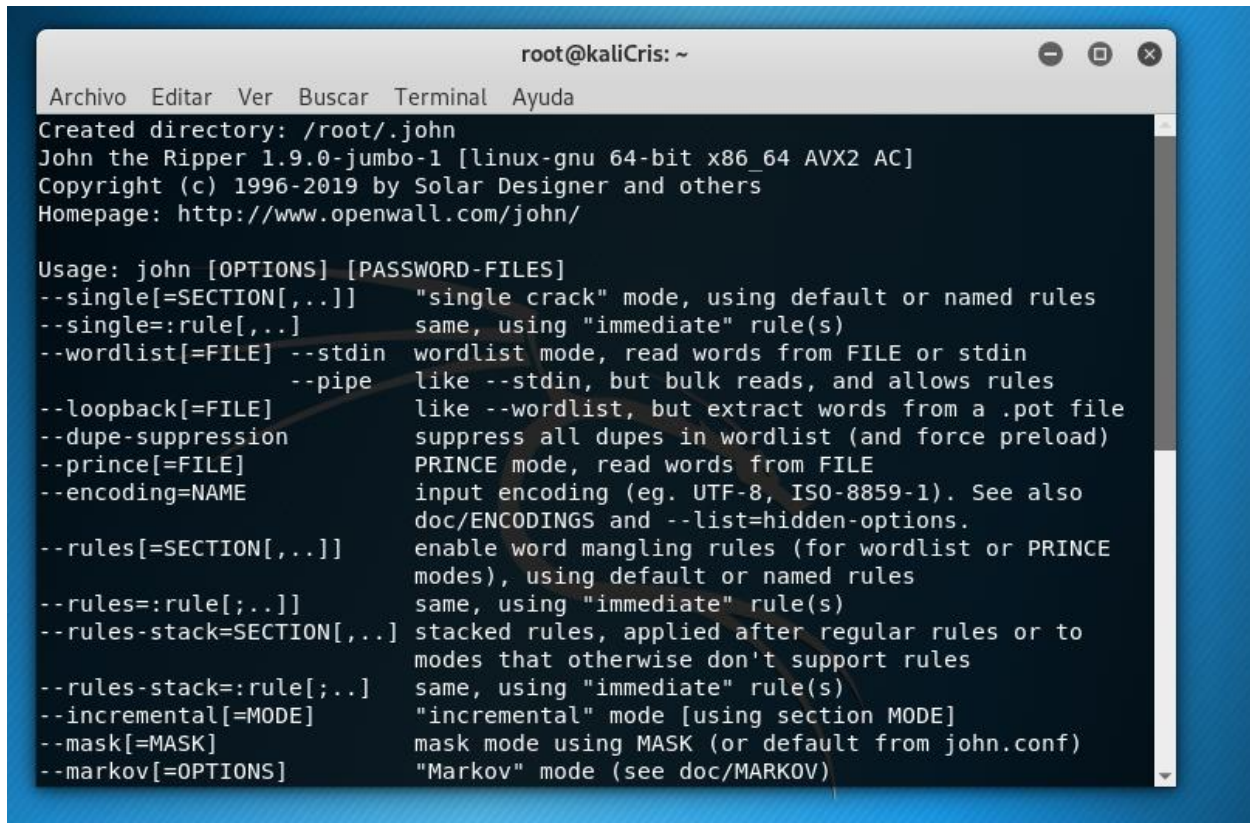


Kali-linux.Herramientas de kali-linux

Ejemplo 2:John The Ripper

John The Ripper es una aplicación para **desencriptar contraseñas por fuerza bruta**. Se basa en un diccionario de contraseñas que puede ser el que se incluye o descargarnos uno que nos guste y lanzarlo.

A screenshot of a terminal window titled 'root@kaliCris: ~'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal output shows the John the Ripper version information and a detailed list of command-line options. The options include: --single[=SECTION[,...]] for single crack mode, --single=:rule[,...] for immediate rules, --wordlist[=FILE] --stdin for wordlist mode, --pipe for bulk reads, --loopback[=FILE] for .pot file extraction, --dupe-suppression for suppressing duplicates, --prince[=FILE] for PRINCE mode, --encoding=NAME for input encoding, --rules[=SECTION[,...]] for word mangling rules, --rules=:rule[;...] for immediate rules, --rules-stack=SECTION[,...] for stacked rules, --rules-stack=:rule[;...] for immediate rules, --incremental[=MODE] for incremental mode, --mask[=MASK] for mask mode, and --markov[=OPTIONS] for Markov mode.

```
root@kaliCris: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Created directory: /root/.john
John the Ripper 1.9.0-jumbo-1 [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,...]]  "single crack" mode, using default or named rules
--single=:rule[,...]      same, using "immediate" rule(s)
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
                        --pipe  like --stdin, but bulk reads, and allows rules
--loopback[=FILE]         like --wordlist, but extract words from a .pot file
--dupe-suppression        suppress all dupes in wordlist (and force preload)
--prince[=FILE]           PRINCE mode, read words from FILE
--encoding=NAME           input encoding (eg. UTF-8, ISO-8859-1). See also
                        doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,...]]  enable word mangling rules (for wordlist or PRINCE
                        modes), using default or named rules
--rules=:rule[;...]      same, using "immediate" rule(s)
--rules-stack=SECTION[,...] stacked rules, applied after regular rules or to
                        modes that otherwise don't support rules
--rules-stack=:rule[;...] same, using "immediate" rule(s)
--incremental[=MODE]     "incremental" mode [using section MODE]
--mask[=MASK]            mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]       "Markov" mode (see doc/MARKOV)
```

Práctica John The Ripper

Averiguaremos una clave de un usuario suponiendo que no la sabemos.

Primero, creo el usuario.

```
root@kaliCris:~# adduser prueba
Añadiendo el usuario `prueba' ...
Añadiendo el nuevo grupo `prueba' (1000) ...
Añadiendo el nuevo usuario `prueba' (1000) con grupo `prueba' ...
Creando el directorio personal `/home/prueba' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para prueba
```

El archivo **/etc/shadow**, es por defecto el archivo en el que Linux almacena las claves encriptadas.

Con el siguiente comando descubrimos la contraseña del usuario prueba.

```
root@kaliCris:~# john -format=crypt /etc/shadow
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [??/64])
Cost 1 (algorithm [1:descript 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 6 for all loaded hashes
Cost 2 (algorithm specific iterations) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
prueba (prueba)
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 47 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
```