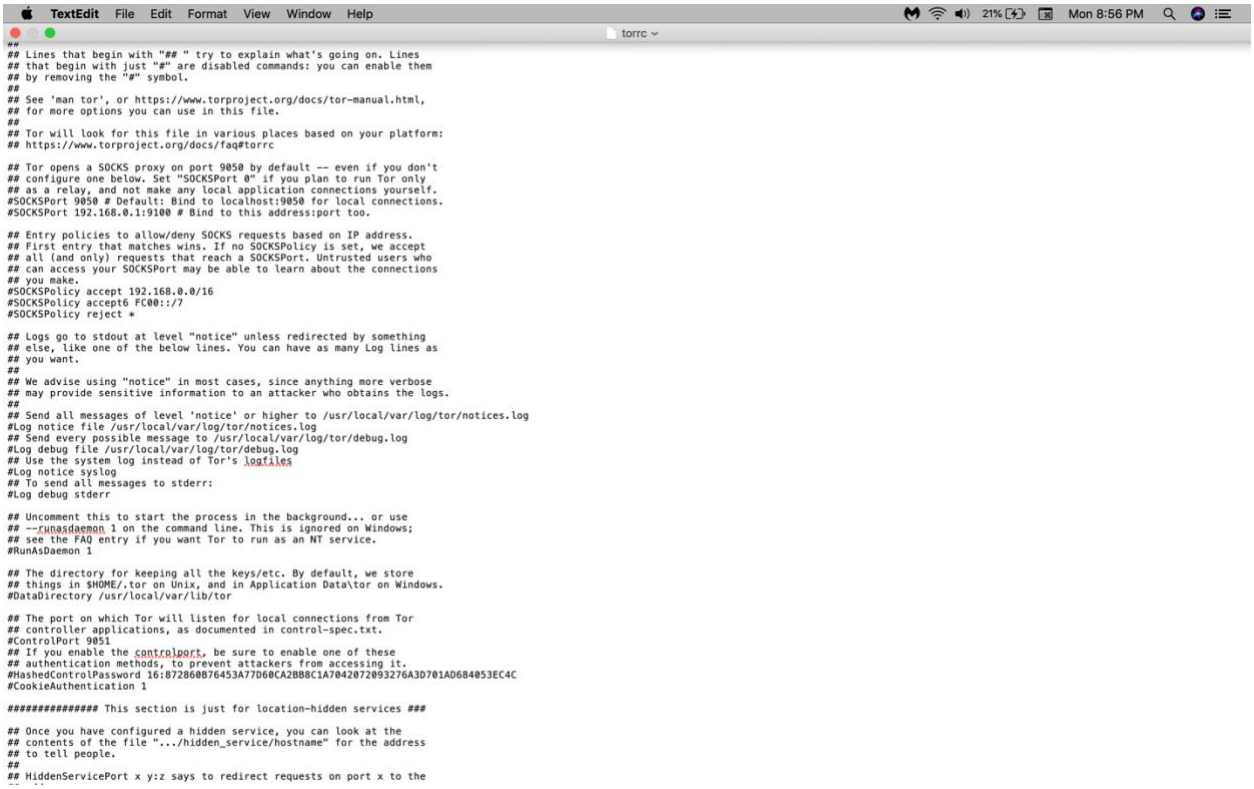
Name – Manav Ahlawat
Net Id – ma5169
ISP Assignment(Tor)

Steps used for this assignment-

1) Tor browser installation.
2) Installed and configured Nginx web server to locally host my onion website.
3) Configured the hidden service by editing the Torrc file.
4) Below I have pasted all the screenshots.

<u>Torrc file:</u>



```
##
## Lines that begin with "## " try to explain what's going on. Lines
## that begin with just "#" are disabled commands: you can enable them
## by removing the "#" symbol.
##
## See 'man tor', or https://www.torproject.org/docs/tor-manual.html,
## for more options you can use in this file.
##
## Tor will look for this file in various places based on your platform:
## https://www.torproject.org/docs/faq#torrc

## Tor opens a SOCKS proxy on port 9050 by default -- even if you don't
## configure one below. Set "SOCKSPort 0" if you plan to run Tor only
## as a relay, and not make any local application connections yourself.
#SOCKSPort 9050 # Default: Bind to localhost:9050 for local connections.
#SOCKSPort 192.168.0.1:9100 # Bind to this address:port too.

## Entry policies to allow/deny SOCKS requests based on IP address.
## First entry that matches wins. If no SOCKSPolicy is set, we accept
## all (and only) requests that reach a SOCKSPort. Untrusted users who
## can access your SOCKSPort may be able to learn about the connections
## you make.
#SOCKSPolicy accept 192.168.0.0/16
#SOCKSPolicy accept6 FC00::/7
#SOCKSPolicy reject *

## Logs go to stdout at level "notice" unless redirected by something
## else, like one of the below lines. You can have as many Log lines as
## you want.
##
## We advise using "notice" in most cases, since anything more verbose
## may provide sensitive information to an attacker who obtains the logs.
##
## Send all messages of level 'notice' or higher to /usr/local/var/log/tor/notices.log
#Log notice file /usr/local/var/log/tor/notices.log
## Send every possible message to /usr/local/var/log/tor/debug.log
#Log debug file /usr/local/var/log/tor/debug.log
## Use the system log instead of Tor's logfiles
#Log notice syslog
## To send all messages to stderr:
#Log debug stderr

## Uncomment this to start the process in the background... or use
## --runasdaemon 1 on the command line. This is ignored on Windows;
## see the FAQ entry if you want Tor to run as an NT service.
#RunAsDaemon 1

## The directory for keeping all the keys/etc. By default, we store
## things in $HOME/.tor on Unix, and in Application Data\tor on Windows.
#DataDirectory /usr/local/var/lib/tor

## The port on which Tor will listen for local connections from Tor
## controller applications, as documented in control-spec.txt.
#ControlPort 9051
## If you enable the controlport, be sure to enable one of these
## authentication methods, to prevent attackers from accessing it.
#HashedControlPassword 16:872860B76453A77D60CA2BB8C1A7042072093276A3D701AD684053EC4C
#CookieAuthentication 1

############## This section is just for location-hidden services ###

## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
```

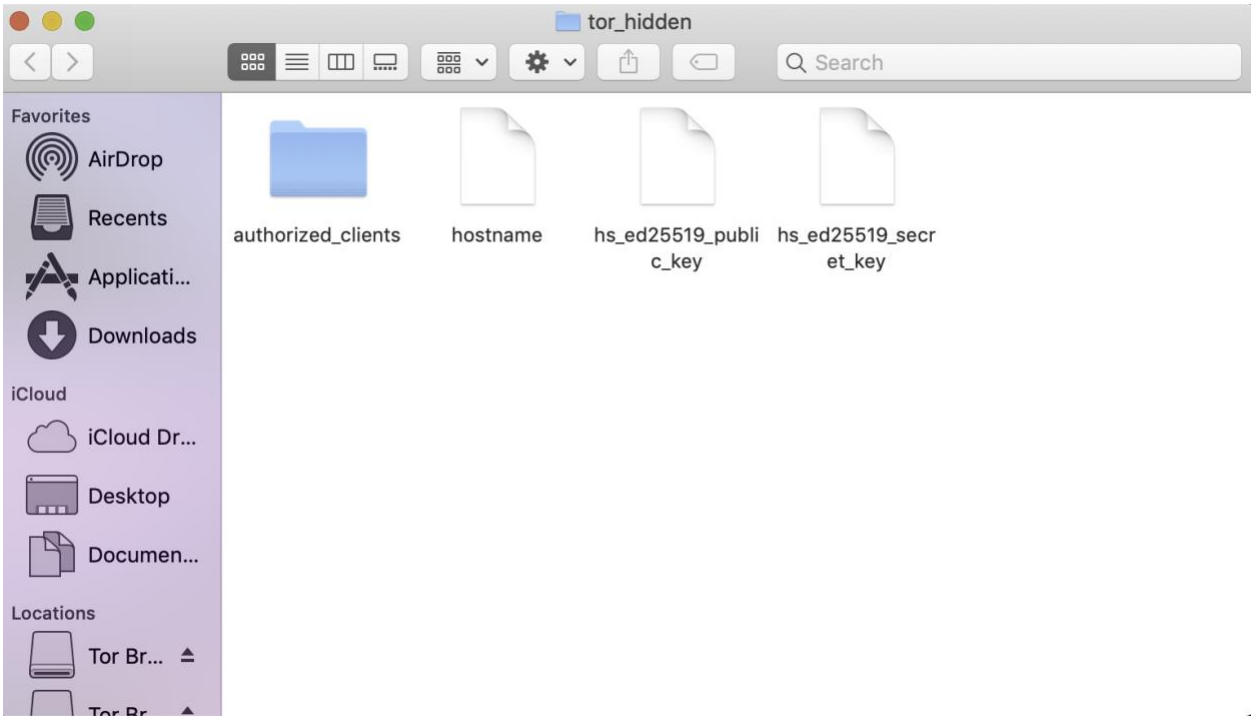
```
## The port on which Tor will listen for local connections from Tor
## controller applications, as documented in control-spec.txt.
#ControlPort 9051
## If you enable the controlport, be sure to enable one of these
## authentication methods, to prevent attackers from accessing it.
#HashedControlPassword 16:872860B76453A77D60CA2BB8C1A7042072093276A3D701AD684053EC4C
#CookieAuthentication 1

############### This section is just for location-hidden services ###

## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

HiddenServiceDir /Users/manavahlawat/Desktop/tor_hidden
HiddenServicePort 8080 127.0.0.1:8080

#HiddenServiceDir /usr/local/var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22
############### This section is just for relays ####################
#
## See https://www.torproject.org/docs/tor-doc-relay for details.

## Required: what port to advertise for incoming Tor connections.
#ORPort 9001
## If you want to listen on a port other than the one advertised in
## ORPort (e.g. to advertise 443 but bind to 9090), you can do it as
## follows.  You'll need to do ipchains or other port forwarding
## yourself to make this work.
#ORPort 443 NoListen
#ORPort 127.0.0.1:9090 NoAdvertise

## The IP address or full DNS name for incoming connections to your
## relay. Leave commented out and Tor will guess.
#Address noname.example.com

## If you have multiple network interfaces, you can specify one for
## outgoing traffic to use.
## OutboundBindAddressExit will be used for all exit traffic, while
## OutboundBindAddressOR will be used for all OR and Dir connections
## (DNS connections ignore OutboundBindAddress).
## If you do not wish to differentiate, use OutboundBindAddress to
## specify the same address for both in a single line.
#OutboundBindAddressExit 10.0.0.4
#OutboundBindAddressOR 10.0.0.5

## A handle for your relay, so people don't have to refer to it by key.
## Nicknames must be between 1 and 19 characters inclusive, and must
## contain only the characters [a-zA-Z0-9].
## If not set, "Unnamed" will be used.
#Nickname iididntedittheconfig

## Define these to limit how much relayed traffic you will allow. Your
## own traffic is still unthrottled. Note that RelayBandwidthRate must
## be at least 75 kilobytes per second.
## Note that units for these config options are bytes (per second), not
## bits (per second), and that prefixes are binary prefixes, i.e. 2^10,
## 2^20, etc.
#RelayBandwidthRate 100 KBytes  # Throttle traffic to 100KB/s (800Kbps)
#RelayBandwidthBurst 200 KBytes # But allow bursts up to 200KB (1600Kb)

## Use these to restrict the maximum traffic per day, week, or month.
## Note that this threshold applies separately to sent and received bytes,
## not to their sum: setting "40 GB" may allow up to 80 GB total before
## hibernating.
```


```
#RelayBandwidthBurst 200 KBytes # But allow bursts up to 200KB (1600Kb)

## Use these to restrict the maximum traffic per day, week, or month.
## Note that this threshold applies separately to sent and received bytes,
## not to their sum: setting "40 GB" may allow up to 80 GB total before
## hibernating.
```


