Getting Started with Hashcat on Kali Linux (Installation guide)

Patrick Fromaget

Hashcat is an important tool to have in your toolbelt (at least on your computer ^^). I've already written several tutorials on how to use Hashcat, but today we'll focus on the installation and first steps, especially on Kali Linux, which is often used for it.

On Kali Linux, Hashcat comes pre-installed with most versions, so you can use it right out of the box. If it's not available on your system, it's in the standard repository and can be installed using APT (the package manager).

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.

How to install Hashcat on Kali Linux (main repository)

Here are a few prerequisites and checks you can do to see if Hashcat is installed, and install it if needed:

- **Keep your system up-to-date before anything else.**
- **List the installed packages and look for hashcat.**
- **Run a benchmark to make sure it's working.**

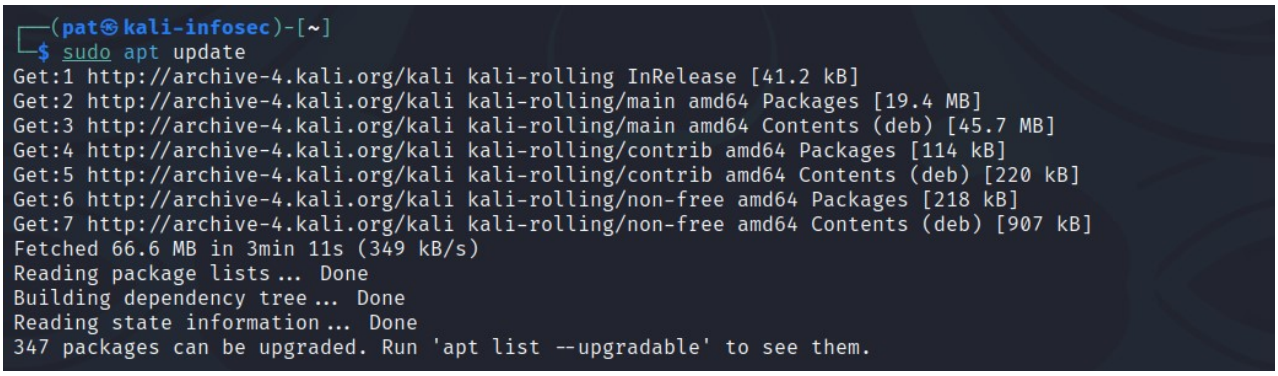
Let's do this in this order.

Update your system

New updates are released on a daily basis. To avoid conflicts and make sure you're installing the latest versions, it's always a good idea to update your system first.

The easiest way to do this is simply to open a terminal and type the following commands:

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



```
┌──(pat㉿kali-infosec)-[~]
└─$ sudo apt update
Get:1 http://archive-4.kali.org/kali kali-rolling InRelease [41.2 kB]
Get:2 http://archive-4.kali.org/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:3 http://archive-4.kali.org/kali kali-rolling/main amd64 Contents (deb) [45.7 MB]
Get:4 http://archive-4.kali.org/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://archive-4.kali.org/kali kali-rolling/contrib amd64 Contents (deb) [220 kB]
Get:6 http://archive-4.kali.org/kali kali-rolling/non-free amd64 Packages [218 kB]
Get:7 http://archive-4.kali.org/kali kali-rolling/non-free amd64 Contents (deb) [907 kB]
Fetched 66.6 MB in 3min 11s (349 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
347 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

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 in my screenshot, you have a lot of new packages to upgrade, it's probably a good idea to reboot your system before proceeding.

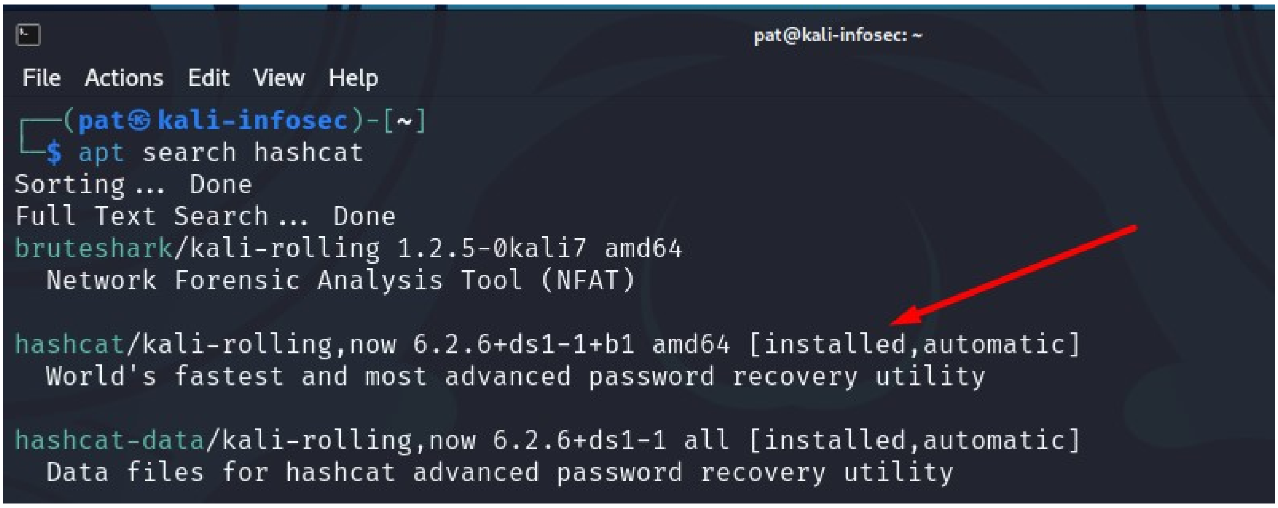
```
sudo reboot
```

Install Hashcat package

As mentioned earlier, in most cases, Hashcat is already installed on Kali Linux if you use a recent version with all the default applications.

Once your system up-to-date, you can use APT to do a search, and see if it's installed:

