DoS Mitigation in Tor

•••

Miles Pütün and Irmak Demir

What is Tor aka “The Onion Router”?

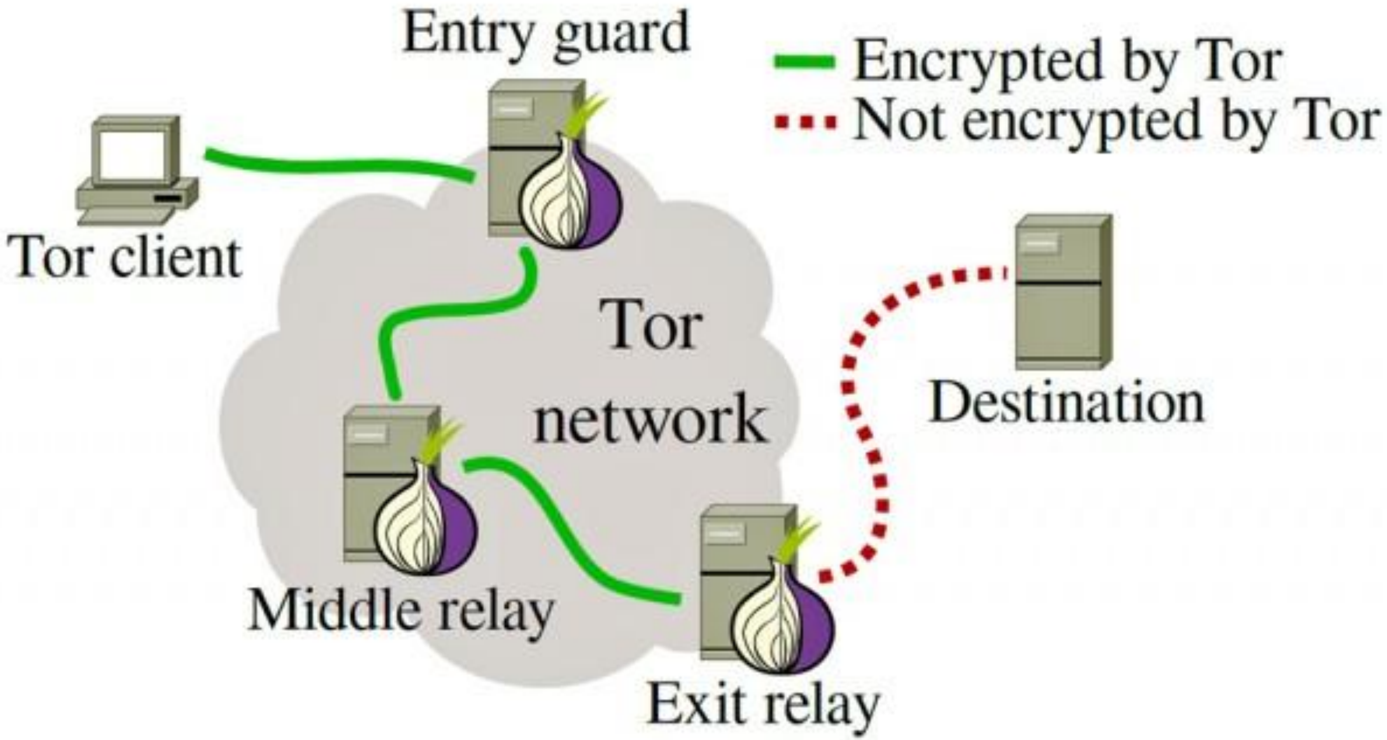
- Tor is an anonymity system that allows users to hide their identities while browsing the internet.

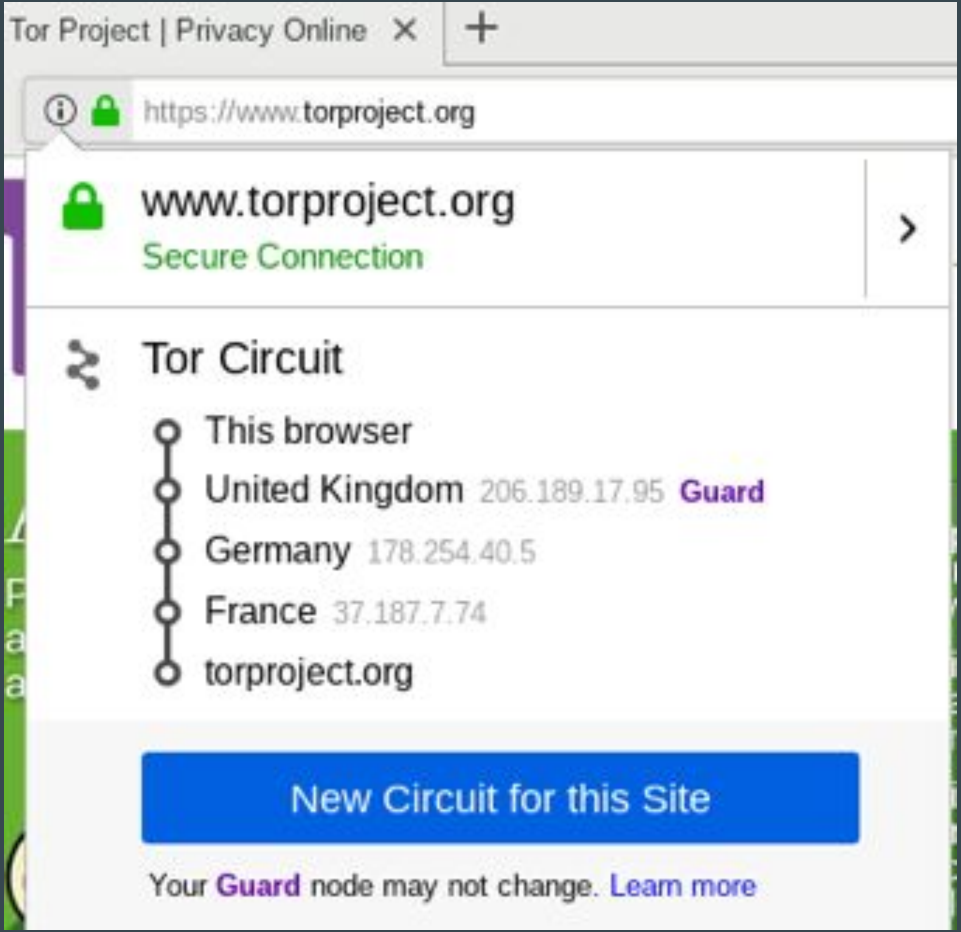
>>>>>>> *How does Tor achieve this?* <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

By separating the endpoints of the communication through a three-hop circuit. Such circuits are built using relays, which are voluntarily operated nodes that form a worldwide infrastructure.

