There are very few methods available which claim to be successful for DDoS or any type of network loss. Let’s see one of such method to perform DDoS attack. This attack is really powerful and requires the only skill that you should know how to operate commands on Kali Linux Operating System.

* First of all, If you want to check that any website has its TCP port 80 opened or not, you can go for nmap, and all the tutorial given for [nmap](https://www.nmapportscanner.info/" \t "_blank).
* This tool we are using is Torshammer. It is written in Python and can give damage to unprotected web servers in an instance that’s why it is a slow post tool.
* Main feature of this tool is it works on the 7th layer of HTTP(Hyper Text Transfer Protocol).

**Install Torshammer tool:**

Go to GitHub dotfighter/torshammer by this [link](https://github.com/dotfighter/torshammer) or, just open a terminal and write this command-

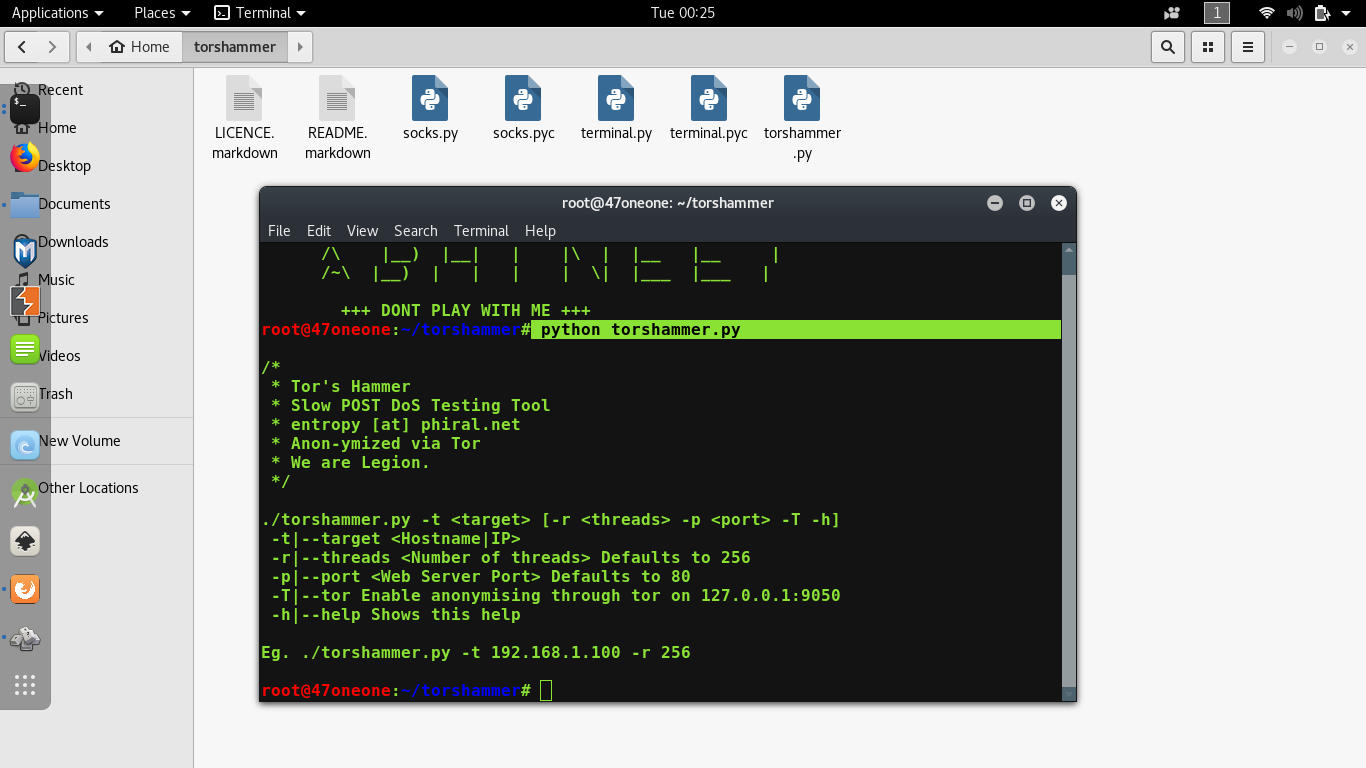
git clone https://github.com/dotfighter/torshammer.git

Now, Come to the directory wherever that script is cloned. You will find something like this:

You can see there are five Python scripts, two for the terminal, two for sockets and remaining one is main torshammer script. Now Right click on the blank space and select “Open In Terminal”, it will directly open a terminal with that right path. Otherwise, you can type “cd torshammer” in the newly opened terminal.