```
apt search hashcat
```



```
┌──(pat㉿kali-infosec)-[~]
└─$ apt search hashcat
Sorting... Done
Full Text Search... Done
bruteshark/kali-rolling 1.2.5-0kali7 amd64
  Network Forensic Analysis Tool (NFAT)

hashcat/kali-rolling,now 6.2.6+ds1-1+b1 amd64 [installed,automatic]
  World's fastest and most advanced password recovery utility

hashcat-data/kali-rolling,now 6.2.6+ds1-1 all [installed,automatic]
  Data files for hashcat advanced password recovery utility
```

In my case, the version available in the repository is the same as on the website directly. 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, if you don't have the mention "installed" near the package name in the previous command, you can install the main package with:

```
sudo apt install hashcat
```

This should install all the dependencies (something like 60 other packages on a fresh Linux system).
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
```

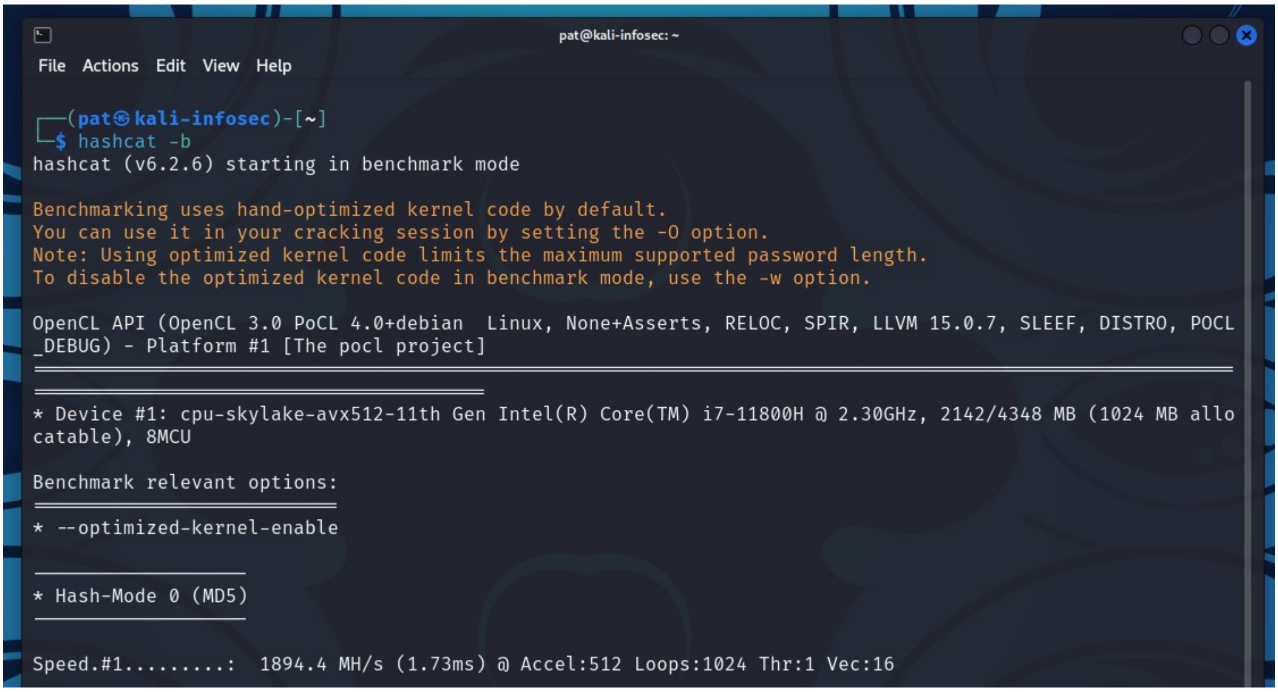
Use Hashcat on Kali Linux

Whether you installed it or it was already there, Hashcat is now available on your 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㉿kali-infosec)-[~]
└─$ hashcat -b
hashcat (v6.2.6) 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 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL
_DEBUG) - Platform #1 [The pocl project]
===========================================================================================================
=======================================