>>>>>>> What does that mean? <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

It means that anyone can donate to become a relay and help Tor network become faster (and therefore more usable), more robust against attacks, more stable in case of outages, safer for its users (spying on more relays is harder than on a few)


Entry guard
Encrypted by Tor
Not encrypted by Tor
Tor client
Tor network
Destination
Middle relay
Exit relay



Tor Project | Privacy Online

https://www.torproject.org

www.torproject.org

Secure Connection

Tor Circuit

- This browser
- United Kingdom 206.189.17.95 Guard
- Germany 178.254.40.5
- France 37.187.7.74
- torproject.org

Your Guard node may not change. Learn more

Exhausting the relays

- While this public list of nodes creates transparency, it also opens the door for DoS attacks.

  An attacker can simply pick nodes from the list and stress them. To prevent DoS attacks, Tor implements a DoS mitigation that blocks overly frequent requests from clients.

Steps

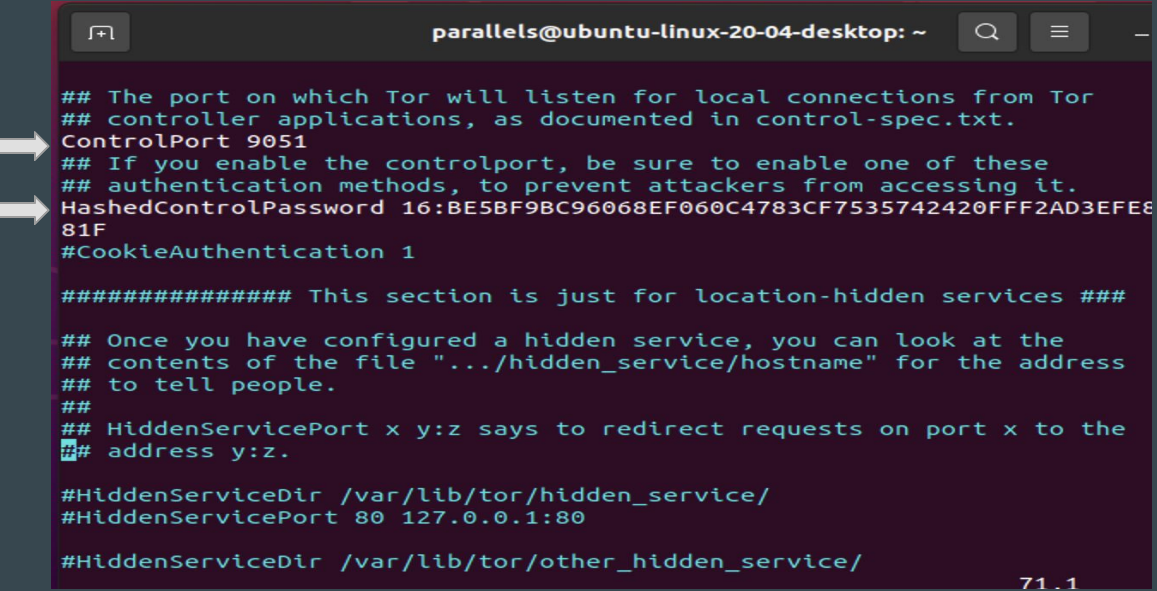
- Create a virtual machine, setup your network configurations (Host-only or Shared)
  - Under the OS of your choice, configure Tor Project's repository and install Tor.

- Modify /etc/tor/torrc file in your intention (Control port, Relay test, Sockslisten, ORport, HashedControlPassword etc.)

- Enable the system for tor (systemctl enable tor) and start tor (systemctl start tor)

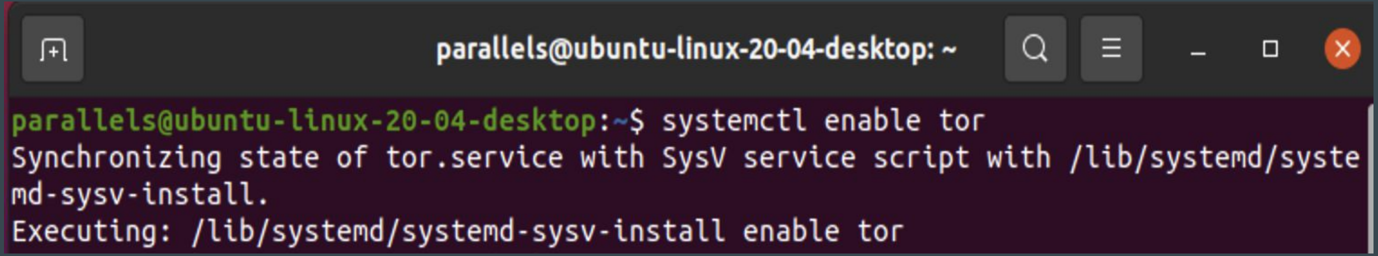
- Start Nyx, a command-line application for monitoring real time Tor status info.

