Table of Contents

Lab Objectives:

1. Slowloris is a type of attack that can cause a website or web server from working. It was created by Robert "RSnake" Hansen. The attack works by keeping many connections open to the target server for as long as possible. It does this by connecting to the server but only completing part of the request.

2. Slowloris sends some information to the server but never finishes making the request. The server keeps these incomplete connections open, waiting for the request to be completed. Slowloris keeps sending more information without completing the request, forcing the server to keep the connections open.

3. This behavior eventually overwhelms the server's ability to handle new connections from legitimate users. The server has a limit on how many connections it can handle at once, and Slowloris uses up all those connections with its incomplete requests. This prevents legitimate users from connecting to the server and using it usually.

4. It is important to know that performing a Slowloris attack is illegal and unethical. Knowledge about this attack should be used to protect your servers from such attacks instead.

Creating Your Website

To make your web server unique, you can create and upload your own webpage. Here is how you can do it:

1. Locate the "data" folder on your desktop.

2. Find the "index" or "index.html" file in that folder.

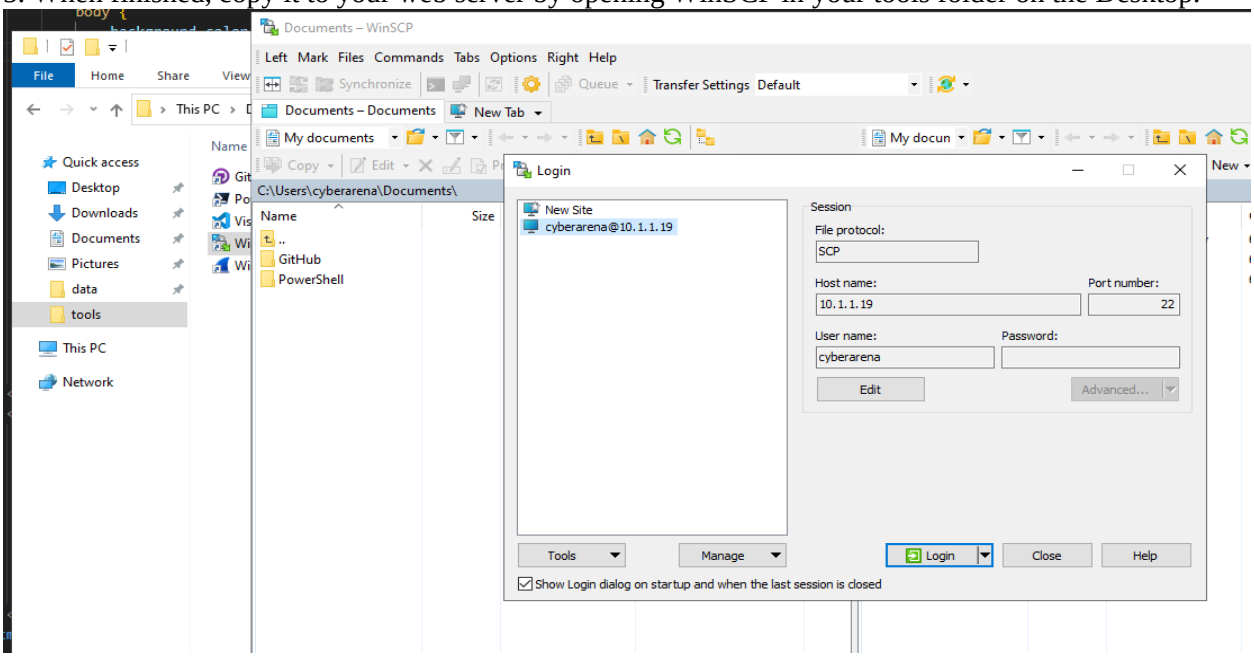
3. Right-click on the file and choose the option "Edit with Code" (or any text editor of your choice).

Now, you will see the default webpage content. You can use this content or modify it to create your personalized webpage. If you need help producing creative ideas for your webpage, feel free to ask ChatGPT for suggestions.

