

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Create a Hidden \(TOR\) Service](#)

The2G - March 13, 2017, 1:32 am

How many of you have heard of a hidden service in TOR like the Silk Road? It's really not some mystical location on the dark side of the Internet, or darknet. While it does sound a bit fantastic, a hidden service in TOR is just a server that is connected to TOR network and is only accessible by a uniquely generated domain name (.onion). The idea is that there aren't supposed to be any IP's associated with the server once it's set up on TOR – making it untraceable. Of course there are ways of exploiting a vulnerability that will reveal that address, but I won't go into that. Essentially a hidden service is just a web service on TOR. In this post, I will show how to create hidden service in TOR like Silk Road or DarkNet.

However, one might think why its necessary to create hidden service in TOR like Silk Road? After all, Silk Road was an illegal service that was taken down. But in many cases It might be necessary not because you want to create something illegal like Silk Road, but it's necessary for the people in oppressed states where you don't have a right to express yourself and you still want information passed onto the outside world. Use it well and for legit purposes.

If you have never used TOR, here's the guide on how to setup TOR in Linux. This guide specifically detail steps required to create hidden service in TOR which can be used on a Kali/Debian/Ubuntu distro etc.

1. Update and upgrade you system

Code `apt-get update`

`apt-get upgrade`

2. Install a Web Server

If you're using Kali Linux, you already have Apache Web Server installed and configured for you. Else install Apache.

Code `apt-get install apache2`

3. Install TOR

Now it's time to install TOR. You can install via apt-get as it's available in any repository. You don't need to download the binary or source code.

Code `apt-get install tor`

4. Edit TOR Configuration file

After you've install TOR, you need to open the configuration file and edit it. It's usually in `/etc/tor/` folder. Use your favorite editor.

Code `vi /etc/tor/torrc` You should change the port numbers in the configuration file. Verify the IP you web server is listening on (change it if you want). I use 6666. What happens in the configuration file is that the TOR service will listen on a certain port and address (accessible only via TOR) and then redirect that traffic to your Web Server.

In the configuration file navigate to the first instance of this:

Code `HiddenServiceDir /Library/Tor/var/lib/tor/hidden_service/`

`HiddenServicePort 80 127.0.0.1:8080`

The HiddenServiceDir field is a directory location (non-arbitrary) in which you specify where you want TOR to create your key and .onion address (hostname). It will generate two files in the directory to which you point it, one for each artifact (see step 6).

The HiddenServicePort field is where you specify which ports you want TOR to listen on and to redirect to.

So in my case, I have TOR listening on port 7777 which then redirects to my Apache Web Server on 6666 (which is what I configured Apache to listen on). So when I navigate to my .onion address on port 7777, I will be sent to the home directory of my Apache server (/var/www). Remember that whatever web server you are running, your traffic will be directed to the HOME directory of that server, wherever that may be. Make sense?

In my case, my torrc file contains these two fields:

```
Code HiddenServiceDir /var/lib/tor/hidden_service
HiddenServicePort 6666 127.0.0.1:7777
```

127.0.0.1:7777 is what TOR is listening on, and 6666 is where it is redirecting (and where Apache is listening). It doesn't matter if Apache is listening on a port that is public or private (localhost). If you have Apache listening on a port on your public interface, then you should block it at the firewall so as to not leave the Web Server open to the world.

Again, by default the TOR service will point to your Web Server's default directory. So in my case when I navigate to my hidden service I get dropped into /var/www. You might be able to change this. You can also have more than one hidden service running at once. Just repeat this configuration for each instance and create different directories on your Web Server.

So to bring this configuration into perspective, let me summarize. You have a TOR service listening on a certain port on a uniquely generated .onion URL that redirects traffic to whatever port your Web Server is listening on. Keep in mind that you are still connected to the internet on your normal IP and your Web Server can get pwned if you make whatever port it's listening in on available to the outside! You should only open up the port that TOR is listening on in your firewall configuration.

Your service will only be accessible via the .onion address so you don't have to worry about people stumbling upon it by accident (unless they guess or steal your .onion address – which should be difficult).

5. Start required services

Start the TOR service and Web Server:

```
Code tor
service apache2 start
```

6. Sit back and enjoy

When you start the tor service for the first time it will generate your key and hostname in the directory you specified in the configuration file. Navigate there and copy your address. This is the URL for your .onion address.

Conclusion

There are some anonymity issues you should keep in mind too:

- As mentioned above, be careful of letting your web server reveal identifying information about you, your computer, or your location. For example, readers can probably determine whether it's httpd or Apache, and learn something about your operating system.
- If your computer isn't online all the time, your hidden service won't be either. This leaks information to an observant adversary.
- It is generally a better idea to host hidden services on a Tor client rather than a Tor relay, since relay uptime and other properties are publicly visible.
- The longer a hidden is online, the higher the risk that its location is discovered. The most

prominent attacks are building a profile of the hidden service's availability and matching induced traffic patterns.

Though tracing something like this will take months of collaboration between TOR service providers and Exit Gateways, but it can be traced. Nothing is untraceable, it just takes time and efforts. Use this guide for educational purposes only.

PD: I just consider that post interesting and I think that should be in this forum too. The original post was not written by me. Hope is useful for you.

Original Post:

<https://www.blackmoreops.com/2015/08/19/create-hidden-service-in-tor-like-silk-road-or-darknet/>

Hopsin - March 13, 2017, 3:33 am

Although I don't need this, thanks for your contribution buddy. Have a nice day! ?

Signature ~ Best regards, Hopsin.

The2G - March 13, 2017, 3:38 am

(Mar 13, 2017 03:33 AM)Hopsin Wrote: [\[CITE\]](#) Although I don't need this, thanks for your contribution buddy. Have a nice day! ?

Signature ~ Best regards, Hopsin.

Thanks!

Hope is useful for other users. :)

Hopsin - March 13, 2017, 3:42 am

(Mar 13, 2017 03:38 AM)Rubba Wrote: [\[CITE\]](#) Thanks!

Hope is useful for other users. :)

No problem mate, just a tip by the way, you could add some coloring in the thread. It can make it a little more attractive ??

Cavs23 - March 13, 2017, 4:47 am

Thanks mate I can now sell drugs on the darkside

The2G - March 13, 2017, 6:07 am

(Mar 13, 2017 03:42 AM)Hopsin Wrote: [\[CITE\]](#) No problem mate, just a tip by the way, you could add some coloring in the thread. It can make it a little more attractive ??

Thanks for the suggestion. I'll make it up to make it better looking.

(Mar 13, 2017 04:47 AM)Cavs23 Wrote: [\[CITE\]](#) Thanks mate I can now sell drugs on the darkside Could be a possibility. But not allowed to speak about that in the forum.

Edward.Whitney - March 13, 2017, 7:56 pm

Thank you.i need this.Can you provide this service?

MotoSwap - March 13, 2017, 7:59 pm

Awesome. I didn't read all of it but it looks like you've got shti figured out for us Noobs

The2G - March 14, 2017, 2:00 am

(Mar 13, 2017 07:56 PM)Edward.Whitney Wrote: [\[CITE\]](#) Thank you.i need this.Can you provide this service?

No I don't provide that service sorry. You could rent a VPS o a Dedicated server in this forum or with other providers and set up teh service following this tutorial.

(Mar 13, 2017 07:59 PM)MotoSwap Wrote: [\[CITE\]](#) Awesome. I didn't read all of it but it looks like you've got shti figured out for us Noobs

Yes, I think that a beginner could follow without any issue.

Leroy Jethro Gibbs - March 14, 2017, 2:03 am

I don't believe you can make this tutorial. Darkweb/deepweb discussions are not allowed.

The2G - March 14, 2017, 2:07 am

(Mar 14, 2017 02:03 AM)Leroy Jethro Gibbs Wrote: [\[CITE\]](#) I don't believe you can make this tutorial. Darkweb/deepweb discussions are not allowed.

Okay... So I guess a moderator have to close/delete it.

Sorry.

Leroy Jethro Gibbs - March 14, 2017, 2:08 am

(Mar 14, 2017 02:07 AM)Rubba Wrote: [\[CITE\]](#) Okay... So I guess a moderator have to close/delete it.

Sorry.

I'd message a staff member and ask if its allowed. Tell them to delete it if its not allowed. It will save you a warning.

The2G - March 14, 2017, 2:09 am

(Mar 14, 2017 02:08 AM)Leroy Jethro Gibbs Wrote: [\[CITE\]](#) I'd message a staff member and ask if its allowed. Tell them to delete it if its not allowed. It will save you a warning.

Okay. Thanks!