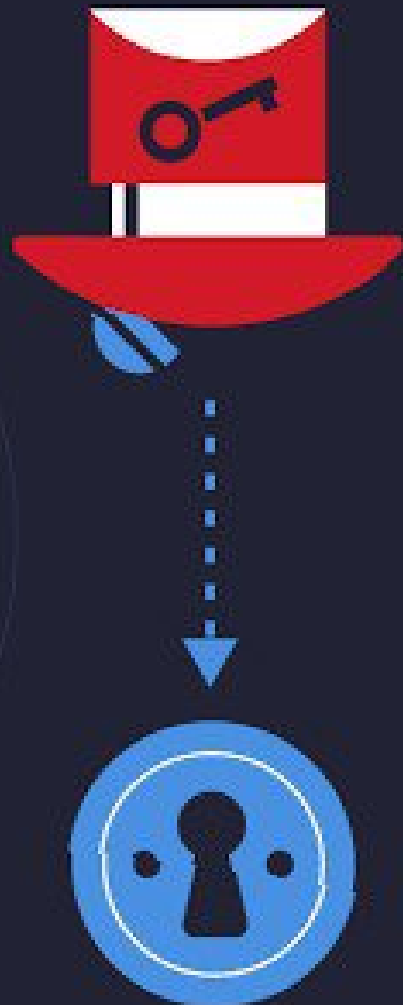


What is John the Ripper and how does it work?



John the Ripper (JTR) is a free, open-source software tool used by hackers, both ethical and otherwise, for password cracking. The software is typically used in a UNIX/Linux and Mac OS X environment where it can detect weak passwords. John the Ripper jumbo supports many cipher and hash types.

Reasons to Use John The Ripper



- Works with **Unix, Windows & Kerberos**
- Also compatible with **LDAP, MySQL & MD4** with the addition of extra modules
- Popular **password cracking tool**
- Preferred by **pentesters**
- Accessible on **multiple platforms**
- **Auto-detects** password hash types
- Can crack **multi-encrypted formats**

How to install John the Ripper in Ubuntu

[John the Ripper](#) is a free program for breaking passwords. It was created for the Unix operating system, but it now runs on fifteen different platforms (eleven of which are architecture-specific versions of Unix, DOS, Win32, BeOS, and OpenVMS). Because it incorporates a variety of password crackers into one package, auto-detects password hash types, and offers a customizable cracker, it is one of the most widely used password testing and breaking tools. It supports a variety of encrypted password forms, including numerous crypt password hash types (based on DES, MD5, or Blowfish), Kerberos AFS, and the Windows NT/2000/XP/2003 LM hash. Additional modules have added support for MD4-based password hashes as well as passwords saved in LDAP, MySQL, and other databases.

John the Ripper is a rapid password breaker that works on a variety of Unix, Windows, DOS, BeOS, and OpenVMS systems. Its main goal is to identify weak Unix passwords. Apart from multiple crypts (3) password hash types typically found on various Unix systems, Windows LM hashes, as well as a variety of additional hashes and ciphers, are supported out of the box.

Installing John the Ripper in Ubuntu

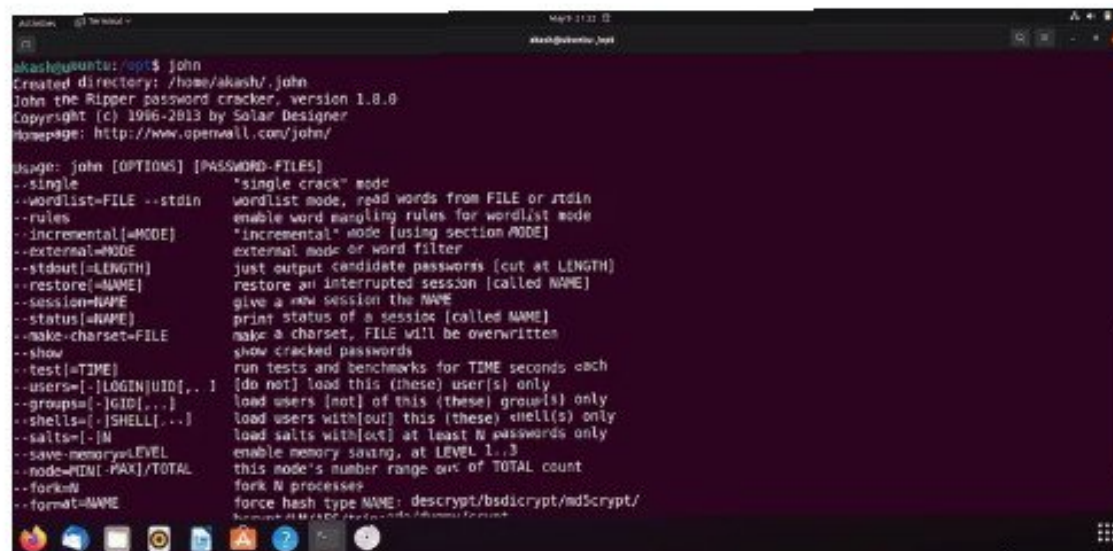
We can download the John the Ripper package in 2 ways:

- Using APT Package Manager
- Using Snap Utility

Let's go through both the installation methods one by one.

Step 2: This will start the installation procedure. When it's done, type 'john' into the terminal.

john



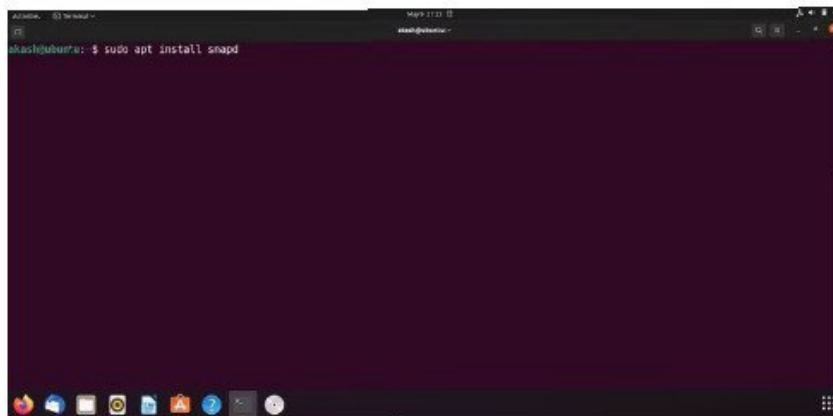
```
akash@ubuntu: ~$ john
Created directory: /home/akash/.john
John the Ripper password cracker, version 1.8.0
Copyright (c) 1996-2013 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin  wordlist mode, read words from FILE or stdin
--rules                 enable word mangling rules for wordlist mode
--incremental[=MODE]    "incremental" mode (using section MODE)
--external=MODE         external mode or word filter
--stdout[=LENGTH]       just output candidate passwords (cut at LENGTH)
--restore[=NAME]         restore an interrupted session (called NAME)
--session=NAME           give a new session the NAME
--status[=NAME]          print status of a session (called NAME)
--make-charset=FILE      make a charset, FILE will be overwritten
--show                  show cracked passwords
--test[=TIME]            run tests and benchmarks for TIME seconds each
--users=[-]LOGIN[UID[.  [do not] load this (these) user(s) only
--groups=[-]GID[...]]    load users [not] of this (these) group(s) only
--shells=[-]SHELL[...]] load users with[out] this (these) shell(s) only
--salts=[-]N             load salts with[out] at least N passwords only
--save-memory=LEVEL      enable memory saving, at LEVEL 1..3
--mode=MIN[-MAX]/TOTAL   this mode's number range out of TOTAL count
--fork=N                 fork N processes
--format=NAME            force hash type NAME: descript/bsdictcrypt/md5crypt/
```

Method 2: Using Snap Utility

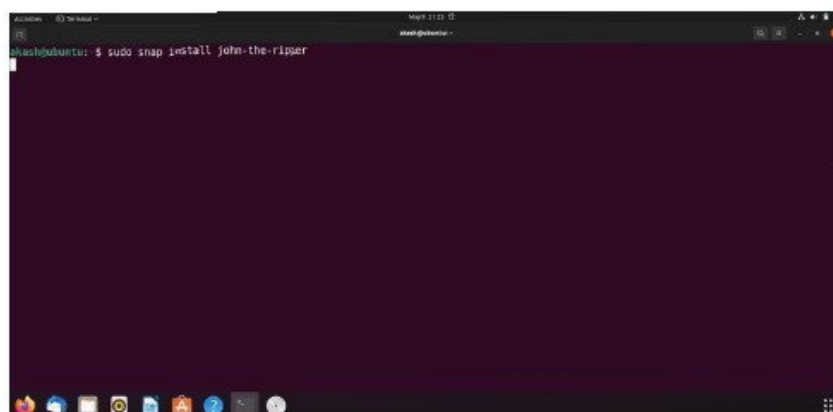
Step 1: Execute the below command in the terminal to install the snapd on the system.

```
sudo apt install snapd
```