Snapshot of /etc/tor/torrc file



```
## 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:BE5BF9BC96068EF060C4783CF7535742420FFF2AD3EFE8
81F
#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 /var/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80

#HiddenServiceDir /var/lib/tor/other_hidden_service/
                                                                71,1
```

Snapshot of starting tor (authentication required)



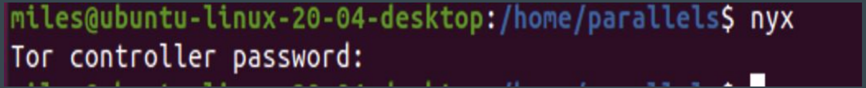
```
parallels@ubuntu-linux-20-04-desktop:~$ systemctl enable tor
Synchronizing state of tor.service with SysV service script with /lib/systemd/syste
md-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable tor
```

Steps continued

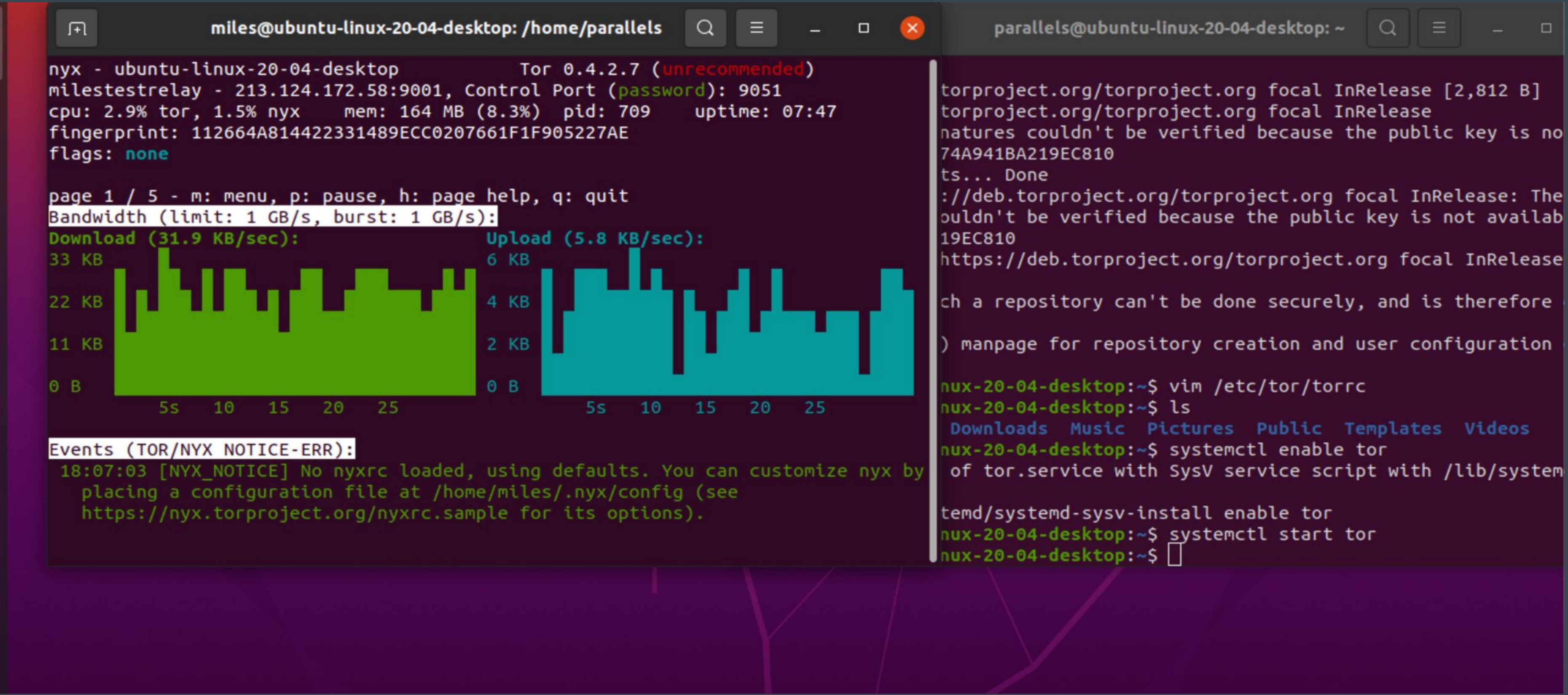
- Control Tor client from the control port

- Enable netcat and test the connection between client and local host (listen port allows certain incoming connections to bind etc.) The control port is opened on localhost.

- Monitor your relay and tcp connections, 3 way handshakes(SYN, SYN-ACK, ACK) that are established.