```
##
## Set a maximum of 40 gigabytes each way per period.
#AccountingMax 40 GBytes
## Each period starts daily at midnight (AccountingMax is per day)
#AccountingStart day 00:00
## Each period starts on the 3rd of the month at 15:00 (AccountingMax
## is per month)
#AccountingStart month 3 15:00

## Administrative contact information for this relay or bridge. This line
## can be used to contact you if your relay or bridge is misconfigured or
## something else goes wrong. Note that we archive and publish all
## descriptors containing these lines and that Google indexes them, so
## spammers might also collect them. You may want to obscure the fact that
## it's an email address and/or generate a new address for this purpose.
##
## If you are running multiple relays, you MUST set this option.
##
#ContactInfo Random Person <nobody AT example dot com>
## You might also include your PGP or GPG fingerprint if you have one:
#ContactInfo 0xFFFFFFFF Random Person <nobody AT example dot com>

## Uncomment this to mirror directory information for others. Please do
## if you have enough bandwidth.
#DirPort 9030 # what port to advertise for directory connections
## If you want to listen on a port other than the one advertised in
## DirPort (e.g. to advertise 80 but bind to 9091), you can do it as
## follows.  below too. You'll need to do ipchains or other port
## forwarding yourself to make this work.
#DirPort 80 NoListen
#DirPort 127.0.0.1:9091 NoAdvertise
## Uncomment to return an arbitrary blob of html on your DirPort. Now you
## can explain what Tor is if anybody wonders why your IP address is
## contacting them. See contrib/tor-exit-notice.html in Tor's source
## distribution for a sample.
#DirPortFrontPage /usr/local/etc/tor/tor-exit-notice.html

## Uncomment this if you run more than one Tor relay, and add the identity
## key fingerprint of each Tor relay you control, even if they're on
## different networks. You declare it here so Tor clients can avoid
## using more than one of your relays in a single circuit. See
## https://www.torproject.org/docs/faq#MultipleRelays
## However, you should never include a bridge's fingerprint here, as it would
## break its concealability and potentially reveal its IP/TCP address.
##
## If you are running multiple relays, you MUST set this option.
##
## Note: do not use MyFamily on bridge relays.
#MyFamily $keyid,$keyid,...

## Uncomment this if you do *not* want your relay to allow any exit traffic.
## (Relays allow exit traffic by default.)
#ExitRelay 0

## Uncomment this if you want your relay to allow IPv6 exit traffic.
## (Relays only allow IPv4 exit traffic by default.)
#IPv6Exit 1

## A comma-separated list of exit policies. They're considered first
## to last, and the first match wins.
##
## If you want to allow the same ports on IPv4 and IPv6, write your rules
## using accept/reject *. If you want to allow different ports on IPv4 and
```

```
#MyFamily $keyid,$keyid,...

## Uncomment this if you do *not* want your relay to allow any exit traffic.
## (Relays allow exit traffic by default.)
#ExitRelay 0

## Uncomment this if you want your relay to allow IPv6 exit traffic.
## (Relays only allow IPv4 exit traffic by default.)
#IPv6Exit 1