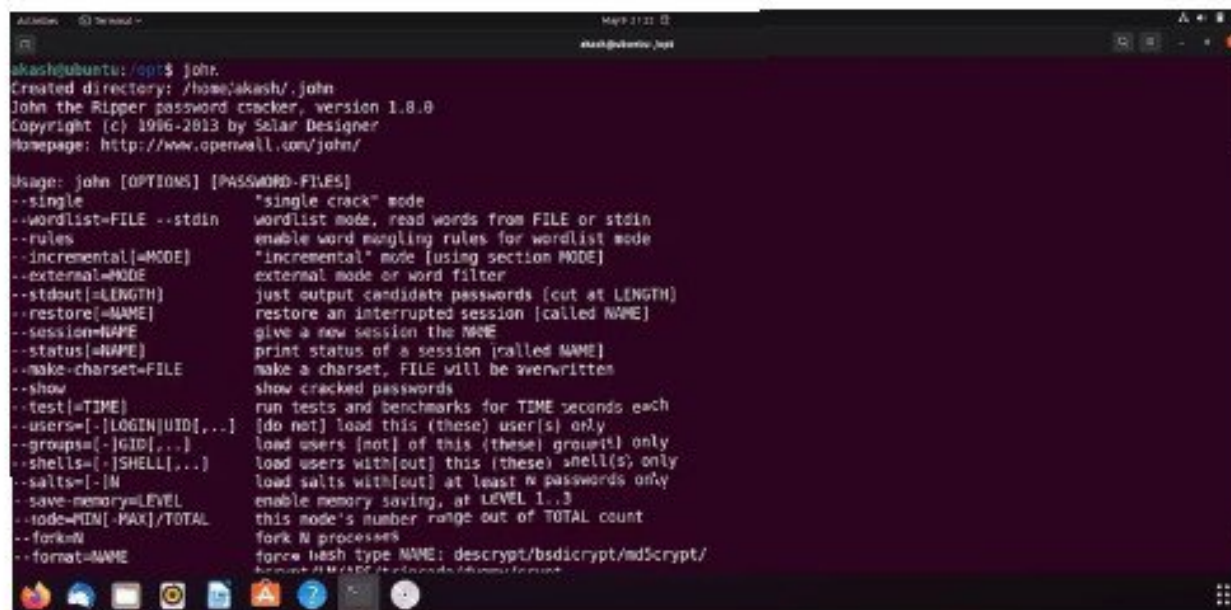
Step 2: Now, execute the below command to install the John the Ripper tool using snap.

```
sudo snap install john-the-rip
```



Step 3: Now, type the following command and press enter to 'launch John-the-ripper tool'.

john



```
akash@ubuntu: /opt$ john
Created directory: /home/akash/.john
John the Ripper password cracker, version 1.8.0
Copyright (c) 1996-2013 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin  wordlist mode, read words from FILE or stdin
--rules                 enable word mangling rules for wordlist mode
--incremental[=MODE]    "incremental" mode [using section MODE]
--external=MODE         external mode or word filter
--stdout[=LENGTH]       just output candidate passwords (cut at LENGTH)
--restore[=NAME]         restore an interrupted session [called NAME]
--session=NAME          give a new session the NAME
--status[=NAME]         print status of a session [called NAME]
--make-charset=FILE     make a charset, FILE will be overwritten
--show                 show cracked passwords
--test[=TIME]           run tests and benchmarks for TIME seconds each
--users=[-]LOGIN[UID,...] [do not] load this (these) user(s) only
--groups=[-]GID[...]    load users [not] of this (these) group(s) only
--shells=[-]SHELL[...]  load users with[out] this (these) shell(s) only
--salts=[-]N            load salts with[out] at least N passwords only
--save-memory=LEVEL     enable memory saving, at LEVEL 1..3
--mode=MID[-MAX]/TOTAL  this mode's number range out of TOTAL count
--fork=N               fork N processes
--format=NAME           force hash type NAME: descrypt/bsdcrypt/md5crypt/
```