How To Install Hashcat On Ubuntu In 2024

infosecscout.com/install-hashcat-on-ubuntu

Patrick Fromaget

Hashcat is an important tool to have in your tool belt (on your computer at least ^^). I already wrote several tutorials on how to use Hashcat, but today we'll stay focus on the installation, especially on a Linux distribution like Ubuntu.

The easiest way to install Hashcat on Ubuntu is to use the package manager (APT), as Hashcat is now available in the default repositories. The installation command would be: *sudo apt install hashcat*.

If you are used to Linux, you know that it's rarely that simple, so let's take a look at each step to install hashcat on your computer.

Install Hashcat on Ubuntu via APT

Start by updating your system

Master your cyber security skills:
Secure your spot in the Accelerator Program, with early access to exclusive resources. Get 1000+ classes, unlimited mentorship, and more.
New updates are released every day on Ubuntu, and to avoid conflicts, it's always a good idea to start by updating your system, to make sure you are using the latest version available for each package.

You can either use the "Ubuntu Software" app, or simply open a terminal and type the following commands:

```
sudo apt update
sudo apt upgrade
```

```
pat@pat-ubuntu:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  accountsservice apparmor apport apport-gtk base-files bind9-dnsutils
  bind9-host bind9-libs cups cups-bsd cups-client cups-common
  cups-core-drivers cups-daemon cups-ipp-utils cups-ppdc cups-server-common
  dirmngr distro-info-data dnsmasq-base dpkg evince evince-common
  evolution-data-server evolution-data-server-common firmware-sof-signed
  fonts-opensymbol gdm3 gir1.2-accountsservice-1.0 gir1.2-gdm-1.0
  gir1.2-gnomedesktop-3.0 gir1.2-gtk-3.0 gir1.2-gtk-4.0
```

Press "Y" to confirm the upgrade of all the listed packages, and wait a few minutes to get them downloaded and installed on your computer.

If, like on my screenshot, you have plenty of new packages to be upgraded, it's probably a good idea to restart your system before going further.

```
sudo reboot
```

Install hashcat

Once your system up-to-date, you can simply install Hashcat with apt.
In my case, the version available in the repository is the same as on the website directly:

```
pat@pat-ubuntu:~$ sudo apt search hashcat
Sorting... Done
Full Text Search... Done
hashcat/jammy 6.2.5+ds1-2 amd64
  World's fastest and most advanced password recovery utility

hashcat-data/jammy,jammy 6.2.5+ds1-2 all
  Data files for hashcat advanced password recovery utility

hashcat-nvidia/jammy,jammy 20210201 all
  Installs hashcat and its dependencies for users with NVIDIA GPU
```

So, there is no need to install it manually at this point. At least, you should give it a try, and switch to the manual procedure I give later if you experience any issue doing this.
Anyway, for now, just install the main package with:
`sudo apt install hashcat`

This should install all the dependencies (something like 60 other packages on a fresh Ubuntu installation).
Type your user password and press “Y” to confirm the installation.

Note: If you have an NVIDIA GPU on your computer, you should also install the corresponding package for better performances:
`sudo apt install hashcat-nvidia`

Use Hashcat on Ubuntu

Hashcat is now installed on your Ubuntu system. You can use the command directly in a terminal:
`hashcat`

You can for example run a benchmark to make sure everything is working properly:
`hashcat -b`

```
pat@pat-ubuntu:~$ hashcat -b
hashcat (v6.2.5) starting in benchmark mode

Benchmarking uses hand-optimized kernel code by default.
You can use it in your cracking session by setting the -O option.
Note: Using optimized kernel code limits the maximum supported password length.
To disable the optimized kernel code in benchmark mode, use the -w option.

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF,
 DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
================================================================================
================================================
* Device #1: pthread-11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz, 1807/3678 M
B (512 MB allocatable), 1MCU

Benchmark relevant options:
===========================
* --optimized-kernel-enable

-------------------
* Hash-Mode 0 (MD5)
-------------------

Speed.#1.........:   277.5 MH/s (0.87ms) @ Accel:256 Loops:1024 Thr:1 Vec:16
```

I’m testing this procedure on a virtual machine for you, which is not optimized at all, but you get the idea. If you get any error doing this test, you probably need to install additional drivers for your GPU, or just use the CPU which should work natively (it’s generally slower though).

As stated on the hashcat website, each GPU require different prerequisites:

> AMD GPUs on Linux require “RadeonOpenCompute (ROCm)” Software Platform (3.1 or later)
> Intel CPUs require “OpenCL Runtime for Intel Core and Intel Xeon Processors” (16.1.1 or later)
> NVIDIA GPUs require “NVIDIA Driver” (440.64 or later) and “CUDA Toolkit” (9.0 or later)
>
> *Source: Hashcat*

On Ubuntu, it should be a problem as you can easily get them. It might be more difficult on Debian or other systems, as the manufacturers are often not supporting all Linux distributions.