## A comma-separated list of exit policies. They're considered first
## to last, and the first match wins.
##
## If you want to allow the same ports on IPv4 and IPv6, write your rules
## using accept/reject *. If you want to allow different ports on IPv4 and
## IPv6, write your IPv6 rules using accept6/reject6 *6, and your IPv4 rules
## using accept/reject *4.
##
## If you want to _replace_ the default exit policy, end this with either a
## reject *:* or an accept *:*. Otherwise, you're _augmenting_ (prepending to)
## the default exit policy. Leave commented to just use the default, which is
## described in the man page or at
## https://www.torproject.org/documentation.html
##
## Look at https://www.torproject.org/faq-abuse.html#TypicalAbuses
## for issues you might encounter if you use the default exit policy.
##
## If certain IPs and ports are blocked externally, e.g. by your firewall,
## you should update your exit policy to reflect this -- otherwise Tor
## users will be told that those destinations are down.
##
## For security, by default Tor rejects connections to private (local)
## networks, including to the configured primary public IPv4 and IPv6 addresses,
## and any public IPv4 and IPv6 addresses on any interface on the relay.
## See the man page entry for ExitPolicyRejectPrivate if you want to allow
## "exit enclaving".
##
#ExitPolicy accept *:6660-6667,reject *:* # allow irc ports on IPv4 and IPv6 but no more
#ExitPolicy accept *:119 # accept nntp ports on IPv4 and IPv6 as well as default exit policy
#ExitPolicy accept *4:119 # accept nntp ports on IPv4 only as well as default exit policy
#ExitPolicy accept6 *6:119 # accept nntp ports on IPv6 only as well as default exit policy
#ExitPolicy reject *:* # no exits allowed

## Bridge relays (or "bridges") are Tor relays that aren't listed in the
## main directory. Since there is no complete public list of them, even an
## ISP that filters connections to all the known Tor relays probably
## won't be able to block all the bridges. Also, websites won't treat you
## differently because they won't know you're running Tor. If you can
## be a real relay, please do; but if not, be a bridge!
##
## Warning: when running your Tor as a bridge, make sure than MyFamily is
## NOT configured.
#BridgeRelay 1
## By default, Tor will advertise your bridge to users through various
## mechanisms like https://bridges.torproject.org/. If you want to run
## a private bridge, for example because you'll give out your bridge
## address manually to your friends, uncomment this line:
#PublishServerDescriptor 0

## Configuration options can be imported from files or folders using the %include
## option with the value being a path. If the path is a file, the options from the
## file will be parsed as if they were written where the %include option is. If
## the path is a folder, all files on that folder will be parsed following lexical
## order. Files starting with a dot are ignored. Files on subfolders are ignored.
## The %include option can be used recursively.
#%include /etc/torrc.d/
#%include /etc/torrc.custom
```

The hidden folder that was created with hostname file:



The Hostname file:

hostname

```
tsfddhfyv6jsjhgtbgqdzibze6zrx5bnhcvcc22peez7uj3s7td46eyd.onion
```

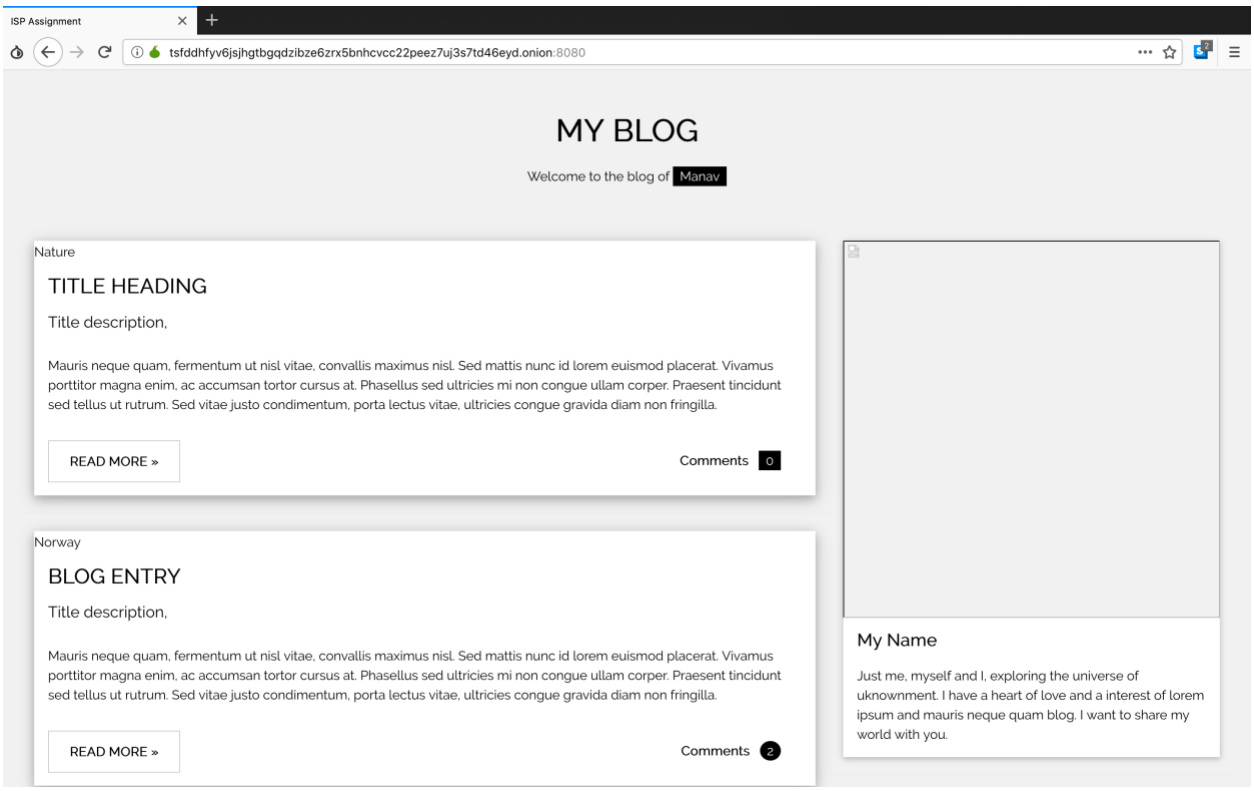
Nginx Server:

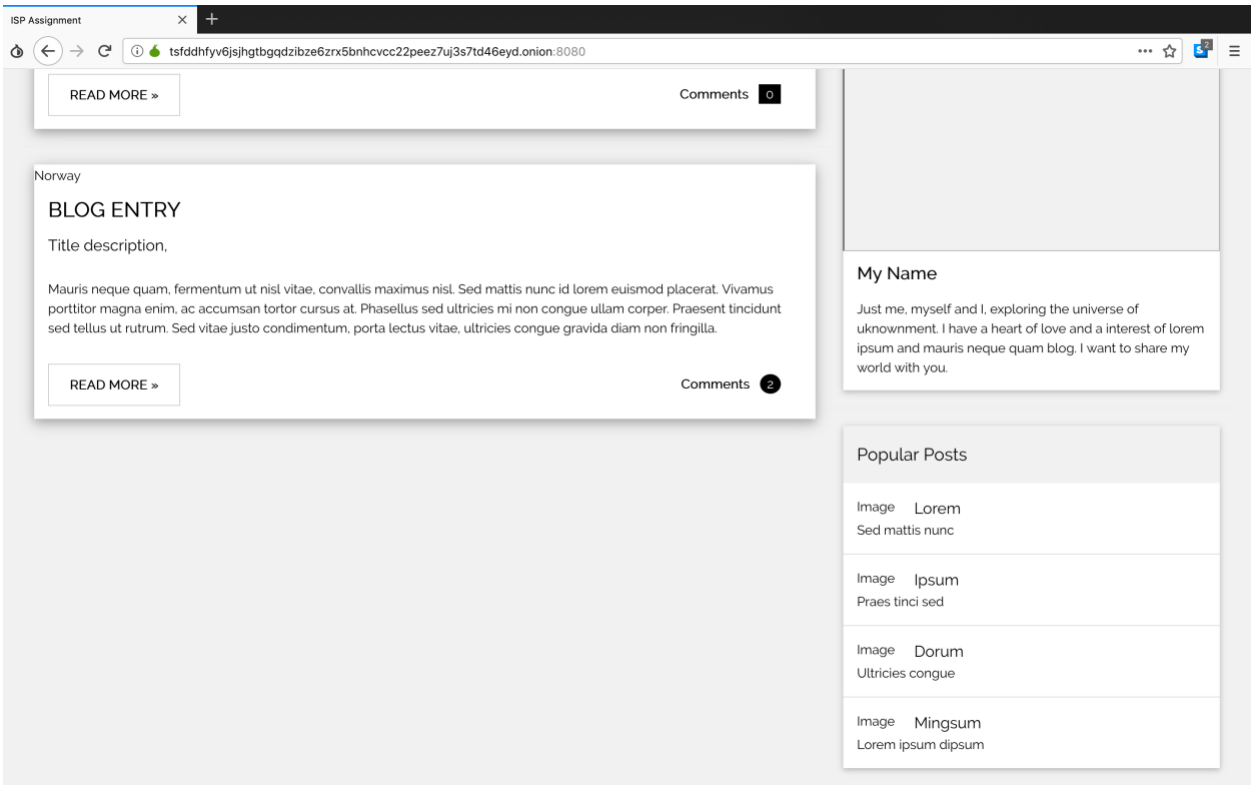
To install and configure Nginx server, I referred to this link https://medium.com/@ThomasTan/installing-nginx-in-mac-os-x-maverick-with-homebrew-d8867b7e8a5a

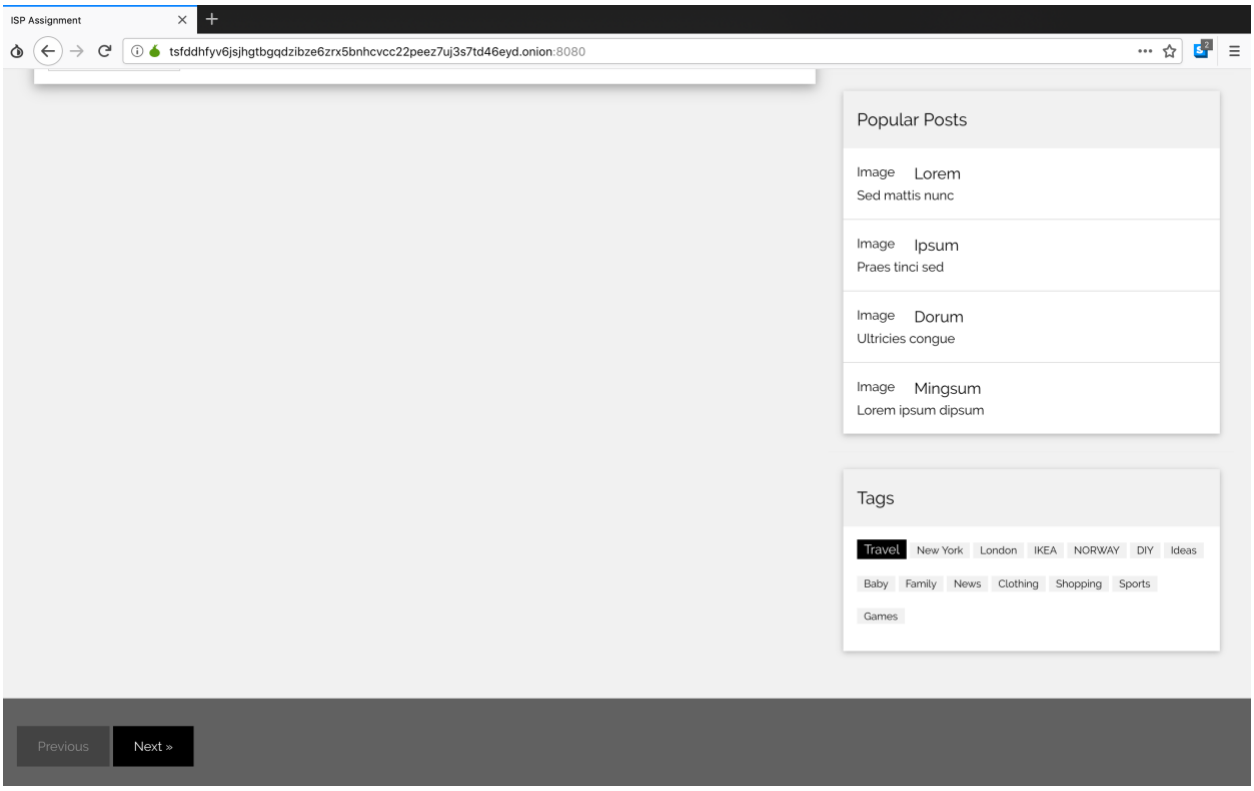
/usr/local — -bash

```
Manavs-MacBook-Pro:nginx manavahlawat$ brew services restart nginx
Stopping `nginx`... (might take a while)
==> Successfully stopped `nginx` (label: homebrew.mxcl.nginx)
==> Successfully started `nginx` (label: homebrew.mxcl.nginx)
```

Tor browser with my website with the hostname and port number specified and linked with Nginx server –




ISP Assignment
tsfddhfyv6jsjhgtbgqdzibze6zrx5bnhcvcc22peez7uj3s7td46eyd.onion:8080
READ MORE »
Comments 0
Norway
BLOG ENTRY
Title description,
Mauris neque quam, fermentum ut nisl vitae, convallis maximus nisl. Sed mattis nunc id lorem euismod placerat. Vivamus porttitor magna enim, ac accumsan tortor cursus at. Phasellus sed ultricies mi non congue ullam corper. Praesent tincidunt sed tellus ut rutrum. Sed vitae justo condimentum, porta lectus vitae, ultricies congue gravida diam non fringilla.
READ MORE »
Comments 2
My Name
Just me, myself and I, exploring the universe of uknownment. I have a heart of love and a interest of lorem ipsum and mauris neque quam blog. I want to share my world with you.
Popular Posts
Image Lorem
Sed mattis nunc
Image Ipsum
Praes tinci sed
Image Dorum
Ultricies congue
Image Mingsum
Lorem ipsum dipsum


ISP Assignment
tsfddhfyv6jsjhgtbgqdzibze6zrx5bnhcvcc22peez7uj3s7td46eyd.onion:8080
Popular Posts
Image Lorem
Sed mattis nunc
Image Ipsum
Praes tinci sed
Image Dorum
Ultricies congue
Image Mingsum
Lorem ipsum dipsum
Tags
Travel New York London IKEA NORWAY DIY Ideas
Baby Family News Clothing Shopping Sports
Games
Previous
Next »

Traditional web services Vs Tor hidden web service:

On the traditional web services, there is no anonymity that can be maintained. If you are hosting a website, anyone can easily track your IP address which would allow them to attack your website using various IP attacks to hack your server. Getting access to IP addresses can even reveal your geolocation which means the attacker can find you physically. Also, this information can be used to get your company secrets and the server might even dumped into trash by the attacker.

Whereas, Tor is an anonymous, secure network that allows access to websites with anonymity. The basic concept of Tor is that people can set up their own anonymous website by creating a hidden service Tor website. That website would run entirely within Tor and no one will know who created and runs the website. That website can only be accessed on Tor browser.

Tor browser is a patched version of Firefox and is maintained and distributed by the Tor Project, it includes a copy of Tor which launches itself when it gets started.
The major advantage of using Tor hidden services is that your website's IP address remains hidden. The IP address of your server cannot be seen and hence there is no way that you can be tracked. Without being able to track you, no one can hack you.