

# Forum:[Hack Forums](#)

Thread: [\[Tutorial\] How to host a TOR hidden service](#)

Lrrr - August 31, 2016, 4:49 pm

## IMPORTANT NOTE:

This is a minimal hidden service setup. This guide is not intended to be used to host illegal or otherwise dissalowed activities and is not designed to keep you anonymous. If you use this setup to host anything that could be considered "blackhat" you will most likely be de-anonymized and busted! This is for educational purposes only.

Note: This setup is for LINUX, if you would like to set up a TOR Hidden Service. [Click here for WINDOWS TOR Hidden Service](#).

## How to host a TOR hidden service

Purpose: The purpose of this tutorial is to show users how to:  
Install and Configure TOR  
Setup a simple Hello World website  
Configure a hidden service  
Generate an .onion host (and how to customize it!)

## Chapter 0: Prerequisites

Requirements: Fresh Linux Server (For this tutorial, I will be using: Ubuntu Server 14.04)  
Basic Knowledge of Linux  
1 Hour of Time

## Chapter 1: Initial Setup

### Server:

I have opted to use Amazon Web Services (AWS) for this tutorial. I am using ami-2d39803a, here are my instance details:

Spoiler [\(Click to View\)](#)

Don't worry about the security groups warning just yet, we will fix that later on.

Click Launch and you will get to a PEM key download page. Use an existing PEM or create a new one. I created a new one, named it Lrrr, and downloaded it...

Spoiler [\(Click to View\)](#)

Now that our instance is setup, we should have a public IP address assigned to us from AWS, time for the fun stuff.

Connect to your instance with the PEM you downloaded earlier  
Code `ssh -i my_pem.pem -l ubuntu <instance IP address>`

NOTE: As a member pointed out, if you are on windows and using putty;

(Sep 1, 2016 11:10 PM)RYDIOO Wrote: [\[CITE\]](#) One thing for anyone trying to connect to the instance with Putty. You need to download Putty Gen and change your .pem file into a putty private key (a .ppk). Then underneath Auth in putty you should be able to select the key. Thank you RYDIOO!

Let's add some sources, and update the box:

Code `sudo nano /etc/apt/sources.list`

At the end of the sources.list file, paste this:

Code `#Tor`

`deb http://deb.torproject.org/torproject.org trusty main`

`deb-src http://deb.torproject.org/torproject.org trusty main`

CTRL+X and Y to save the file.

Now we need to add our keys, update the repo's, and install tor,nginx,make, and gcc:

Code `sudo gpg --keyserver keys.gnupg.net --recv 886DDD89`

`sudo gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add -`

`sudo apt-get update`

`sudo apt-get upgrade -y`

`sudo apt-get install tor deb.torproject.org-keyring -y`

`sudo apt-get install gcc unzip make libcurl4-openssl-dev nginx -y`

`sudo apt-get dist-upgrade`

If all of this goes as planned, you should be able to run the following command and the output should say TOR is running:

Code `$ service tor status`

`* tor is running`

If you have anything other than \* Tor is running, check the output for any failures and post them here.

## Chapter 2: Firewall & Routing

Remember when I said we would worry about the security group policies at a later time? Now is that time! Head back over to your AWS instance panel, highlight your instance, and choose "launch-wizard-n" where n is whatever the auto-increment has made it to, ie: launch-wizard-30.

Once you are at the Security Groups screen, you will see four (4) tabs in the bottom pane, click the INBOUND pane and select EDIT. If you have been following this guide, a single SSH rule exists for source "Anywhere". Change that source to "My IP". Save.

Because TOR works off a socks proxy, there is no need to open any ports other than port 22 (ssh) to access the server.

## Chapter 3: Generating an .onion Host

Now that we have tor running, we need to make some modifications to our torrc file.

Code `sudo nano /etc/tor/torrc`

find and remove the # symbol from the following:

```
#RunAsDaemon 1
#DataDirectory /var/lib/tor
#HiddenServiceDir /var/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80
```

The first option will run tor as a daemon

The second will set the main data directory to /var/lib/tor

The third will set a hidden service to be found in /var/lib/tor/

The fourth is stating port 80, meaning we want the hidden service to be some type of website.

