M04 Lab Homework report

# Reservation of Resources

A screenshot of a computer

Description automatically generated

Nodes reserved, shown in list view.

# SSH-ing to nodes

A computer screen with white text

Description automatically generated

Sshd into the server sucessfully

# Accessing the apache server before the DOS attack

A screenshot of a computer program

Description automatically generated

# Attack initiation on the client

A computer screen with white text

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

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.

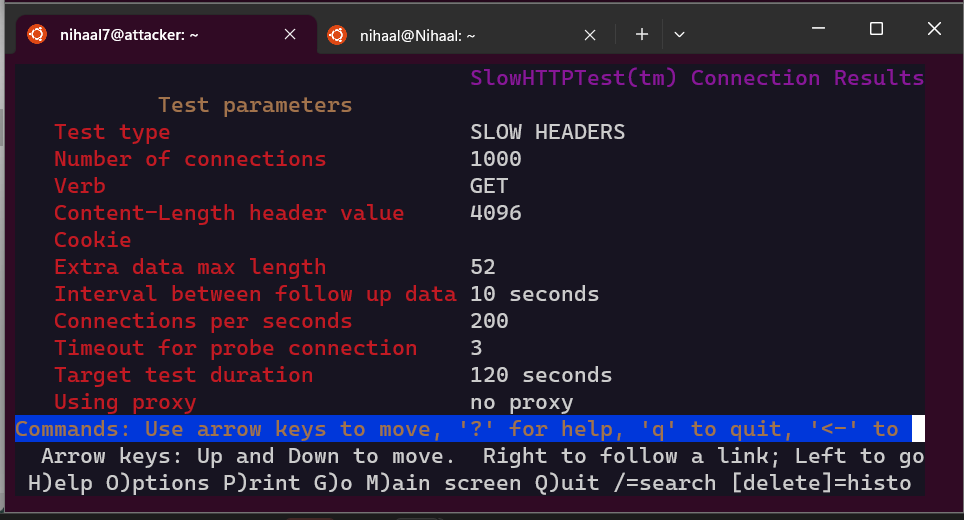
A screenshot of a computer

Description automatically generated

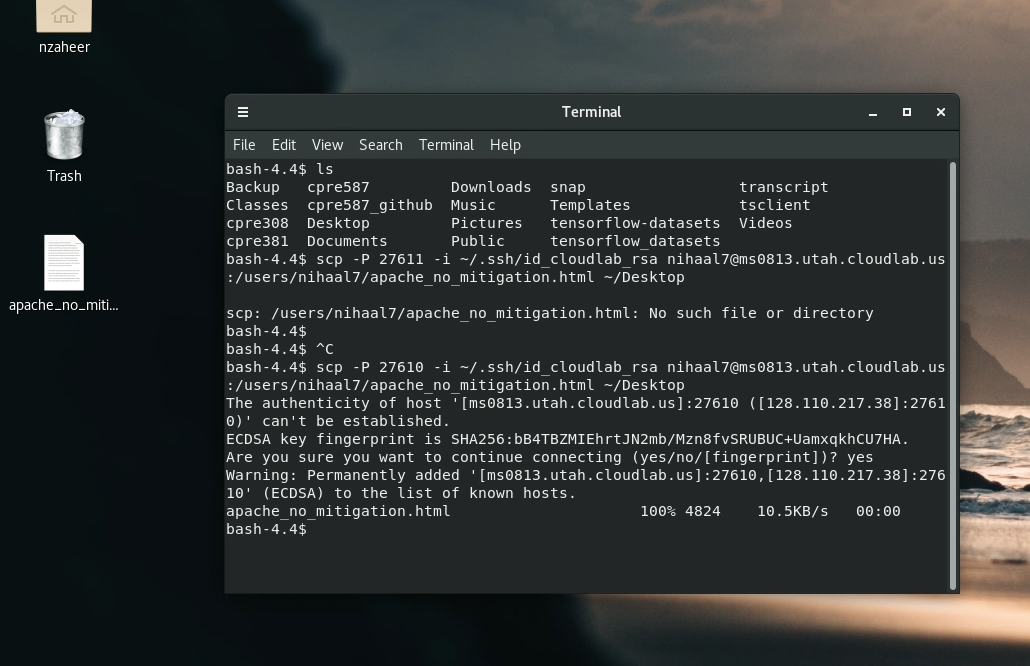
# Command to limit rate of traffic and DOS result after this modification



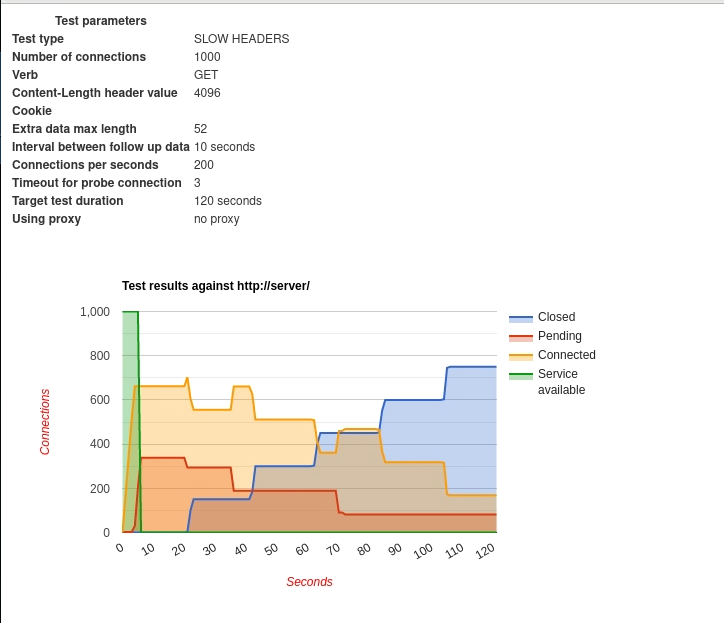
Above shows that apache\_no\_mitigation.html was copied from the client to my local PC.



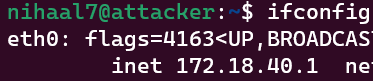
Since I am using Windows Subsystem for Linux, I was not able to access a browser to open the html file. So I used lynx instead to open it, and the above is the result.



I used the VDI to open it instead



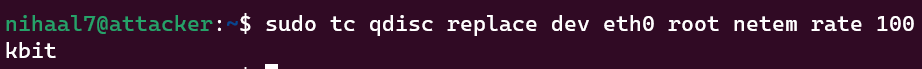
"apache\_no\_mitigation.html



A black background with white text

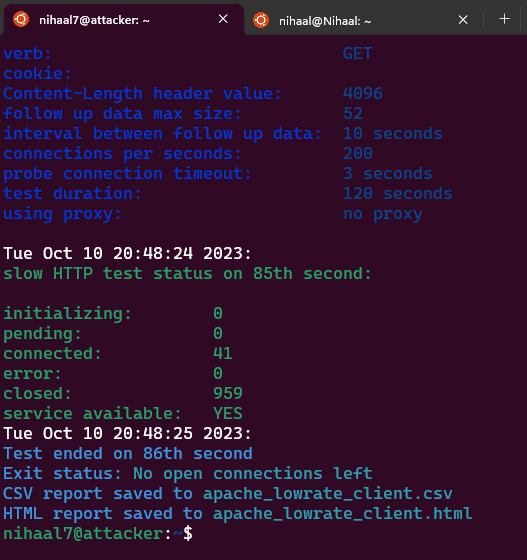
Description automatically generated

Ifconfig





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.



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

A graph with different colored lines

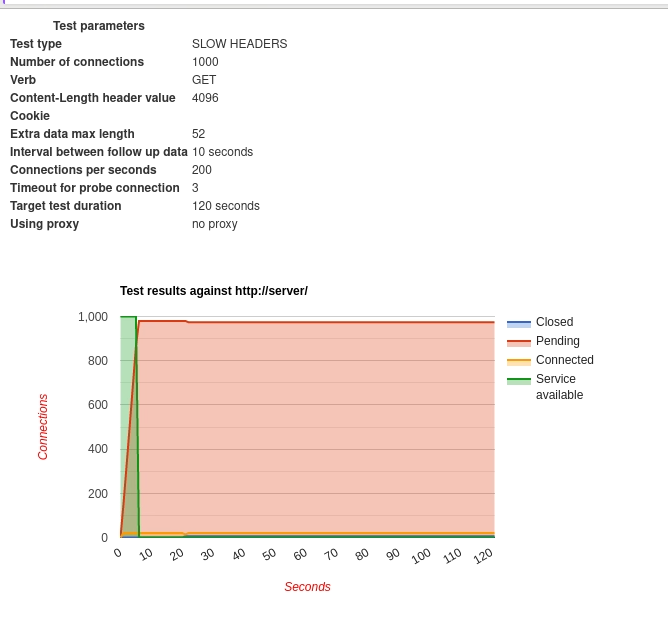
Description automatically generated

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:



After running these commands,

A computer code with text

Description automatically generated with medium confidence

A screenshot of a computer screen

Description automatically generated

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

Using

****

nginx\_no\_mitigation.html:

**A screenshot of a graph

Description automatically generated**

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.