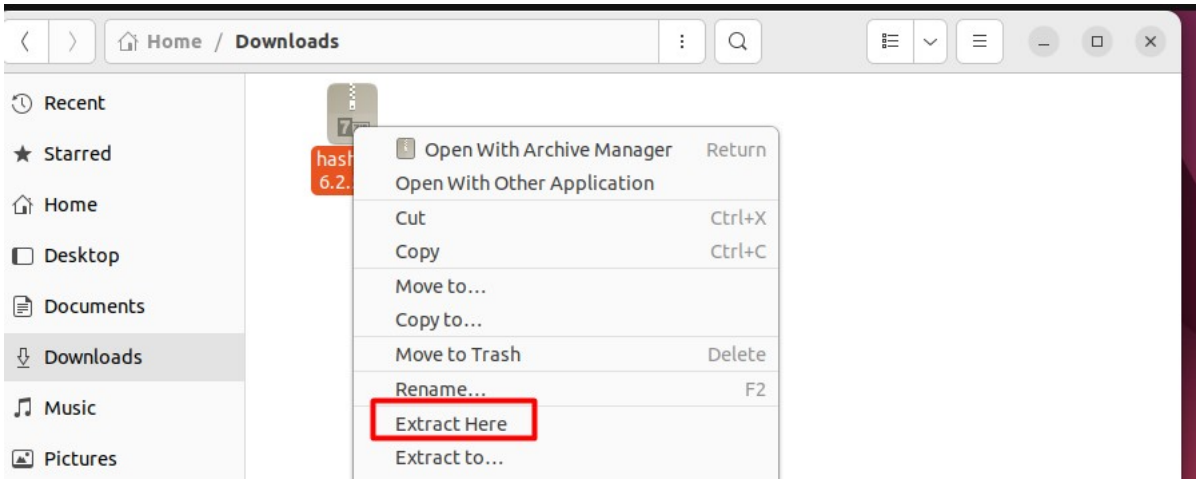
From there, I recommend reading this article to learn how to use hashcat on Ubuntu (or any other system). I explain the different attack modes, and take an example with some MD5 hashes. But the idea is the same with any algorithm once you understand the basics.

Install Hashcat on Ubuntu with the binaries files

If for any reason you prefer to install Hashcat manually on Ubuntu, here is the procedure you can follow instead of using APT:

- Go to the Hashcat website, and get the link to the binaries file.
  You can either download it directly from your web browser, or use the command line:
  `wget https://hashcat.net/files/hashcat-6.2.5.7z`
  Don’t forget to change the file version with the latest one available on the website.

- Extract the file from your file explorer (right-click > extract here):



  Or do it from a terminal with:
  `7z <filename>`
  You may need to install 7zip first, with:
  `sudo apt install p7zip-full`
- Then, open a terminal, and move to the new folder.
  Probably something like:
  `cd Downloads/hashcat-6.2.5/`
- And run the hashcat benchmark with:
  `./hashcat.bin -b`

At this point, you'll likely get an error, as some CPU or GPU runtime will be missing:

```
pat@pat-ubuntu:~/Downloads/hashcat-6.2.5$ ./hashcat.bin -b
hashcat (v6.2.5) starting in benchmark mode

Benchmarking uses hand-optimized kernel code by default.
You can use it in your cracking session by setting the -O option.
Note: Using optimized kernel code limits the maximum supported password length.
To disable the optimized kernel code in benchmark mode, use the -w option.

ATTENTION! No OpenCL, HIP or CUDA installation found.

You are probably missing the CUDA, HIP or OpenCL runtime installation.

* AMD GPUs on Linux require this driver:
  "AMD ROCm" (4.5 or later)
* Intel CPUs require this runtime:
  "OpenCL Runtime for Intel Core and Intel Xeon Processors" (16.1.1 or later)
* NVIDIA GPUs require this runtime and/or driver (both):
  "NVIDIA Driver" (440.64 or later)
  "CUDA Toolkit" (9.0 or later)
```

The previous installation method with APT will do this for you, but in this case you have to install the missing requirements manually.

In my case, the easiest way to fix this was to use apt to install these two packages:
`sudo apt install ocl-icd-libopencl1 pocl-opencl-icd`
But the solution will be different if you have an NVIDIA or AMD GPU. Check this page for

more details for each scenario.

Anyway, I hope this tutorial was useful, and helped you to get started with Hashcat on Ubuntu.
You should now be ready to experiment cool things with this tool, check my other tutorials for more details:

- Is MD5 Easy to Crack? (and how long does it really takes)
- How to Brute Force a Password? (MD5 Hash)
- How to Install and Use Hashcat to Decrypt MD5? (Tutorial)

Whenever you're ready for more security, here are things you should think about: