How To Easily Install Tor on Kali Linux

🔒 **infosecscout.com**/install-tor-on-kali-linux

Patrick Fromaget
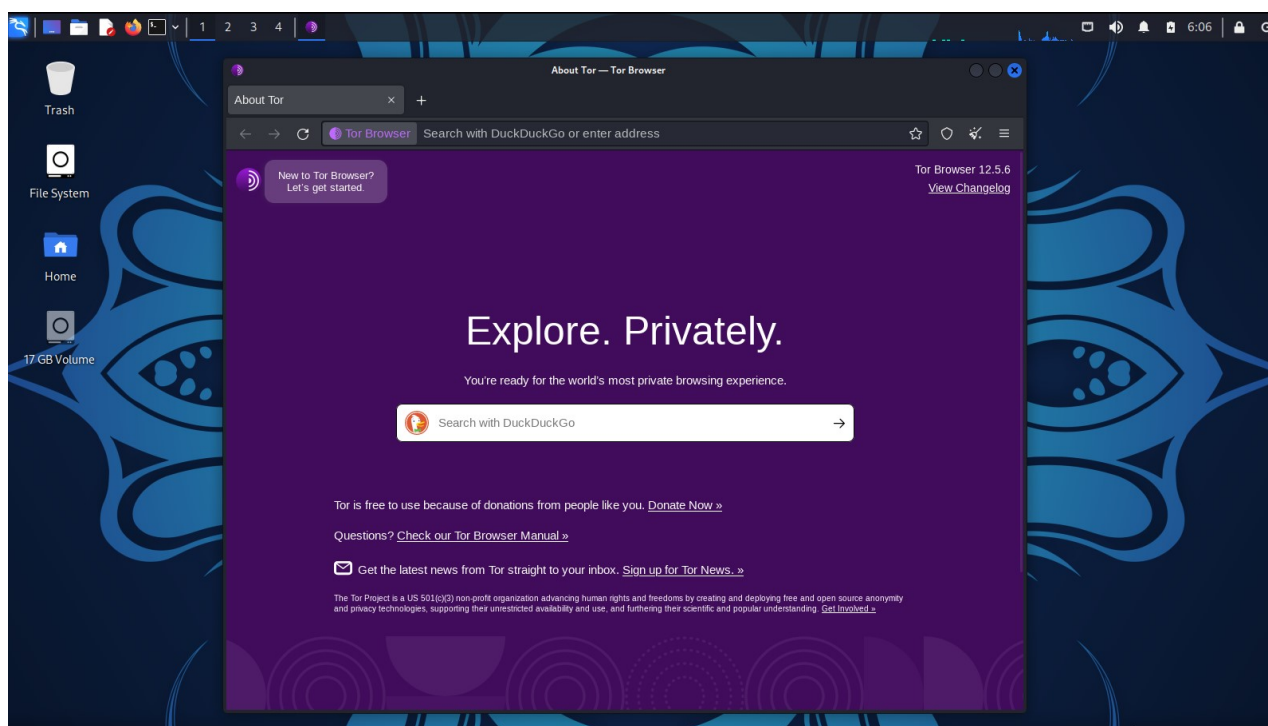
Enabling Tor on Kali Linux is pretty useful and is not that complicated. As often, Kali as everything we need included in the default repository, so it's great. You can quickly switch to the Tor browser if you want to stay anonymous online.

The Tor protocol and the Tor browser are both available by default in the Kali Linux repository. So, Tor can be installed by using the package manager (APT) in one command: "sudo apt install torbrowser-laucher".

Need a more step-by-step guide? Keep reading for the full story about installation and use of this protocol.

Master Linux Commands
Your essential Linux handbook
Want to level up your Linux skills? Here is the perfect solution to become efficient on Linux. **20% off today!**

Download now

How to install Tor Browser on Kali Linux

The Tor Browser is available in the default Kali Linux repositories. The package's name is "torbrowser-launcher" and can be installed with APT in one command.

I like how things are often easier on Kali Linux that a typical Debian system, and it's once again the case with Tor. As it's a common application to be added on this system, they make it easy for us.

Hide your IP address and location with a free VPN:
Try it for free now, with advanced security features.
2900+ servers in 65 countries. It's free. Forever.
You can add the Tor browser to your system by opening a terminal and typing:

```
sudo apt install torbrowser-launcher
```

```
┌──(pat㊉kali-infosec)-[~]
└─$ sudo apt install torbrowser-launcher
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  torbrowser-launcher
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 54.1 kB of archives.
After this operation, 241 kB of additional disk space will be used.
```

It's a small package, with few dependencies, so it should be available quickly.

Getting started with Tor Browser on Kali Linux

Using Tor Browser is not that different from using a traditional web browser. There are just a few things to check on the first run to make sure the Tor network is enabled in the browser configuration.

First start

Once installed, you can start Tor Browser from the main menu, a shortcut has been added under "Internet".
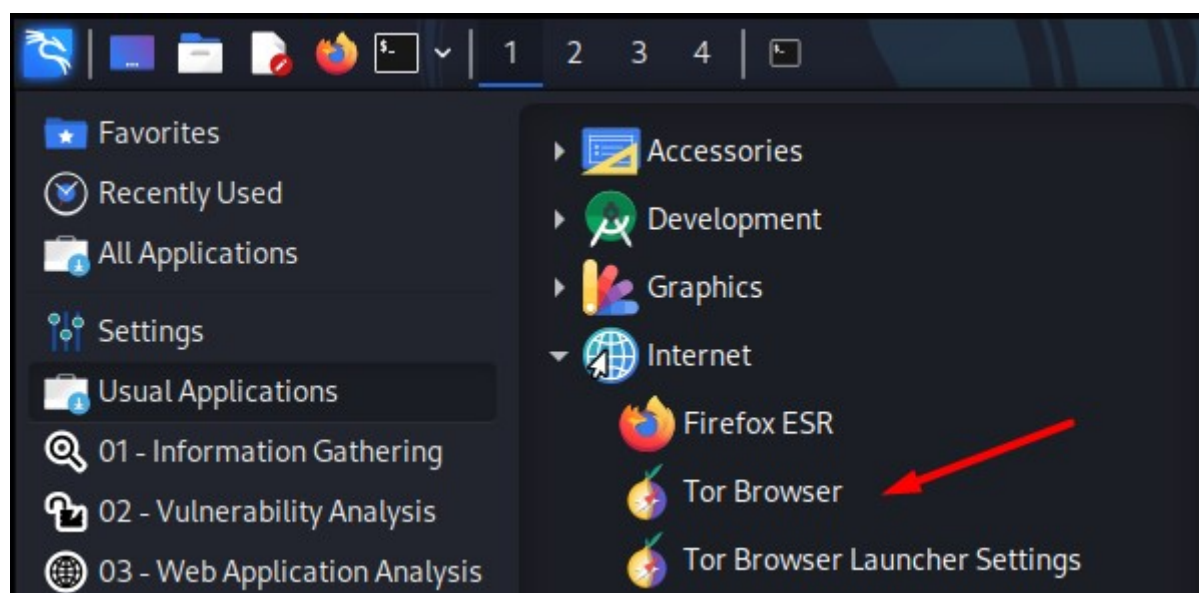
The default Internet icon in the top bar is not updated (still Firefox), which is probably a good thing (you don't need Tor for everything, like reading this tutorial).

Anyway, on the first start, Tor Browser will ask if you want to connect to the Tor network and if it should be done automatically or not. I suggest checking the "Always connect automatically" box, and then click on "Connect".
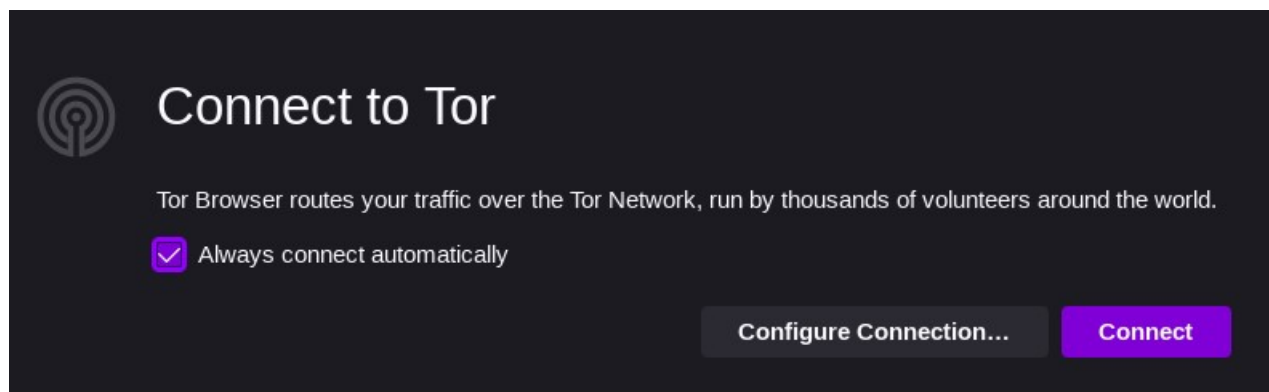
There is no point in using Tor Browser if you don't browse the web via the Tor network, so we might as well enable it all the time. You can decide to use it only for anonymous browsing, and keep Firefox or any other web browser the rest of the time, so you don't have to worry about this.

Once done, you get access to the default page, with DuckDuckGo as the search engine.
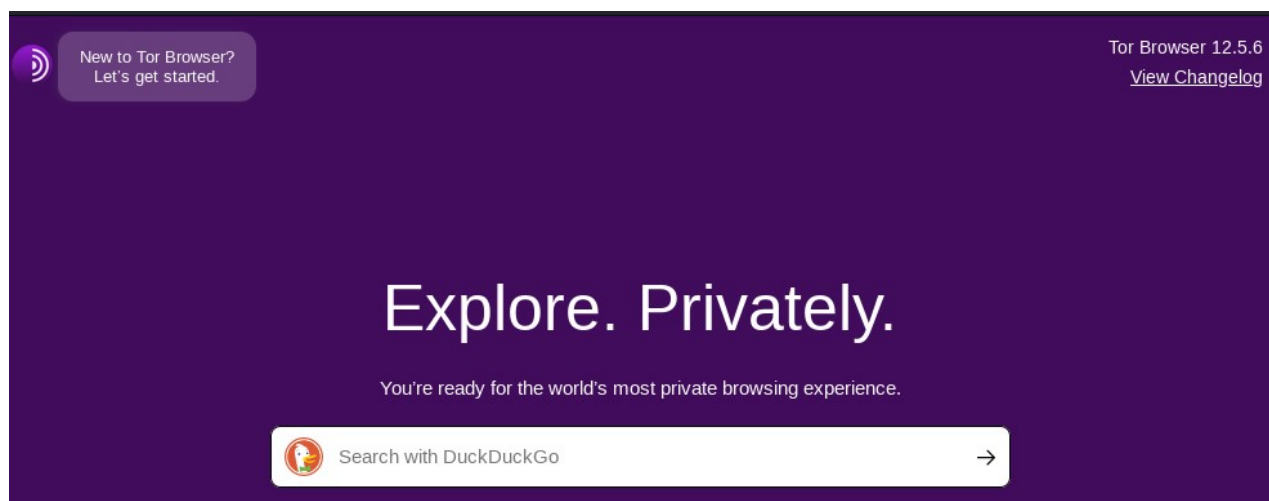
If you don't know, DuckDuckGo is an alternative to the Google search engine that focuses on user privacy. It's a good fit when you use Tor Browser (I guess if you don't want to share your data via the Google browser, you don't want to use their search engine either).

Testing Tor connectivity

One last step, before using Tor Browser like any web browser, is to check that you're properly connected to the Internet via the Tor network.

You can use the official Tor network tool for this, here's the link: http://check.torproject.org/

If you followed this tutorial carefully, you should get a green message, looking like this:

Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **185.220.101.6**

If you get a red message saying that you're not using Tor, you probably missed the previous step, or are not using Tor Browser.

By the way, the IP address mentioned on this page shouldn't be your real public IP address, it's one of the Tor network nodes (the last one you go through I guess).

If I use an IP tester tool to get details about the IP address associated with my connection, it gives me another one, and locates me in the Netherlands (where I'm not):

MY IP ADDRESS

Your IP address is: 192.42.116.189

Estimated location:

City	
Region	
Country	Netherlands

That's the goal of using Tor Browser instead of the other options.

Our connection goes through the Tor network, our public IP is hidden, and the traffic encrypted, which should keep your data and Internet history safe.

Other options and settings

Except for the specific connection method used by Tor Browser, the browser usage in itself is very much like Firefox. This is not a surprise because Tor Browser is based on Firefox.

Hide your IP address and location with a free VPN:
Try it for free now, with advanced security features.
2900+ servers in 65 countries. It's free. Forever.
If you're used to Firefox and open the settings, you shouldn't be lost, that's basically the same:
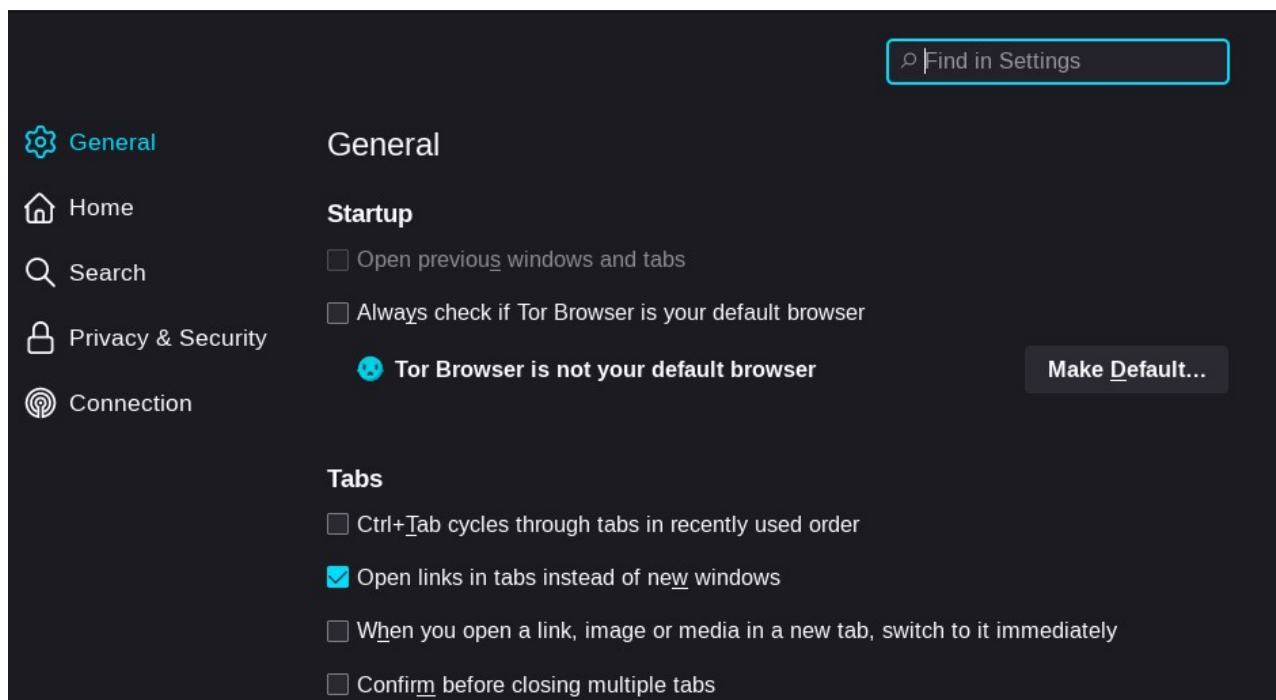
Feel free to browse the options available, change your default browser, search engine or language there if you want.

The only new thing here is the "Connection" tab, which you may need to check if you get issues by using Tor in your country, location, or network. In most cases, you don't have to change anything there.

Final thoughts

Using Tor Browser is great to keep your privacy online, but remember that using Tor Browser will slow down your Internet connection.

I got a speed test of around 75 MB/s with Chromium, but only 15 MB/s via Tor. It's fine if you have a decent connection, but can be very slow if your base speed is already not that good.

Except for that, using Tor Browser is not that different from using Firefox, enjoy!

Want to do more with Kali? Here are a few tutorials you should read next:

- [Brave on Kali Linux: A step-by-step guide](#)
- [50 Basic Linux Commands you Need to Know on Kali Linux](#)
- [Does Kali Linux have a VPN client? (Get one for free)](#)

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

- **Break free from Gmail**: You should be able to choose what happens to your data. With Proton, only you can read your emails. [Get private email](#).

- **Protect yourself online**: Use a high-speed Swiss VPN that safeguards your privacy. Open-source, no activity logs. [Get Proton VPN risk-free](#).

- **Master Linux commands**: A sure method to learn (and remember) Linux commands. Useful ones only, one at a time, with clear explanations. [Download the e-book](#).