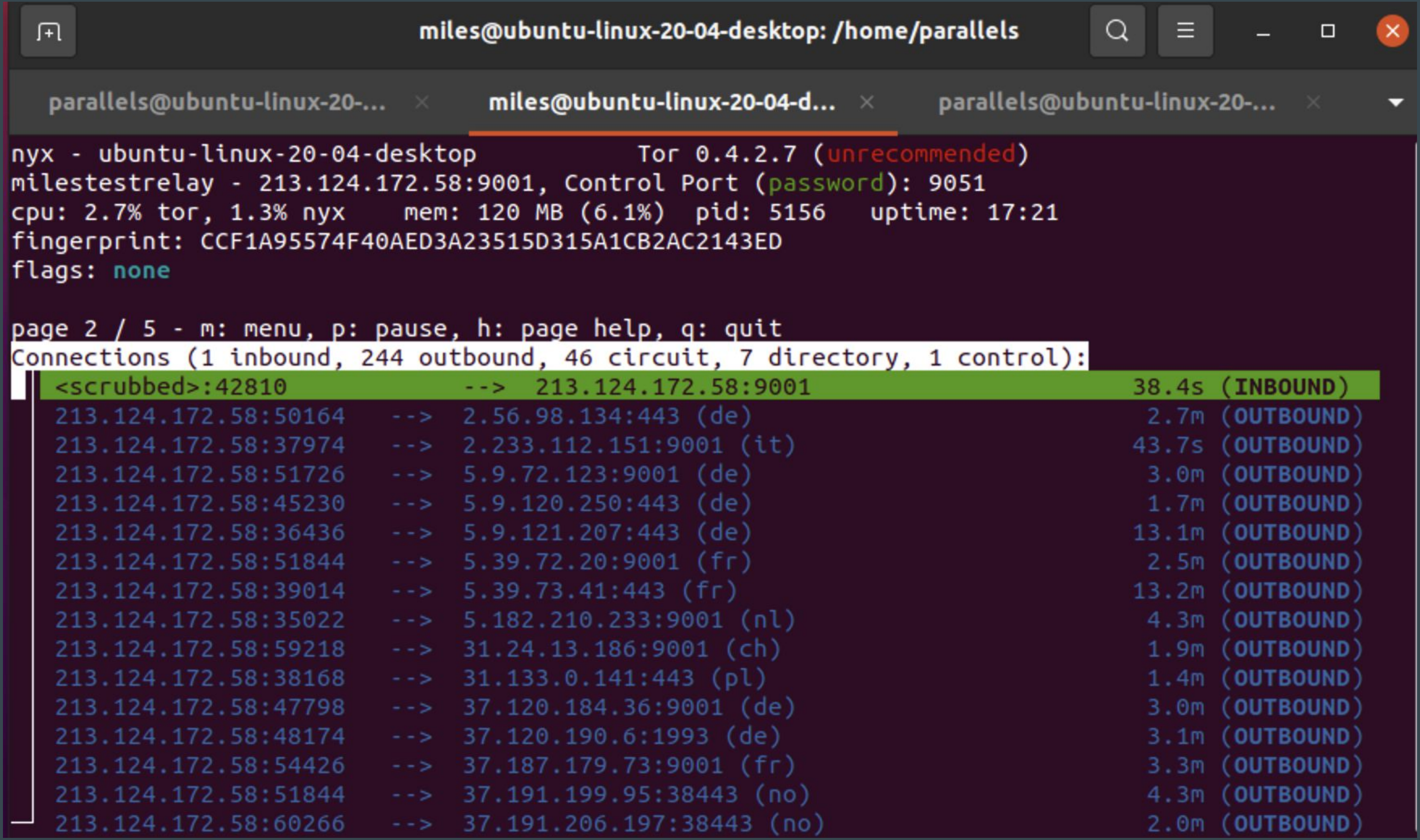
```
miles@ubuntu-linux-20-04-desktop:/home/parallels$ nyx
Tor controller password:
```



miles@ubuntu-linux-20-04-desktop: /home/parallels
parallels@ubuntu-linux-20-04-desktop: ~

```
nyx - ubuntu-linux-20-04-desktop           Tor 0.4.2.7 (unrecommended)
milestestrelay - 213.124.172.58:9001, Control Port (password): 9051
cpu: 2.9% tor, 1.5% nyx    mem: 164 MB (8.3%)  pid: 709    uptime: 07:47
fingerprint: 112664A814422331489ECC0207661F1F905227AE
flags: none

page 1 / 5 - m: menu, p: pause, h: page help, q: quit
Bandwidth (limit: 1 GB/s, burst: 1 GB/s):
Download (31.9 KB/sec):                   Upload (5.8 KB/sec):
33 KB                                     6 KB

22 KB                                     4 KB

11 KB                                     2 KB

0 B                                       0 B
          5s   10   15   20   25                    5s   10   15   20   25

Events (TOR/NYX NOTICE-ERR):
 18:07:03 [NYX_NOTICE] No nyxrc loaded, using defaults. You can customize nyx by
   placing a configuration file at /home/miles/.nyx/config (see
   https://nyx.torproject.org/nyxrc.sample for its options).
```

```
torproject.org/torproject.org focal InRelease [2,812 B]
torproject.org/torproject.org focal InRelease
natures couldn't be verified because the public key is no
74A941BA219EC810
ts... Done
://deb.torproject.org/torproject.org focal InRelease: The
ouldn't be verified because the public key is not availab
19EC810
https://deb.torproject.org/torproject.org focal InRelease

ch a repository can't be done securely, and is therefore

) manpage for repository creation and user configuration

nux-20-04-desktop:~$ vim /etc/tor/torrc
nux-20-04-desktop:~$ ls
 Downloads  Music  Pictures  Public  Templates  Videos
nux-20-04-desktop:~$ systemctl enable tor
 of tor.service with SysV service script with /lib/system

temd/systemd-sysv-install enable tor
nux-20-04-desktop:~$ systemctl start tor
nux-20-04-desktop:~$ 
```


miles@ubuntu-linux-20-04-desktop: /home/parallels
parallels@ubuntu-linux-20-...
miles@ubuntu-linux-20-04-d...
parallels@ubuntu-linux-20-...

```
nyx - ubuntu-linux-20-04-desktop           Tor 0.4.2.7 (unrecommended)
milestestrelay - 213.124.172.58:9001, Control Port (password): 9051
cpu: 2.7% tor, 1.3% nyx    mem: 120 MB (6.1%)  pid: 5156   uptime: 17:21
fingerprint: CCF1A95574F40AED3A23515D315A1CB2AC2143ED
flags: none

page 2 / 5 - m: menu, p: pause, h: page help, q: quit
Connections (1 inbound, 244 outbound, 46 circuit, 7 directory, 1 control):
   <scrubbed>:42810            -->  213.124.172.58:9001                  38.4s (INBOUND)
   213.124.172.58:50164   -->  2.56.98.134:443 (de)                     2.7m (OUTBOUND)
   213.124.172.58:37974   -->  2.233.112.151:9001 (it)                 43.7s (OUTBOUND)
   213.124.172.58:51726   -->  5.9.72.123:9001 (de)                     3.0m (OUTBOUND)
   213.124.172.58:45230   -->  5.9.120.250:443 (de)                     1.7m (OUTBOUND)
   213.124.172.58:36436   -->  5.9.121.207:443 (de)                    13.1m (OUTBOUND)
   213.124.172.58:51844   -->  5.39.72.20:9001 (fr)                     2.5m (OUTBOUND)
   213.124.172.58:39014   -->  5.39.73.41:443 (fr)                     13.2m (OUTBOUND)
   213.124.172.58:35022   -->  5.182.210.233:9001 (nl)                  4.3m (OUTBOUND)
   213.124.172.58:59218   -->  31.24.13.186:9001 (ch)                   1.9m (OUTBOUND)
   213.124.172.58:38168   -->  31.133.0.141:443 (pl)                    1.4m (OUTBOUND)
   213.124.172.58:47798   -->  37.120.184.36:9001 (de)                  3.0m (OUTBOUND)
   213.124.172.58:48174   -->  37.120.190.6:1993 (de)                   3.1m (OUTBOUND)
   213.124.172.58:54426   -->  37.187.179.73:9001 (fr)                  3.3m (OUTBOUND)
   213.124.172.58:51844   -->  37.191.199.95:38443 (no)                 4.3m (OUTBOUND)
   213.124.172.58:60266   -->  37.191.206.197:38443 (no)                2.0m (OUTBOUND)
```

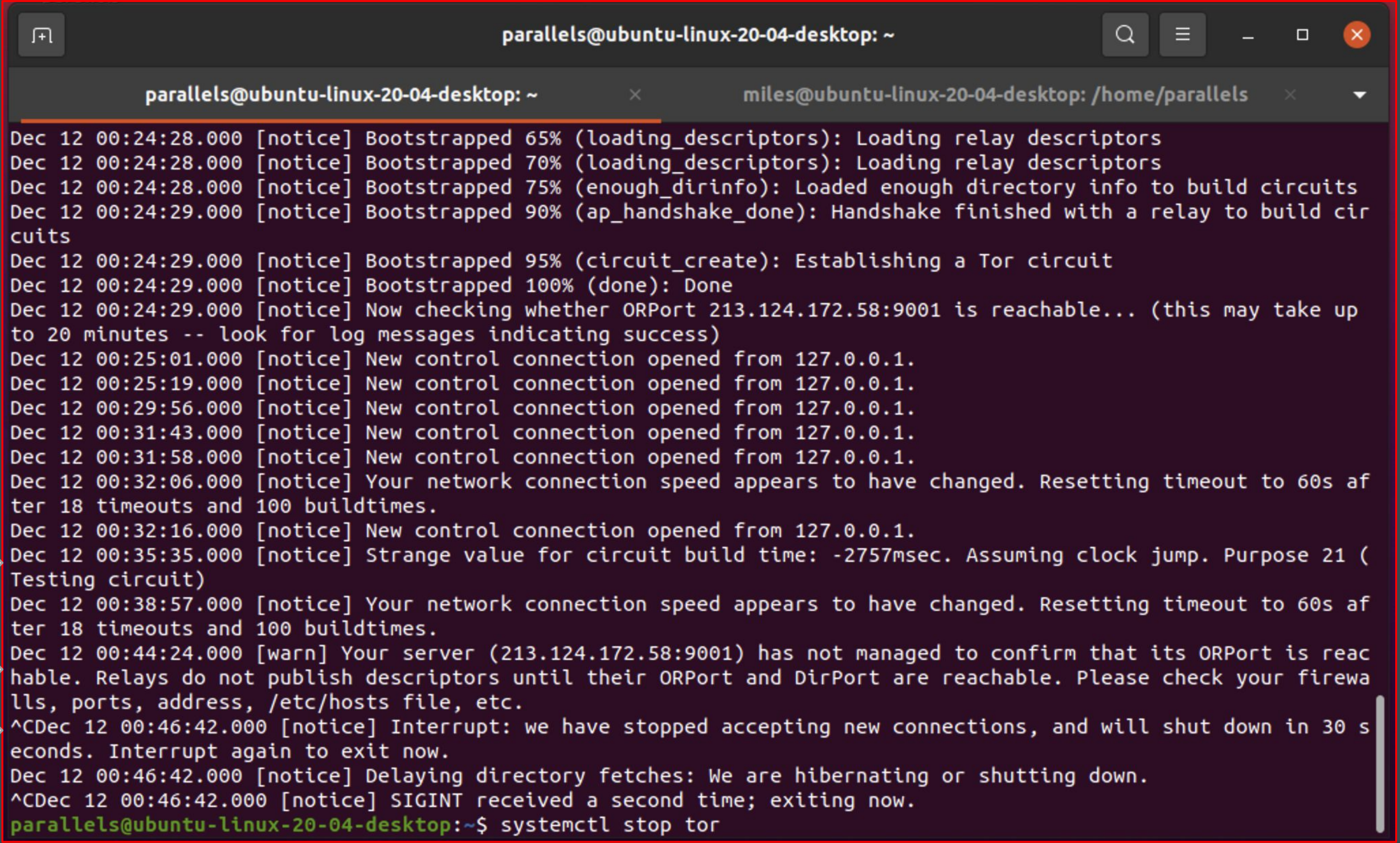
Attack Phase

- The type of attack we would like to accomplish is called Tor’s Hammer, a type of Denial of Service attack that the connection purpose is the ability to exhaust the relay ip and port.

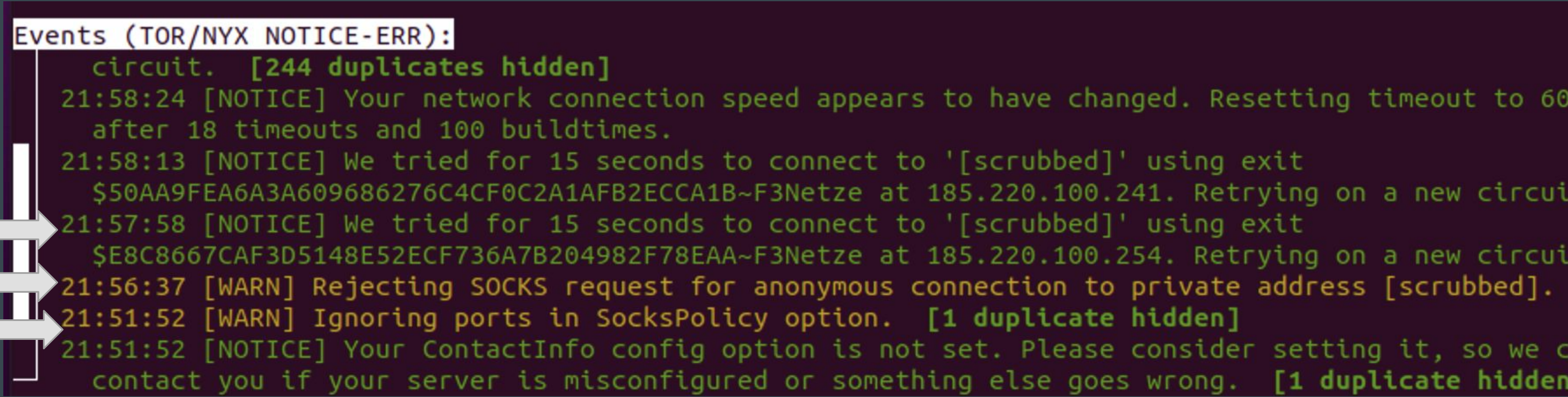
- We have used a python script based on slow post tool. As localhost, we have the IP/Server/Port with necessary permissions. (see /etc/tor/torrc)

- Then we have attacked our own relay.

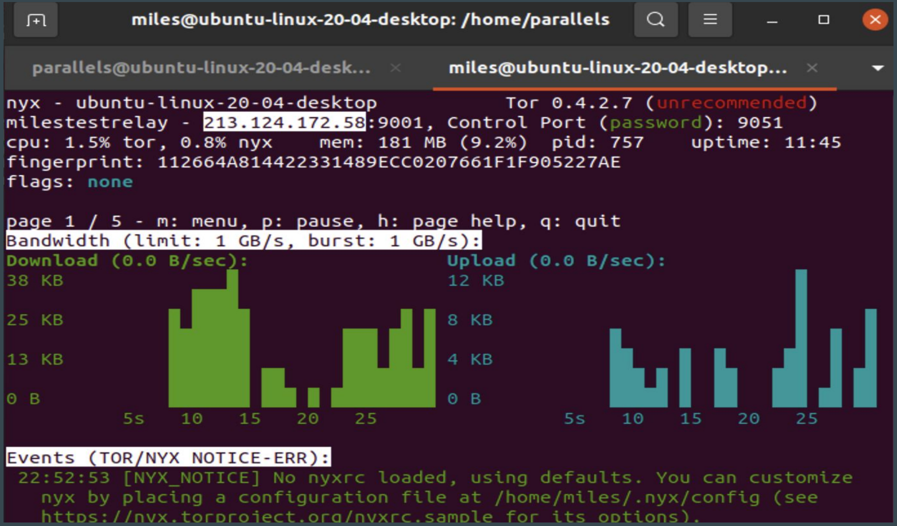
What did we see?


parallels@ubuntu-linux-20-04-desktop: ~
parallels@ubuntu-linux-20-04-desktop: ~
miles@ubuntu-linux-20-04-desktop: /home/parallels

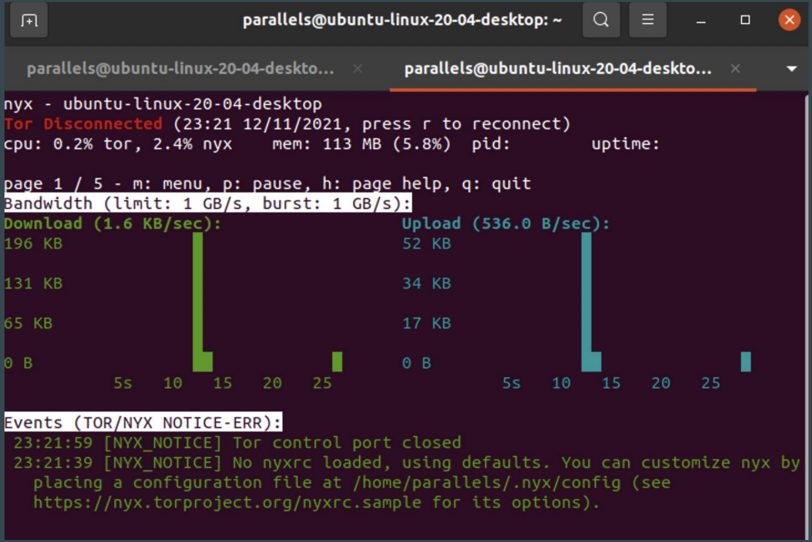
```
Dec 12 00:24:28.000 [notice] Bootstrapped 65% (loading_descriptors): Loading relay descriptors
Dec 12 00:24:28.000 [notice] Bootstrapped 70% (loading_descriptors): Loading relay descriptors
Dec 12 00:24:28.000 [notice] Bootstrapped 75% (enough_dirinfo): Loaded enough directory info to build circuits
Dec 12 00:24:29.000 [notice] Bootstrapped 90% (ap_handshake_done): Handshake finished with a relay to build cir
cuits
Dec 12 00:24:29.000 [notice] Bootstrapped 95% (circuit_create): Establishing a Tor circuit
Dec 12 00:24:29.000 [notice] Bootstrapped 100% (done): Done
Dec 12 00:24:29.000 [notice] Now checking whether ORPort 213.124.172.58:9001 is reachable... (this may take up
to 20 minutes -- look for log messages indicating success)
Dec 12 00:25:01.000 [notice] New control connection opened from 127.0.0.1.
Dec 12 00:25:19.000 [notice] New control connection opened from 127.0.0.1.
Dec 12 00:29:56.000 [notice] New control connection opened from 127.0.0.1.
Dec 12 00:31:43.000 [notice] New control connection opened from 127.0.0.1.
Dec 12 00:31:58.000 [notice] New control connection opened from 127.0.0.1.
Dec 12 00:32:06.000 [notice] Your network connection speed appears to have changed. Resetting timeout to 60s af
ter 18 timeouts and 100 buildtimes.
Dec 12 00:32:16.000 [notice] New control connection opened from 127.0.0.1.
Dec 12 00:35:35.000 [notice] Strange value for circuit build time: -2757msec. Assuming clock jump. Purpose 21 (
Testing circuit)
Dec 12 00:38:57.000 [notice] Your network connection speed appears to have changed. Resetting timeout to 60s af
ter 18 timeouts and 100 buildtimes.
Dec 12 00:44:24.000 [warn] Your server (213.124.172.58:9001) has not managed to confirm that its ORPort is reac
hable. Relays do not publish descriptors until their ORPort and DirPort are reachable. Please check your firewa
lls, ports, address, /etc/hosts file, etc.
^CDec 12 00:46:42.000 [notice] Interrupt: we have stopped accepting new connections, and will shut down in 30 s
econds. Interrupt again to exit now.
Dec 12 00:46:42.000 [notice] Delaying directory fetches: We are hibernating or shutting down.
^CDec 12 00:46:42.000 [notice] SIGINT received a second time; exiting now.
parallels@ubuntu-linux-20-04-desktop:~$ systemctl stop tor
```



