

Forum:[Hack Forums](#)

Thread: [Setting up a Hidden Service || .onion](#)

guardian - December 29, 2020, 6:29 am

A quick & dirty tutorial, showing you how to setup your first own hidden service

System: Debian 10

Before you start:

Make sure your hosting providers allows the usage of Tor. A lot of them do not and it might get you into trouble.

To begin, you first have to install tor

Code `apt -y install tor`

When tor has been installed, edit the torrc

Code `nano /etc/tor/torrc`

In there, search for the lines starting with HiddenServiceDir and HiddenServicePort

Uncomment them by removing the # at the beginning of each line

It should then look something like this

I set the port to 80 on localhost, so when I start a local service on port 80, it will automatically be reachable through its hidden service address

Now restart the Tor service, so that changes can take effect

Code `sudo systemctl restart tor`

If we now cd into `/var/lib/tor/hf_tutorial`, we can see that the folder has been created and files have been put into it

The public key and the private key are saved in this directory, as they are needed for the encryption of the hidden service to function properly

authorized is a directory that can be used for client authorization, but this is not something we will go over in this tutorial

Finally, the hostname.

This file contains your onion address, in this case v3.

We will now test our hidden service by running an nginx server and accessing from our onion address

Code `apt -y install nginx`

After installing nginx and changing it's index file, we get the following, when accessing the .onion url from Tor Browser

Congratulations, you just installed your own hidden service!

Of course there is a lot more to do, if you want it to be completely anonymous and bulletproof
But this tutorial should just present you the basics of how things work, hope you enjoyed it

ONiON xmad - January 1, 2021, 2:13 pm

That right there is just starting for brother no offence. Also keep in mind it now seems ready for deployment, but it has 10 times more code than prompted here before it's a real hidden service

guardian - January 1, 2021, 2:21 pm

(Jan 1, 2021 03:13 PM) Onion Breath Wrote: [\[CITE\]](#) That right there is just starting for brother no offence. Also keep in mind it now seems ready for deployment, but it has 10 times more code than prompted here before it's a real hidden service

So you always specify a Hidden Service Dir and comment out that line, when you start Tor?
A hidden service is a service (smtp, ssh, http) that is hosted on the tor network, thus can only be accessed by using tor relays and ends with .onion

As stated in the OP, it is not secure or anything, BUT it is a hidden service

This tutorial is not intended for someone that wants to start a darknet marketplace, more for people that want to get a basic understanding

Edit: Tor's tutorial on how to setup hidden services

<https://2019.www.torproject.org/docs/tor-onion-service.html.en> what did they do to make it a hidden service? or do they not know how to use their own software?

oofa420 - January 3, 2021, 12:46 am

Side-note, you can add in the following to nginx config:

```
Code location /bins/ {  
    autoindex on;  
    allow all;  
}
```

then run `Code mkdir /var/www/tor/bins/`

Then upload and host a file (say... an exe) with it. Just put your bins in the /var/www/tor/bins directory.

Then you can use a tor2web gateway and now you've got file hosting over TOR

Take your onion URL: sfhsidghsigjsdfghkdjfg.onion and make it sfhsidghsigjsdfghkdjfg.onion.pet

.onion.pet does not block anything ;) Use it in a downloader but test it first :)

Not sure how to do on Windows, sorry :(

Turns out they find out rather quickly and block it

ONiON xmad - January 10, 2021, 8:18 am

There is a lot of ways to use and setup tor. I would say I am not comfy with either of those (or everything except tor2web) the other about autoindex etc is fair enough. But also I would like to add to my saying that when I look at hidden service, I mean hidden-hidden, so it's «safe» and «untraceable». Using tor half way in my opinion is like taking a shower with an umbrella above the head. Tor is meant for anonymity, privacy and personal safety.

If this guide was called «how to enable tor and generate a .onion url» I would agree, but it's not at any point a complete setup for a hidden service *my opinion along with privacy geeks*. But then again I would include cathuggers mko224o onion v3 generator for personal v3 domains, or schallot for v2 urls.

I can learn you a thing or two regarding reverse proxy, onionbalance and so on for «real» hidden service, but im currently selling this kind of services, so we will save that for another time.

Have an awesome sunday, dear gentlemen ;-) i might write a guide on this once, will see when i have time.