Write this command-

python torshammer.python

It will finally open the main interface for the tool.  


Let’s understand these first:

Any Python tool in Kali Linux should start with “python” suffix and follow by toolname(.)py also. Like that any PHP tool should start with “php” and follow by toolname(.)php.

**-t**is for the target, some domain or ip-address.  
**-p** is for port Defaults to 80.  
**-r** is for the threads, how many threads we want to run for this attack.  
**-T**stands for tor customized attacks.

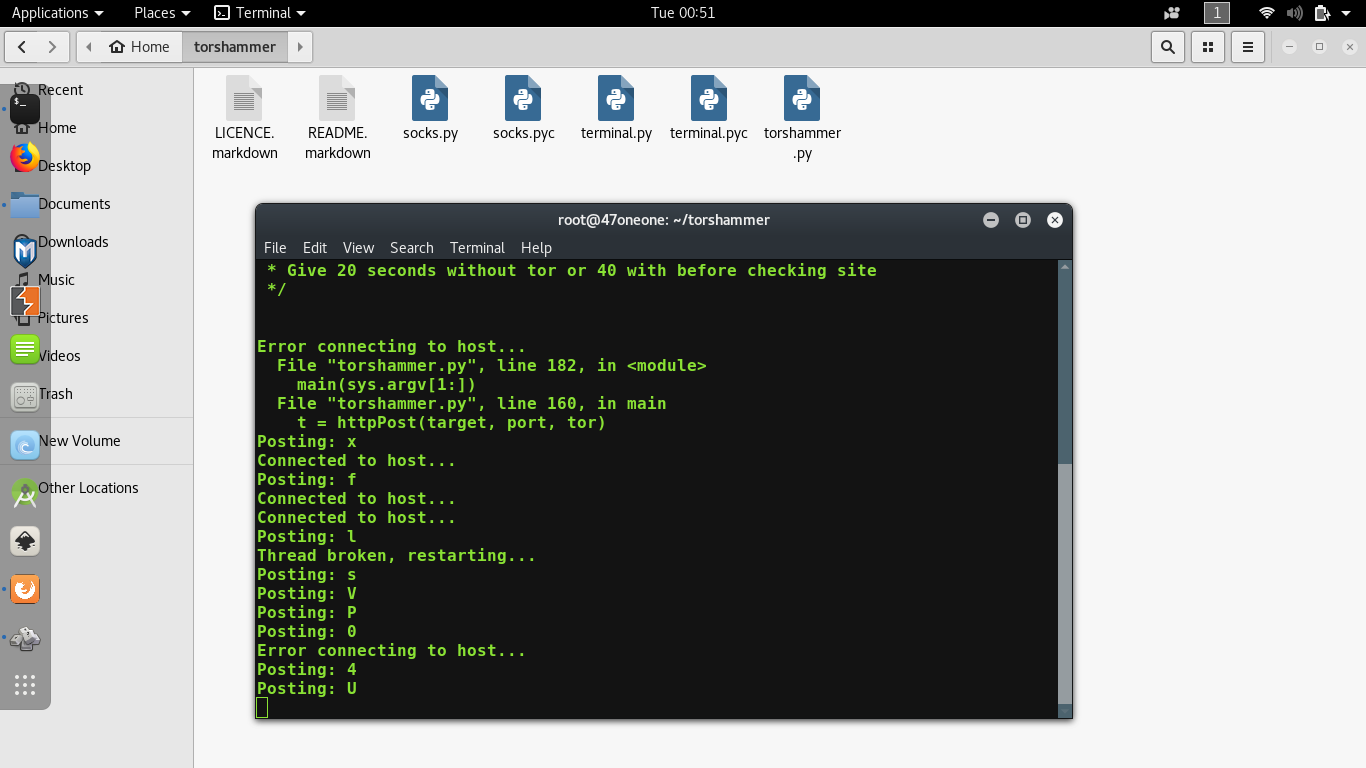
Let’s do the main thing:

python torshammer.py <i>any hostname/IP</i> -t -p 80 -r 5000

For example-

python torshammer.py -t xyz.com -p 80 -r 5000

As you hit enter after writing those commands, something will appear like this:



So, you have successfully run an attack. Please note that, if that website is opening normally then they have settled up their website on some Content Delivery Network(CDN) e.g. Akamai, Cloudflare which is designed to work against any kind of DoS or DDoS attacks. For checking that attack is successful or not, you can go to [isitdownrightnow](http://www.isitdownrightnow.com/" \t "_blank) to verify.