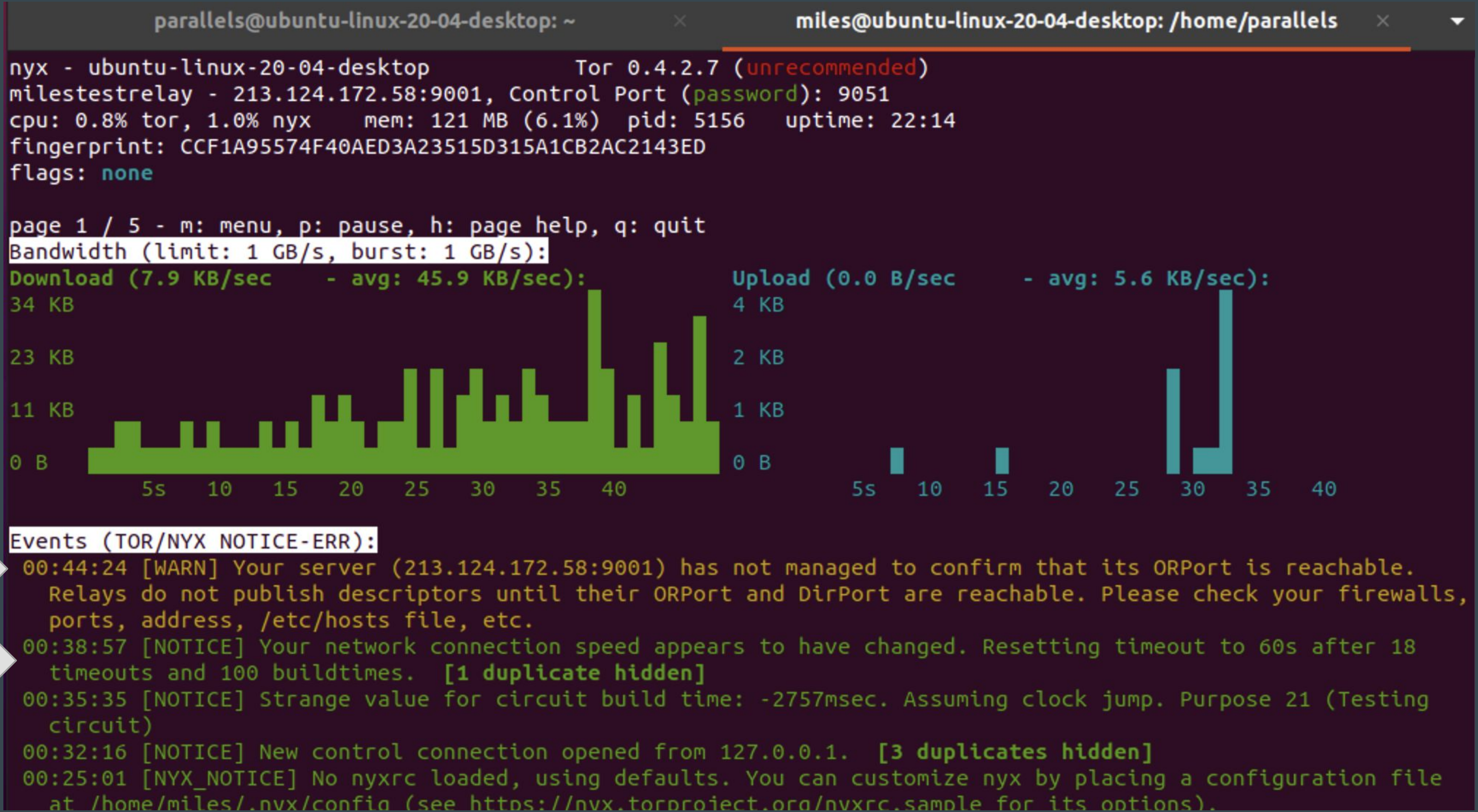
```
Events (TOR/NYX NOTICE-ERR):
   circuit.  [244 duplicates hidden]
 21:58:24 [NOTICE] Your network connection speed appears to have changed. Resetting timeout to 60
   after 18 timeouts and 100 buildtimes.
 21:58:13 [NOTICE] We tried for 15 seconds to connect to '[scrubbed]' using exit
   $50AA9FEA6A3A609686276C4CF0C2A1AFB2ECCA1B~F3Netze at 185.220.100.241. Retrying on a new circui
 21:57:58 [NOTICE] We tried for 15 seconds to connect to '[scrubbed]' using exit
   $E8C8667CAF3D5148E52ECF736A7B204982F78EAA~F3Netze at 185.220.100.254. Retrying on a new circui
 21:56:37 [WARN] Rejecting SOCKS request for anonymous connection to private address [scrubbed].
 21:51:52 [WARN] Ignoring ports in SocksPolicy option.  [1 duplicate hidden]
 21:51:52 [NOTICE] Your ContactInfo config option is not set. Please consider setting it, so we c
   contact you if your server is misconfigured or something else goes wrong.  [1 duplicate hidden
```