* Device #1: cpu-skylake-avx512-11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz, 2142/4348 MB (1024 MB allo
catable), 8MCU

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

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

Speed.#1.........:  1894.4 MH/s (1.73ms) @ Accel:512 Loops:1024 Thr:1 Vec:16
```

I'm testing this on a virtual machine for you, which is not optimized at all, but you get the idea.

If you get an error during this test, you probably need to install additional drivers for your GPU, or just use the CPU, which should work natively (but is generally slower).

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

> - AMD GPUs on Linux require "AMDGPU" (21.50 or later) and "ROCm" (5.0 or later)
> - AMD GPUs on Windows require "AMD Adrenalin Edition" (Adrenalin 22.5.1 exactly)
> - 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*

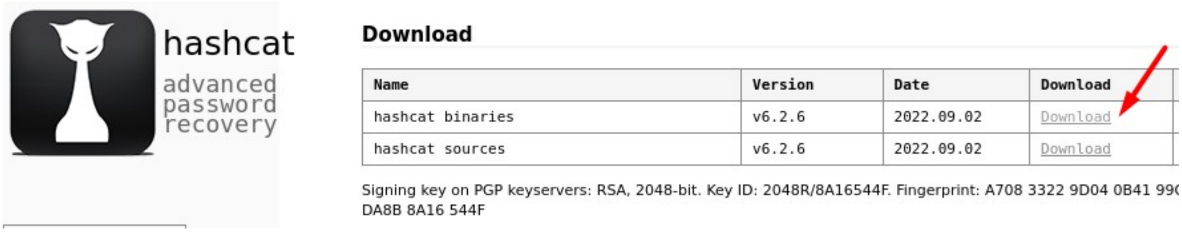
On Linux, it can be difficult to get them, as the vendors often do not support all Linux distributions. But you don't necessarily need the latest version, so try to get them if possible.

From there, I recommend reading this article to learn how to use hashcat. 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 Kali Linux (with the binaries files)

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

- Go to the Hashcat website, and get the link to the binaries file.



Download

Name	Version	Date	Download
hashcat binaries	v6.2.6	2022.09.02	Download
hashcat sources	v6.2.6	2022.09.02	Download

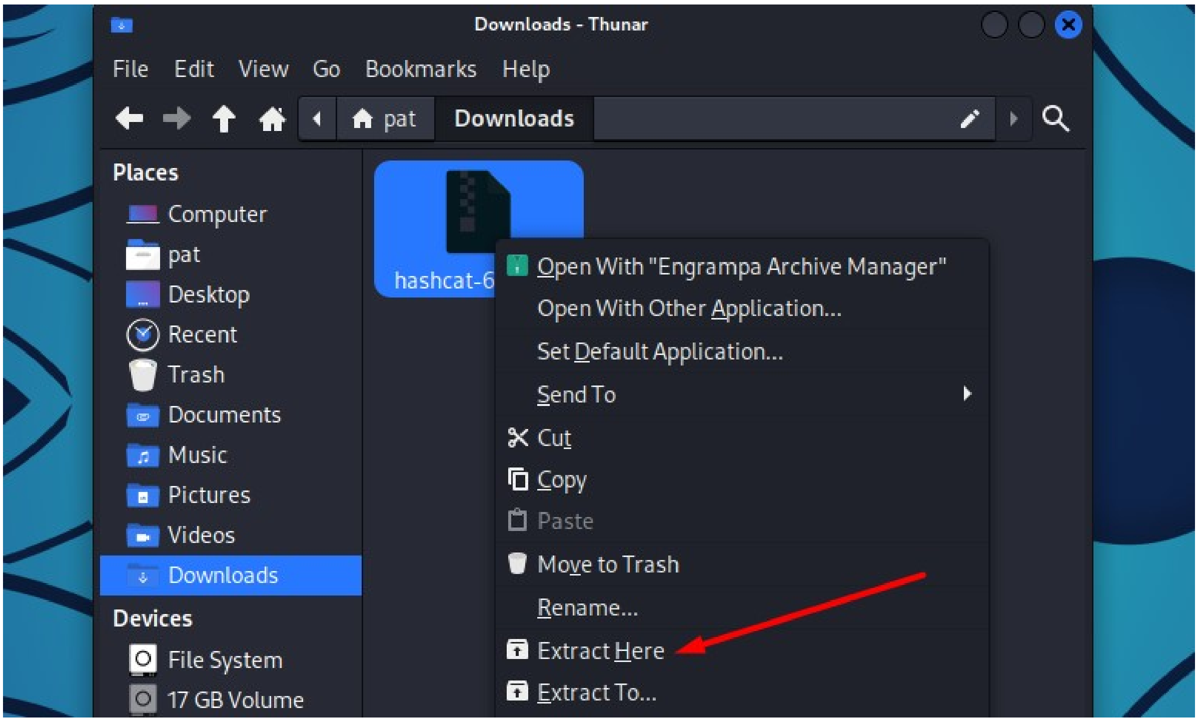
Signing key on PGP keyservers: RSA, 2048-bit. Key ID: 2048R/8A16544F. Fingerprint: A708 3322 9D04 0B41 99(
DA8B 8A16 544F

You can either download it directly from your web browser, or use the command line:

```
wget https://hashcat.net/files/hashcat-6.2.6.7z
```

Don’t forget to replace the file version with the latest one available on the website.

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



Or do it from a terminal with:

```
7z <filename>
```

You may need to install 7zip first, with:

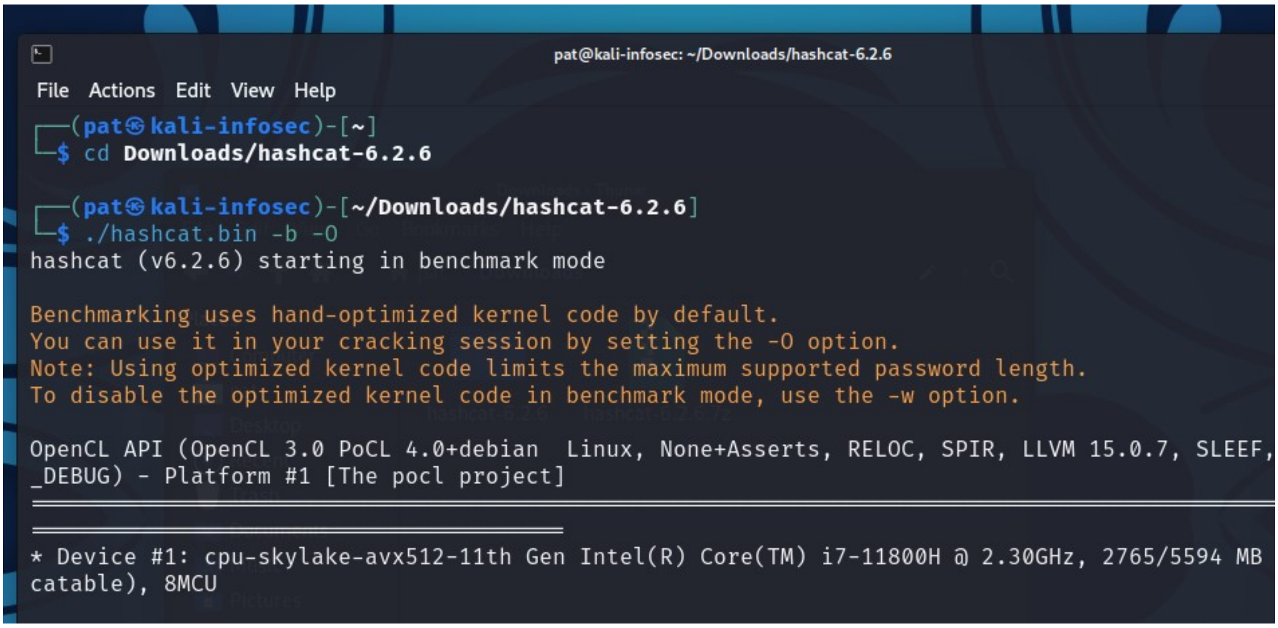
```
sudo apt install p7zip-full
```

- Then, open a terminal, and move to the new folder.
  Probably something like:

```
cd Downloads/hashcat-6.2.6/
```

- 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@kali-infosec: ~/Downloads/hashcat-6.2.6
File Actions Edit View Help

```
┌──(pat㉿kali-infosec)-[~]
└─$ cd Downloads/hashcat-6.2.6

┌──(pat㉿kali-infosec)-[~/Downloads/hashcat-6.2.6]
└─$ ./hashcat.bin -b -O
hashcat (v6.2.6) 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 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF,
_DEBUG) - Platform #1 [The pocl project]
==========================================================================================
========================================
* Device #1: cpu-skylake-avx512-11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz, 2765/5594 MB
catable), 8MCU
```

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 example, the easiest way to fix this was to use apt to install these two missing 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 Kali Linux.
You should now be ready to do cool things with this tool, check out 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: