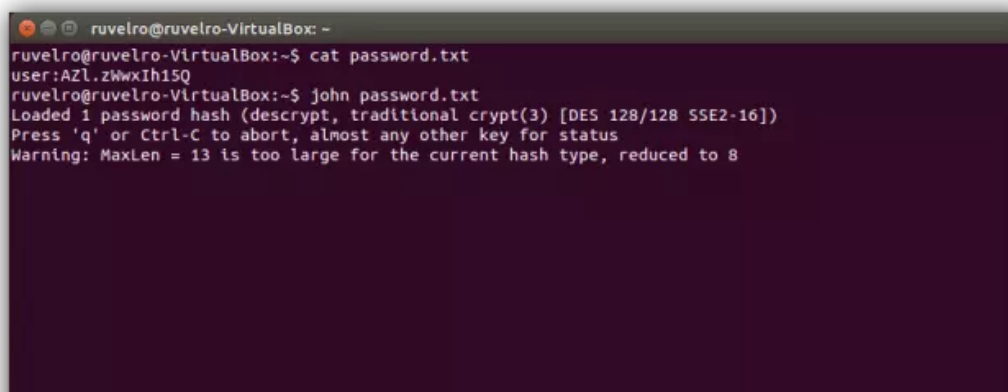
Para ello creamos un nuevo archivo de texto, por ejemplo, en nuestra carpeta personal de Ubuntu con el siguiente contenido:

```
user:AZl.zWwxIh15Q
```

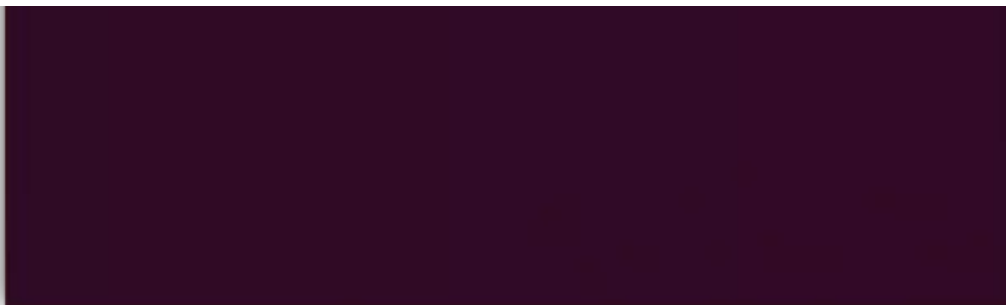
A continuación vamos a indicar a John que empiece a trabajar para crackear la contraseña del archivo anterior. Para ello tecleamos:

```
john password.txt
```

La herramienta empezará a trabajar.

A screenshot of a terminal window titled 'ruvelro@ruvelro-VirtualBox: ~'. The terminal shows the following commands and output:

```
ruvelro@ruvelro-VirtualBox:~$ cat password.txt
user:AZl.zWwxIh15Q
ruvelro@ruvelro-VirtualBox:~$ john password.txt
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: MaxLen = 13 is too large for the current hash type, reduced to 8
```



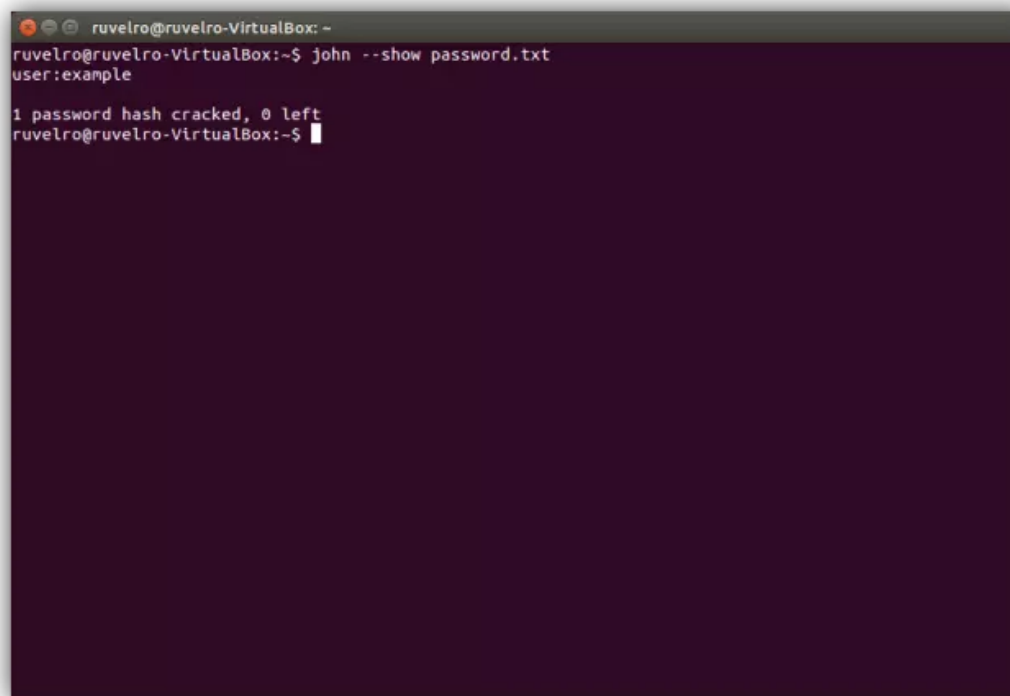
Debemos esperar a que John the Ripper consiga crackear la contraseña del anterior archivo. Este proceso puede tardar horas e incluso días según la dificultad de la misma. Cuando el proceso finalice veremos un resultado similar al siguiente.

```
ruvelro@ruvelro-VirtualBox: ~  
ruvelro@ruvelro-VirtualBox:~$ cat password.txt  
user:AZL.zWwxIh15Q  
ruvelro@ruvelro-VirtualBox:~$ john password.txt  
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Warning: MaxLen = 13 is too large for the current hash type, reduced to 8  
0g 0:00:00:27 3/3 0g/s 4480Kp/s 4480Kc/s 4480Kc/s krl0893..krl0013  
0g 0:00:02:00 3/3 0g/s 4918Kp/s 4918Kc/s 4918Kc/s 1bs1009..1bs1043  
example  
      (user)  
1g 0:00:05:49 3/3 0.002864g/s 4986Kp/s 4986Kc/s 4986Kc/s exampys..exempl3  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed  
ruvelro@ruvelro-VirtualBox:~$
```

Nuestra contraseña está crackeada. Para verla simplemente

debemos utilizar el comando `--show` de la siguiente manera:

```
john --show password.txt
```



```
ruvelro@ruvelro-VirtualBox: ~  
ruvelro@ruvelro-VirtualBox:~$ john --show password.txt  
user:example  
  
1 password hash cracked, 0 left  
ruvelro@ruvelro-VirtualBox:~$
```

Nuestra contraseña era «example» (tal como viene en el ejemplo de la [Wikipedia](#)). Ya podemos intentar iniciar sesión en el sistema con el usuario «user» y la contraseña «example», o por lo menos podríamos hacerlo si hubiéramos trabajado directamente con el fichero `/etc/shadow`, aunque el tiempo de crackeo hubiera tardado mucho más que varios minutos.

Más adelante veremos cómo utilizar esta misma herramienta pero para crackear contraseñas utilizando un diccionario como fuente de

claves.

Para finalizar os vamos a dejar un pequeño reto para practicar con este programa, copiando exactamente un caso práctico de un archivo `/etc/shadow`:

```
redes-
```

```
zone:$6$85X6KHD9$10GCEYlO7fVYKh4kIIaiEN37zCB/ROaG1hYmLYane90m1teephQHE  
/grdlB/cgg/1cfEuMIt2UUI1lQkI.
```

## Caso práctico 2: Crackear contraseñas de usuarios de Linux utilizando un diccionario de claves

Al igual que en el tutorial anterior, en este caso vamos a partir de una clave de ejemplo que hemos guardado a mano en un documento llamado «password.txt»:

```
user:AZl.zWwxIh15Q
```

A continuación lo que tenemos que hacer es tener o crear un diccionario de claves personalizado. Podemos descargar estos diccionarios de Internet, pero para hacer las primeras pruebas del programa vamos a crear nosotros un diccionario sencillo, al que llamaremos «passwords.lst» y en el que introduciremos varios valores, cada uno en una línea, pero siendo uno de ellos la palabra «example» (ya que corresponde con nuestra contraseña).

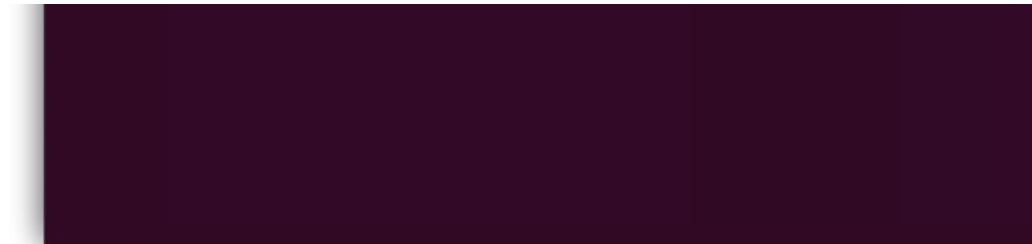
```
ruvelro@ruvelro-VirtualBox: ~  
ruvelro@ruvelro-VirtualBox:~$ cat passwords.lst  
1  
11  
2  
12  
a  
aa  
aaa  
prueba  
redeszone  
Example  
eXaMplE  
EXAMPLE  
example  
contraseña  
password  
incorrecta  
  
ruvelro@ruvelro-VirtualBox:~$
```

A continuación simplemente debemos ejecutar John the Ripper con el parámetro `--wordlist=` seguido de la ruta de nuestro archivo. A continuación ponemos un ejemplo con los dos archivos que hemos generado (el de la contraseña cifrada y el diccionario):

```
john --wordlist=passwords.lst password.txt
```

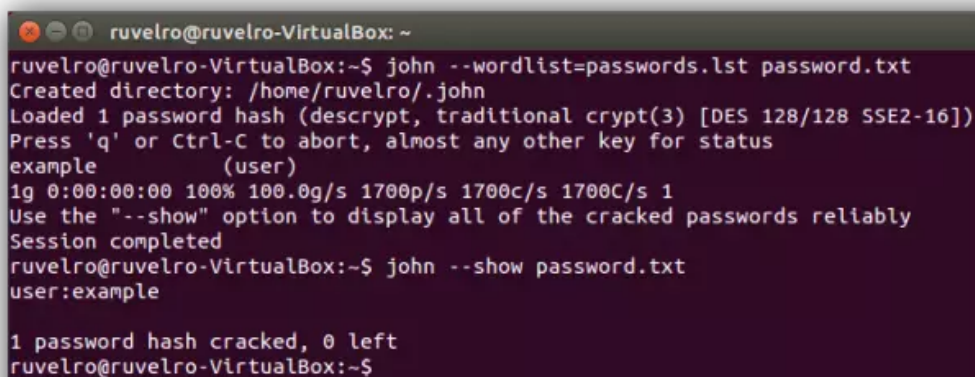
```
ruvelro@ruvelro-VirtualBox: ~  
ruvelro@ruvelro-VirtualBox:~$ john --wordlist=passwords.lst password.txt  
Created directory: /home/ruvelro/.john  
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])  
Press 'q' or Ctrl-C to abort, almost any other key for status  
example (user)  
1g 0:00:00:00 100% 100.0g/s 1700p/s 1700c/s 1700C/s 1  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed  
ruvelro@ruvelro-VirtualBox:~$
```





Al tener una clave sencilla y pocas entradas del diccionario el proceso será prácticamente instantáneo. Ya hemos crackeado, o descifrado, la contraseña. Lo único que nos queda por hacer es utilizar el parámetro `--show` para que nos muestre el resultado.

```
john --show password.txt
```



```
ruvelro@ruvelro-VirtualBox: ~
ruvelro@ruvelro-VirtualBox:~$ john --wordlist=passwords.lst password.txt
Created directory: /home/ruvelro/.john
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
example (user)
1g 0:00:00:00 100% 100.0g/s 1700p/s 1700c/s 1700C/s 1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
ruvelro@ruvelro-VirtualBox:~$ john --show password.txt
user:example

1 password hash cracked, 0 left
ruvelro@ruvelro-VirtualBox:~$
```

Hasta aquí hemos llegado con nuestro manual de John The Ripper,

esperamos que os sirva de ayuda. Os invitamos a visitar [nuestra sección de Seguridad Informática](#) donde encontraréis más tutoriales.