

## **How to host a website in darkweb**

### **1. Installing & Configuring nginx**

### **2. Installing Tor**

### **3. Configuring the Tor server**

#### **Install nginx**

```
# apt update
# apt install nginx
# service nginx start
# service nginx status
```

***Find your IP address in inet your-IP-address. Note it down, using that now make a curl request.***

```
# ifconfig
# curl our-ip-address:port
```

***The console should print out the HTML code of the default nginx page.***

#### **Installing Tor**

```
# apt install apt-transport-https
[check our os version (eg: VERSION="(Xenial Xerus)"]]
```

***and add the following lines in***

```
# nano /etc/apt/sources.list
"
deb http://deb.torproject.org/torproject.org xenial main
deb-src http://deb.torproject.org/torproject.org xenial main "
```

***if you have bionic version***

```
"
deb https://deb.torproject.org/torproject.org bionic main
deb-src https://deb.torproject.org/torproject.org bionic main "
```

***This is to add the gpg key used to sign the Tor packages.***

```
# curl
https://deb.torproject.org/torproject.org/A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD
89.asc | gpg --import
#gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | apt-key add -
```

***" the above command will show "OK" in success "***

***install Tor and also a package which will help to keep the signing key current.***

```
# apt update
# apt install tor deb.torproject.org-keyring
# service nginx start
# service nginx status
```

**By default all Tor client services, relays, and hidden services are commented out and disabled. Let's active the hidden service by editing the torrc file**

```
# nano /etc/tor/torrc
```

***uncomment these lines;***

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

OR

```
#HiddenServiceDir /var/lib/tor/other_hidden_service/  
#HiddenServicePort 80 127.0.0.1:80
```

### Restart Tor

```
# service tor stop  
# service tor start  
# service tor status
```

**Couple of files should have generated by Tor. First is a hostname file. Open it up to get your .onion address.**

```
# cat /var/lib/tor/other_hidden_service/hostname  
The URL to your all-new dark website will be printed in the console. To test if it's working  
# curl -v --socks5-hostname localhost:9050 http://hostname
```

*The URL is actually your-public-RSA-key.onion. Tor has a different way of identifying websites, i.e. via their public RSA key*

**Edit the main Nginx configuration file to disable undesirable information sharing.**

```
# nano /etc/nginx/nginx.conf  
add this three lines under "http" block
```

```
{  
  
server_name_in_redirect off;  
    server_tokens off;  
    port_in_redirect off;  
}
```

**restart nginx**

```
# systemctl restart nginx
```

### Configuring the Tor server

**Make a directory to hold our files for the web server.**

```
# mkdir /var/www/dark_web  
# sudo nano /var/www/dark_web/index.html (to test its working)
```

**Set the permissions so that Nginx can access the files.**

```
# chown -R www-data:www-data /var/www/dark_web/  
# sudo chmod 755 /var/www/dark_web/  
# systemctl restart nginx
```

**Make a new site in the sites-available directory**

```
# sudo nano /etc/nginx/sites-available/dark_web
```

**Inside add the following replacing the root and server\_name values for your instance.**

```
Server { listen 127.0.0.1:80;  
        root /var/www/dark_web/  
        index index.html;  
        server_name 2rjp7e2cn4ppizgn.onion;  
  
}
```

**Add this site the the site\_enabled.**

```
# sudo ln -s /etc/nginx/sites-available/dark_web /etc/nginx/sites-enabled/
```

**Python3 is needed to run the site**

```
# sudo apt-get install python3
```

```
# python3 -m http.server --bind 127.0.0.1 8080 ("keep running in a window")
```

**install tor browser and call you hostname.onion Add this site the the site\_enabled.**