Now when you restart tor, it will create the hidden\_service directory and generate a new onion hostname:

```
Code service nginx start; sudo service tor restart;
```

```
* Stopping tor
```

```
daemon... [ OK ]
```

```
* Starting tor
```

```
daemon... [ OK ]
```

```
sudo cat /var/lib/tor/hidden_service/hostname
```

```
3pet3xqf7phhqufd.onion
```

This should work \*out of the box\*. To test, go ahead and open your tor browser and head to the onion host you got from the last command and you should see:

```
Code Welcome to nginx!
```

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org).

Commercial support is available at [nginx.com](http://nginx.com).

Thank you for using nginx.

Spoiler ([Click to View](#))

## Chapter 4: Onion Host Customization

So a random .onion host isn't cutting it for you, and you want a fancy host with some custom letters in the host...something like HFGodxqf7phhqufd.onion (not a real onion as of 31/08/2016)

For this, we will need to use a tool to basically "brute" (for lack of a better term). There are a few tools to help you do this: Onionhash - Linux

Shallot - Linux

Eschalot - Linux

Scallion - Linux

Garlic - Windows

For this tutorial, I will be setting up and using Shallot, because I think it's the easiest to setup. Login to your server and run the following:

```
Code sudo su
```

```
cd ~
```

```
wget https://github.com/katmagic/Shallot/archive/master.zip
```

```
unzip master.zip
```

```
cd Shallot-master/  
./configure && make  
cp ./shallot /usr/bin/shallot; chmod +x /usr/bin/shallot;  
Now that we have shallot installed as a global script, we can test this by generating a test host:
```

Code shallot ^Hack

This will start a search/brute of any onion host starting with "Hack"....according to Shallot's github page the following breakdown for how long this should take is as follows:

| Characters | Time to generate   |
|------------|--------------------|
| 1          | Less than 1 second |
| 2          | Less than 1 second |
| 3          | Less than 1 second |
| 4          | 2 seconds          |
| 5          | 1 minute           |
| 6          | 30 minutes         |
| 7          | 1 day              |

As you can see, the more precise you try to get, the longer it takes to generate the required keys.

For this test, I used the term "lol" to make a match quickly.

Code shallot ^lol

```
-----  
Found matching domain after 17215 tries: lolaklefegef7caci.onion  
-----
```

-----BEGIN RSA PRIVATE KEY-----

```
MIICXAIBAAKBgQCmFppQ4OfaY1RljHXBRA0KjwT/NkqlxwGFYV3ExxBzYidlhi8b  
qoTvYu0B/WCFcV9i8ZjcEDXB+BNdGMcDeBeL5LK4hHW+EMwIOTZOyVcoDHWJjIQq  
x4T4V7IPP8eTdbuqCqRuzwOxuw7iUCLn5wy/wdtmRoNQOwloOFex9QauwIDAUw7  
AoGAJ6PaljNDkMTVa9sr7wv5Nz4R1zd1VAm5eC6XsMKTs/WudoBEE8cR0BGsWbL4  
HL4J6QSAthUdkZMljy9FOifYG5Oa1gEcys4u46Xqh3f+BuQUIMuHX8n6Lod1n7cQ  
WC5KJRjWf3hAC+aVumhGxv632WAKpVBbkQEnhwgr0MWyNMMCQQDTILbUMub5r4hg  
uq0VgAYHljdmU95wC9m/56dCyCmiqB/QjNTpMqL88Dfo5mE0/aQr6pEjqRfCxIHl  
6POal8ppAkEAyPTqaSZxkPwZkJ4tgKlvfli3XrybbY5E1q1u3kl6L8KY2/YlagaA  
o60thbgUEQNIRjfgelTB/Rg9HuAua8RvgwJAX0a2GNtHfjIBIEeKPUNm7oe/4nRO  
/XJfRRKV15mitkThfjVSbf0pAR6dP1tfnpTx9uXygh1RUDK/3MKVIAw0WwJAFhK1  
W0S5Ge1eDlaVAB1mAvzJHLQTa4MzQDMWf7h/bXvd3l6vcUPZ8vg5ZDpLjooGP3H2  
mJArAOTWMIqliB/XJwJBAJro6e0qo2htUParsFteTxze4/1aGcdVrBwntPlc1uvD  
Ri9aVGOnBdrTrVsOxzXSa6NcfNxqo90po6FGvHtknBE=
```

-----END RSA PRIVATE KEY-----

Now, with this info we can set your new host:

```
Code cd /var/lib/tor/hidden_service/  
echo "lolaklefegef7caci.onion" > hostname  
echo "" > private_key; nano private_key;  
now paste the key Shallot gave you into the private_key file and restart tor.
```

Code service tor restart

\* Stopping tor daemon...

\* Starting tor daemon...

Open TOR browser and direct it to your new host: lolaklefegef7caci.onion

[ OK ]

[ OK ]

You should see your "Welcome to nginx!" message again.

## Conclusion

Hopefully this tutorial helped you, if you have any questions on how or why this setup works, please don't hesitate to post below.

-Lrrr

**Lucent** - August 31, 2016, 4:50 pm

Great tutorial OP!

Bookmarking this to read all of it later.

**Regulus** - August 31, 2016, 5:05 pm

This is one amazing and detailed tutorial Lrrr.

Great job my man!

**Lufasu** - August 31, 2016, 5:05 pm

Amazing HQ tutorial by HQ user :)!

**SIM-2015410** - August 31, 2016, 5:51 pm

Very nice tutorial, thanks for sharing this Lrrr ?

**duisucks** - August 31, 2016, 6:05 pm

This guide is very helpful to a lot of people thank you mate.

**Lrrr** - September 1, 2016, 10:33 am

Thank's guys, let me know if you need help setting this up on your own!

**Mino** - September 1, 2016, 10:34 am

I was 99.9999999% sure we could not discuss this stuff on Hf? Am I mistaken?

**Pharaoh1100** - September 1, 2016, 10:34 am

LOL, I'm glad someone copied + pasted this tutorial from other places. This tutorial is nowhere near being new. Great leeching, OP! Never thought this forum would partially mirror L•eakForums

<https://www.torproject.org/docs/tor-hidden-service.html.en>

I don't think that, you OP, realize the consequences, and the other lots of security measurements, which should be taken regarding having a darknet web server. Ubuntu is the WORST distribution of choice for this. If you're familiar with the development of the distribution, you'd know. I can't bother explaining. You can't just blindly-guide a lot of unacknowledged people like this.

**Lrrr** - September 1, 2016, 11:34 am

(Sep 1, 2016 10:34 AM)Pharaoh1100 Wrote: [\[CITE\]](#) LOL, I'm glad someone copied + pasted this tutorial from other places. This tutorial is nowhere near being new. Great leeching, OP! Never thought this forum would partially mirror L•eakForums

<https://www.torproject.org/docs/tor-hidden-service.html.en>

I don't think that, you OP, realize the consequences, and the other lots of security measurements, which should be taken regarding having a darknet web server. Ubuntu is the WORST distribution of

choice for this. If you're familiar with the development of the distribution, you'd know. I can't bother explaining. You can't just blindly-guide a lot of unacknowledged people like this.

Since I wrote the entire thing myself, I'd love for you to show me where I copied pasted anything. Thanks <3

**Pharaoh1100** - September 1, 2016, 11:35 am

(Sep 1, 2016 11:34 AM)Lrrr Wrote: [\[CITE\]](#) Since I wrote the entire thing myself, I'd love for you to show me where I copied pasted anything. Thanks <3

Right from where I've posted the link ?

This is way too basic information. You're not the first one to create this type of a tutorial.

**Lrrr** - September 1, 2016, 11:36 am

(Sep 1, 2016 10:34 AM)Mino Wrote: [\[CITE\]](#) I was 99.9999999% sure we could not discuss this stuff on Hf? Am I mistaken?

We can discuss TOR and how it works, we can NOT discuss the other shit that happens there...

(Sep 1, 2016 11:35 AM)Pharaoh1100 Wrote: [\[CITE\]](#) Right from where I've posted the link ?

This is way too basic information. You're not the first one to create this type of a tutorial.

My tutorial at the very top stated "do not use this for blackhat or you will be de-anonymized". I did not cover any type of black-hat related topics because it is against HF rules.

And again, it is written word for word by me ?

**Pharaoh1100** - September 1, 2016, 11:43 am

(Sep 1, 2016 11:36 AM)Lrrr Wrote: [\[CITE\]](#) My tutorial at the very top stated "do not use this for blackhat or you will be de-anonymized". I did not cover any type of black-hat related topics because it is against HF rules.

And again, it is written word for word by me ?

You're only proving of having no idea about what you're writing. First of all, security measurements have nothing to do with Blackhat. These are 2 absolutely different things. Security measurement while imposing something illegal (blackhat) is called OpSec as an abbreviation of Operation Security. And operation security can be implemented not just for blackhat-related activities, but over-all because you have the will and rights to do so. Mostly, to defend yourself or something yours from receiving malicious files, or being targeted by malicious hackers. I.e: using a VPN for educational purpose, or just to hide your real IP by encrypting your network data.

It's not called a hidden service. These are the key-words exposing that you're leeching this information from another source, just a little re-modifying the form and structure of text. Yeah, there is some information added by you, but it's completely arrogant to say that this tutorial is 100%-written by you. This information exists way before your acknowledgement. It's called a darknet web server. It's called "hidden service", because it contains hidden partitions, ultimately spoofing a lot of things.

It's all ok just to mention that your tutorial is not fully-written by you.

**Lrrr** - September 1, 2016, 11:56 am

Quote:You're only proving of having no idea about what you're writing. First of all, security measurements have nothing to do with Blackhat. Are you aware of the rules on HF related to TOR? You should take this time to get acquainted with them.

Quote:It's not called a hidden service. That's literally what it's called....

Quote:These are the key-words exposing that you're leeching this information from another source, just a little re-modifying the form and structure of text. Yeah, there is some information added by

you, but it's completely arrogant to say that this tutorial is 100%-written by you. While the subject of setting up a hidden service may very well have been covered countless time, I again state this tutorial is written by me. Sorry bro, I am still waiting for you to prove otherwise. Pro-tip: You can't

Quote:This information exists way before your acknowledgement. I agree

Quote:It's called a darknet web server. It's called "hidden service", because it contains hidden partitions, ultimately spoofing a lot of things. Didn't you tell me just above that it's NOT called a hidden service? Furthermore there is no hidden partition broski, its simply a SOCKS proxy loop into the TOR node.

Quote:It's all ok just to mention that your tutorial is not fully-written by you. ....but it is, and your just being a LQ troll. I'm done with your silly arguments. Believe whatever the fuck you want.

**Pharaoh1100** - September 1, 2016, 12:03 pm

(Sep 1, 2016 11:56 AM)Lrrr Wrote: [\[CITE\]](#) While the subject of setting up a hidden service may very well have been covered countless time, I again state this tutorial is written by me. Sorry bro, I am still waiting for you to prove otherwise. Pro-tip: You can't

I agree

This is, literally, what leeching means, and you're confirming it. The information is freely-available anywhere else, but you've just took it and compiled it into a tutorial, ultimately leeching this information.

Let me simplify the meaning. This tutorial is written by you, but the information is taken from other places, which leads to leeching information.

Malicious hackers could target not just black-hat-related activity, but anything legal as well. Ergo, security measurement, ergo OpSec, ergo hackers could target your "hidden service". Thus, security measurements could be used not only for OpSec in regards of being secure, while imposing your activity to something illegal.

Hopefully you understand what I'm trying to say. I appreciate the effort putten into compiling it in a tutorial, but there is a huge amount of other tutorials. You should mention with what, your tutorial, is special.

**Skeetz** - September 1, 2016, 1:35 pm

This is against HF's rules. Discussion of the deep web is not allowed.

**Lrrr** - September 1, 2016, 1:53 pm

(Sep 1, 2016 01:35 PM)Skeetz Wrote: [\[CITE\]](#) This is against HF's rules. Discussion of the deep web is not allowed.

Discussion of TOR and how it works is allowed. Please feel free to report this post, but I already had it OKed by staff.

**SIM-2848947** - September 1, 2016, 11:10 pm

Kind of laughing at some of the replies right now xD Good work Lrrr. The tutorial does what it intends and does it well.

One thing for anyone trying to connect to the instance with Putty. You need to download Putty Gen and change your .pem file into a putty private key (a .ppk). Then underneath Auth in putty you should be able to select the key.

I remember having problems with that first time I used ec2 and then relising how much of an idiot I was being.

**Aliasllias** - September 1, 2016, 11:14 pm

Thanks for this HQ tutorial, will read it better when I have some more time.

**Lrrr** - September 2, 2016, 12:22 am

(Sep 1, 2016 11:10 PM)RYDIOO Wrote: [\[CITE\]](#) One thing for anyone trying to connect to the instance with Putty. You need to download Putty Gen and change your .pem file into a putty private key (a .ppk). Then underneath Auth in putty you should be able to select the key.

I remember having problems with that first time I used ec2 and then relising how much of an idiot I was being.

Great point, sorry I totally forgot about the windows thing. PuttyGen is avabile at the official putty site. As RYDIOO stated, convert the pem to a ppk file to connect if you are using AWS. QUOTES this in the tutorial

**ShNuG** - September 3, 2016, 12:22 pm

Amazing, Tutorial. Can you please add or make another thread on making it truly anonymous ? :)

**Lrrr** - September 3, 2016, 1:33 pm

(Sep 3, 2016 12:22 PM)Topher Brink Wrote: [\[CITE\]](#) Amazing, Tutorial. Can you please add or make another thread on making it truly anonymous ? :)

I could probably make another tutorial about securing a system that runs a tor bridge for countries that monitor tor usage....

I'm not sure when exactly I could get around to writing it though, but thats what you would want to look into.

Basically, a hardened minimal OS, with OpenVPN as a gateway for your second minimal application instance. Look into the way Whonix operates :)

**Pharaoh1100** - September 4, 2016, 12:43 pm

(Sep 3, 2016 12:22 PM)Topher Brink Wrote: [\[CITE\]](#) Amazing, Tutorial. Can you please add or make another thread on making it truly anonymous ? :)

Securing the server sounds easy, but it requires a lot of work. First of all, you should be acknowledged about the exploits, to which protocols are vulnerable in the Tor and network sphere. Be sure to, either have you, or someone from your team, that follows the news regarding exploits and such, then patch them as soon as you get acknowledged.

Your site's vulnerabilities.

And then the easiest, but most work-requiring thing, have a virtual machine, inside a virtual machine. Not a RDP, nor a VPS, but a VM.

VM (1) Whonix Gateway > VM (2) Tails Linux > VM (And here's where you should configure, modify, and host your server) (3) I'd go for Kali Linux.

Use a proxifier, and SSH tunneling routed through Tor in the end of the virtual machine chain.

Have your own dedicated server, and run your own proxy on it, which you could use with the proxifier as a great advantage, such as DDoS immunity. Not fully, but it's strong.

Hosting a darknet service requires a lot of work. You'd need, not only experienced, but a staff that is experienced and trust-worthy.

AND, always, PATCH, PATCH, PATCH.

If there's a Tor update, UPDATE IT! If you don't, you'd be vulnerable to exploits.

ALSO, Tor bridge relays <https://www.torproject.org/docs/bridges.html.en> so that your VPNP/ISP wouldn't know, if you're using Tor network.

And also, if you have an experienced russian friend, this is of an enormous priority.

Russian hackers are the most skillful ones, followed by asian hackers.

**Lrrr** - September 5, 2016, 7:02 pm

(Sep 4, 2016 12:43 PM)Pharaoh1100 Wrote: [\[CITE\]](#) Securing the server sounds easy, but it requires a lot of work. First of all, you should be acknowledged about the exploits, to which protocols are vulnerable in the Tor and network sphere. Be sure to, either have you, or someone from your team, that follows the news regarding exploits and such, then patch them as soon as you get acknowledged.

Your site's vulnerabilities.

And then the easiest, but most work-requiring thing, have a virtual machine, inside a virtual machine. Not a RDP, nor a VPS, but a VM.

VM (1) Whonix Gateway > VM (2) Tails Linux > VM (And here's where you should configure, modify, and host your server) (3) I'd go for Kali Linux.

Use a proxifier, and SSH tunneling routed through Tor in the end of the virtual machine chain.

Have your own dedicated server, and run your own proxy on it, which you could use with the proxifier as a great advantage, such as DDoS immunity. Not fully, but it's strong.

Hosting a darknet service requires a lot of work. You'd need, not only experienced, but a staff that is experienced and trust-worthy.

AND, always, PATCH, PATCH, PATCH.

If there's a Tor update, UPDATE IT! If you don't, you'd be vulnerable to exploits.

ALSO, Tor bridge relays <https://www.torproject.org/docs/bridges.html.en> so that your VPNP/ISP wouldn't know, if you're using Tor network.

And also, if you have an experienced russian friend, this is of an enormous priority.

Russian hackers are the most skillful ones, followed by asian hackers.

Finally a half decent addition, thanks.

**ballack\_perllo** - September 6, 2016, 5:50 am

Great job man!.....

**Confound** - September 7, 2016, 11:01 pm

Very solid tutorial. Thanks for the share, Lrrr.

**Armada** - September 9, 2016, 7:58 am

Great write up man, enjoyed the read.?

**Lrrr** - September 9, 2016, 9:30 am

(Sep 6, 2016 05:50 AM)ballack\_perllo Wrote: [\[CITE\]](#) Great job man!.....

(Sep 7, 2016 11:01 PM)Confound Wrote: [\[CITE\]](#) Very solid tutorial. Thanks for the share, Lrrr.

(Sep 9, 2016 07:58 AM)Armada Wrote: [\[CITE\]](#) Great write up man, enjoyed the read.?

Thanks Guys!

**Fantom4242** - October 6, 2016, 2:38 pm

(Sep 4, 2016 12:43 PM)Pharaoh1100 Wrote: [\[CITE\]](#) Securing the server sounds easy, but it requires a lot of work. First of all, you should be acknowledged about the exploits, to which protocols are vulnerable in the Tor and network sphere. Be sure to, either have you, or someone from your team, that follows the news regarding exploits and such, then patch them as soon as you get acknowledged.

Your site's vulnerabilities.

And then the easiest, but most work-requiring thing, have a virtual machine, inside a virtual

machine. Not a RDP, nor a VPS, but a VM.

VM (1) Whonix Gateway > VM (2) Tails Linux > VM (And here's where you should configure, modify, and host your server) (3) I'd go for Kali Linux.

Use a proxy, and SSH tunneling routed through Tor in the end of the virtual machine chain.

Have your own dedicated server, and run your own proxy on it, which you could use with the proxy as a great advantage, such as DDoS immunity. Not fully, but it's strong.

Hosting a darknet service requires a lot of work. You'd need, not only experienced, but a staff that is experienced and trust-worthy.

AND, always, PATCH, PATCH, PATCH.

If there's a Tor update, UPDATE IT! If you don't, you'd be vulnerable to exploits.

ALSO, Tor bridge relays <https://www.torproject.org/docs/bridges.html.en> so that your VPN/ISP wouldn't know, if you're using Tor network.

And also, if you have an experienced russian friend, this is of an enormous priority.

Russian hackers are the most skillful ones, followed by asian hackers.

This guy is clearly uneducated towards Linux Distributions, and their different functions, but he did mention some very good points.

To add to this, the Linux Distro, which anyone should be using, first of all, should be on a computer, which purpose would serve as a workstation, and the distribution should be focused on being server-host. Gentoo hardened is a pretty good suggestion.

Pretty much patch, patch, and patch, but a lot of things. Linux's kernel, your distribution, the website's vulnerabilities, etc, etc.

Anyone, who is planning to host a site, should know that he is obligated to be up-to-date with the news regarding his Linux Distro, and site.

I can help anyone out, if you need help on the security, PM me, I'd be more than glad to help for free.

Thank you for the great tutorial, OP, sorry for biasing off the main post so much.

**R^ptor** - October 6, 2016, 3:48 pm

Good and more secure this way.

**Guzzie** - October 6, 2016, 3:53 pm

Amazing tutorial ,had a great read. Gonna bookmark it for further. :)

**146918496** - October 6, 2016, 3:55 pm

Really cool tutorial,

Thanks a lot.

Posting to visit later

**Lrrr** - October 7, 2016, 12:14 pm

(Oct 6, 2016 02:38 PM)Fantom4242 Wrote: [CITE](#) This guy is clearly uneducated towards Linux Distributions, and their different functions, but he did mention some very good points.

To add to this, the Linux Distro, which anyone should be using, first of all, should be on a computer, which purpose would serve as a workstation, and the distribution should be focused on being server-host. Gentoo hardened is a pretty good suggestion.

Pretty much patch, patch, and patch, but a lot of things. Linux's kernel, your distribution, the website's vulnerabilities, etc, etc.

Anyone, who is planning to host a site, should know that he is obligated to be up-to-date with the news regarding his Linux Distro, and site.

I can help anyone out, if you need help on the security, PM me, I'd be more than glad to help for free.

Thank you for the great tutorial, OP, sorry for biasing off the main post so much.

Really great points in this post. Thank you!

(Oct 6, 2016 03:53 PM)Guzzie Wrote: [\[CITE\]](#) Amazing tutorial ,had a great read. Gonna bookmark it for further. :)Thanks man, if you need help let me know.

(Oct 6, 2016 03:55 PM)146918496 Wrote: [\[CITE\]](#) Really cool tutorial, Thanks a lot.

Posting to visit laterAwesome! Let me know if you need help mate!

Mr. Robot - October 7, 2016, 12:24 pm

Version 2, very simple windows.

Download Xampp

<http://sourceforge.net/projects/xampp/files/>

Install it.

Download Tor

<https://www.torproject.org/>

Create a folder somewhere called tor\_site, the 2 files in the below picture will make themselves in a minute.

Open up your TOR installed directory, Mine is

C:\Users\Mr. Robot\Desktop\TorT\Tor Browser\Browser\TorBrowser\Data\Tor\torrc

Edit torrc file in notepad

This is how mine looks now

Code # This file was generated by Tor; if you edit it, comments will not be preserved

# The old torrc file was renamed to torrc.orig.1 or similar, and Tor will ignore it

DataDirectory C:\Users\Mr. Robot\Desktop\TorT\Tor Browser\Browser\TorBrowser\Data\Tor

GeoIPFile C:\Users\Mr. Robot\Desktop\TorT\Tor Browser\Browser\TorBrowser\Data\Tor\geoip

GeoIPv6File C:\Users\Mr. Robot\Desktop\TorT\Tor Browser\Browser\TorBrowser\Data\Tor\geoip6

HiddenServiceStatistics 0

# Hidden Service

HiddenServiceDir C:\Users\Mr. Robot\Desktop\tor\_site

HiddenServicePort 80 127.0.0.1:80

So just add on the # Hidden service lines and change to your own.

Now open up Xampp and in C:\xampp\htdocs put your website files in there.

Now start Apache on Xampp

Go to your tor\_site folder and open "hostname" in notepad to find your current onion URL.

=====

If you want to secure it more, there are plenty of ways to do so. Other than that, to make a custom tor URL

Download <https://github.com/lachesis/scallion/raw/binaries/scallion-v2.0.zip>

Now in CMD, CD into your downloaded folder for scallion.

Type

scallion.exe facebook

Now let it run, it will take a while depending on your setup and how long you want your .onion. Change facebook to what you want.

When it's done, take the .onion URL and replace it in your hostname file in your tor\_site folder. Take the PGP key and paste that into private\_key

-----

Only typing this up because I can, not to take away from Lrrrs tut.

**Lrrr** - October 7, 2016, 12:56 pm

(Oct 7, 2016 12:24 PM)Mr. Robot Wrote: [\[CITE\]](#) -snip-  
You mind if I add this to the OP for windows users?

**Mr. Robot** - October 7, 2016, 1:00 pm

(Oct 7, 2016 12:56 PM)Lrrr Wrote: [\[CITE\]](#) You mind if I add this to the OP for windows users?  
If you want mate, I can add in some shit to make the directory more secure if you want.

**Cyber Warrior** - October 7, 2016, 1:01 pm

Nice tutorial, thank you for the informations.

**Lrrr** - October 7, 2016, 2:15 pm

(Oct 7, 2016 01:00 PM)Mr. Robot Wrote: [\[CITE\]](#) If you want mate, I can add in some shit to make the directory more secure if you want.  
Added a link to your post in the OP, thanks man!

**Mr. Robot** - October 7, 2016, 2:17 pm

(Oct 7, 2016 02:15 PM)Lrrr Wrote: [\[CITE\]](#) Added a link to your post in the OP, thanks man!  
Sounds good man, thanks.

**Fantom4242** - October 7, 2016, 2:22 pm

All the great minds in one thread. I loved Mr. Robot's contribution, noted it for future reference

**spamboss** - *April 18, 2018, 9:50 pm*

is this tutorial still useful in 2018 ?