miles@ubuntu-linux-20-04-desktop: /home/parallels
parallels@ubuntu-linux-20-04-desk...
miles@ubuntu-linux-20-04-desktop...

```
nyx - ubuntu-linux-20-04-desktop          Tor 0.4.2.7 (unrecommended)
milestestrelay - 213.124.172.58:9001, Control Port (password): 9051
cpu: 1.5% tor, 0.8% nyx    mem: 181 MB (9.2%)  pid: 757    uptime: 11:45
fingerprint: 112664A814422331489ECC0207661F1F905227AE
flags: none

page 1 / 5 - m: menu, p: pause, h: page help, q: quit
Bandwidth (limit: 1 GB/s, burst: 1 GB/s):
Download (0.0 B/sec):                        Upload (0.0 B/sec):
38 KB                                        12 KB

25 KB                                        8 KB

13 KB                                        4 KB

0 B                                          0 B
            5s    10    15    20    25                   5s    10    15    20    25

Events (TOR/NYX NOTICE-ERR):
 22:52:53 [NYX_NOTICE] No nyxrc loaded, using defaults. You can customize
   nyx by placing a configuration file at /home/miles/.nyx/config (see
   https://nyx.torproject.org/nyxrc.sample for its options).
```


parallels@ubuntu-linux-20-04-desktop: ~
parallels@ubuntu-linux-20-04-deskto...
parallels@ubuntu-linux-20-04-deskto...

```
nyx - ubuntu-linux-20-04-desktop
Tor Disconnected (23:21 12/11/2021, press r to reconnect)
cpu: 0.2% tor, 2.4% nyx    mem: 113 MB (5.8%)  pid:        uptime:

page 1 / 5 - m: menu, p: pause, h: page help, q: quit
Bandwidth (limit: 1 GB/s, burst: 1 GB/s):
Download (1.6 KB/sec):                   Upload (536.0 B/sec):
196 KB                                   52 KB

131 KB                                   34 KB

65 KB                                    17 KB

0 B                                      0 B
          5s   10   15   20   25                   5s   10   15   20   25

Events (TOR/NYX NOTICE-ERR):
 23:21:59 [NYX_NOTICE] Tor control port closed
 23:21:39 [NYX_NOTICE] No nyxrc loaded, using defaults. You can customize nyx by
   placing a configuration file at /home/parallels/.nyx/config (see
   https://nyx.torproject.org/nyxrc.sample for its options).
```


parallels@ubuntu-linux-20-04-desktop: ~
miles@ubuntu-linux-20-04-desktop: /home/parallels

```
nyx - ubuntu-linux-20-04-desktop          Tor 0.4.2.7 (unrecommended)
milestestrelay - 213.124.172.58:9001, Control Port (password): 9051
cpu: 0.8% tor, 1.0% nyx    mem: 121 MB (6.1%)  pid: 5156   uptime: 22:14
fingerprint: CCF1A95574F40AED3A23515D315A1CB2AC2143ED
flags: none

page 1 / 5 - m: menu, p: pause, h: page help, q: quit
Bandwidth (limit: 1 GB/s, burst: 1 GB/s):
Download (7.9 KB/sec    - avg: 45.9 KB/sec):           Upload (0.0 B/sec     - avg: 5.6 KB/sec):
34 KB                                                  4 KB

23 KB                                                  2 KB

11 KB                                                  1 KB

0 B                                                    0 B

         5s   10   15   20   25   30   35   40                  5s   10   15   20   25   30   35   40

Events (TOR/NYX NOTICE-ERR):
 00:44:24 [WARN] Your server (213.124.172.58:9001) has not managed to confirm that its ORPort is reachable.
   Relays do not publish descriptors until their ORPort and DirPort are reachable. Please check your firewalls,
   ports, address, /etc/hosts file, etc.
 00:38:57 [NOTICE] Your network connection speed appears to have changed. Resetting timeout to 60s after 18
   timeouts and 100 buildtimes.  [1 duplicate hidden]
 00:35:35 [NOTICE] Strange value for circuit build time: -2757msec. Assuming clock jump. Purpose 21 (Testing
   circuit)
 00:32:16 [NOTICE] New control connection opened from 127.0.0.1.  [3 duplicates hidden]
 00:25:01 [NYX_NOTICE] No nyxrc loaded, using defaults. You can customize nyx by placing a configuration file
   at /home/miles/.nyx/config (see https://nyx.torproject.org/nyxrc.sample for its options).
```

Findings

- Realized that the protection in the relay is determined by the amount of requests the client send. Although the relay remains in place, the IP that is reaching the node will be blocked after too many requests.

- Acknowledged that due to the nature of the Tor network and the anonymity of it make the nodes susceptible to distributed DoS attacks. Although the reluctant changes in our relay itself lasted for a limited amount of time until the server dropped the connection, we effectively used our relay's resources with our meaningless requests and made it temporarily available.

- Concluded that having more relays build and help Tor network become faster (and therefore more usable), more robust against attacks, more stable in case of outages, safer for its users (spying on more relays is harder than on a few)

- In a real world-setting, although there is no specific filter which we could analyze, the possible indicators of a Dos Attack would be following the TCP streams; numerous TCP handshakes followed by TCP segmented packets only, absence of meaningful data packets, absence of FIN packets.