TIP: To copy and paste between ChatGPT and your lab environment, you must click on the desktop in your browser and type Ctrl-Alt-Shift (or swipe for touch screen). This will open the clipboard shared between your lab and your computer. You can paste it inside the clipboard textbox. Then, when you click into the lab, you will be able to paste the clipboard's contents.

4. Test your site on the desktop by right-clicking anywhere in Visual Studio Code and selecting Show Preview.

5. When finished, copy it to your web server by opening WinSCP in your tools folder on the Desktop.

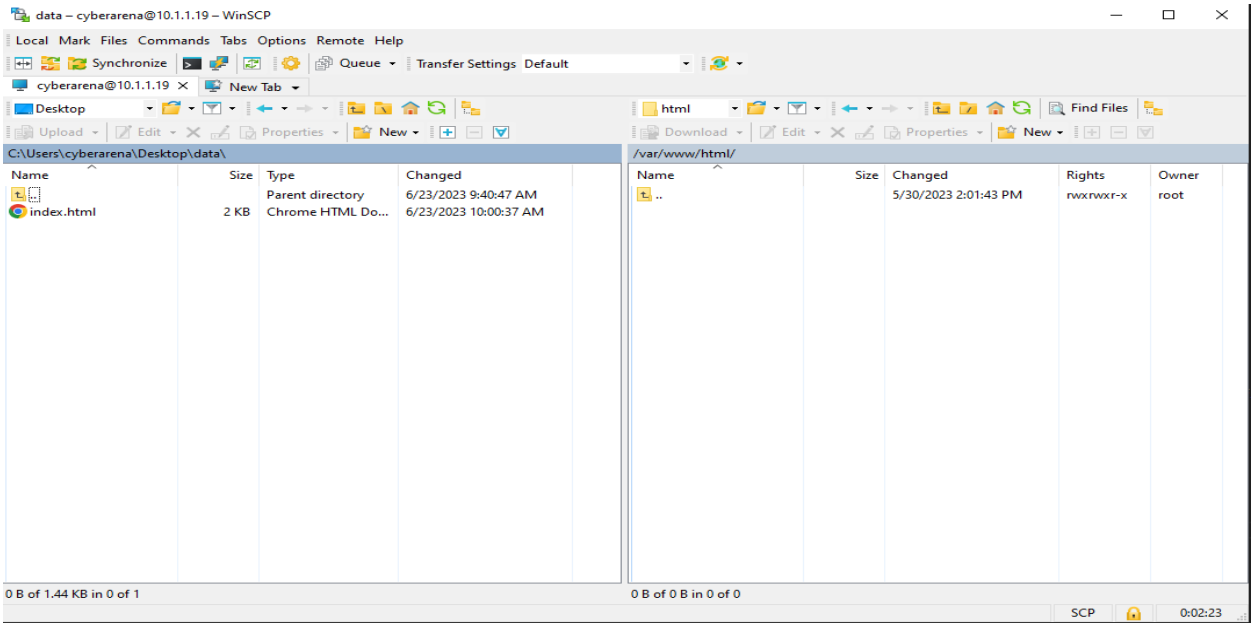


Accessing your Servers:

6. log in to the "cyberarena@10.1.1.19" connection using the "Let's workout!" password. This will establish a secure connection between your desktop and the SSH webserver, allowing file transfer.

7. Once connected, you will see a split screen. You will see your desktop on the left side (with caps-lock). You will see your web server on the right side (with enter).

8. Double-click on the grey bar in the desktop section to open the "C:\Users\cyberarena\Desktop\data" folder. Double-click on the grey bar in the web server section and enter the directory "/var/www/html".



3. Finally, copy over your index.html from the Desktop to the web server by dragging and dropping.
4. The /var/www/html folder is the default location that content is served on your web server, and your web server will automatically look for an index.html file. You can check this by opening up a browser in the lab and navigating to http://10.1.1.19.

   NOTE: Anyone else in the world can access your site by using the DNS name on your workout landing page

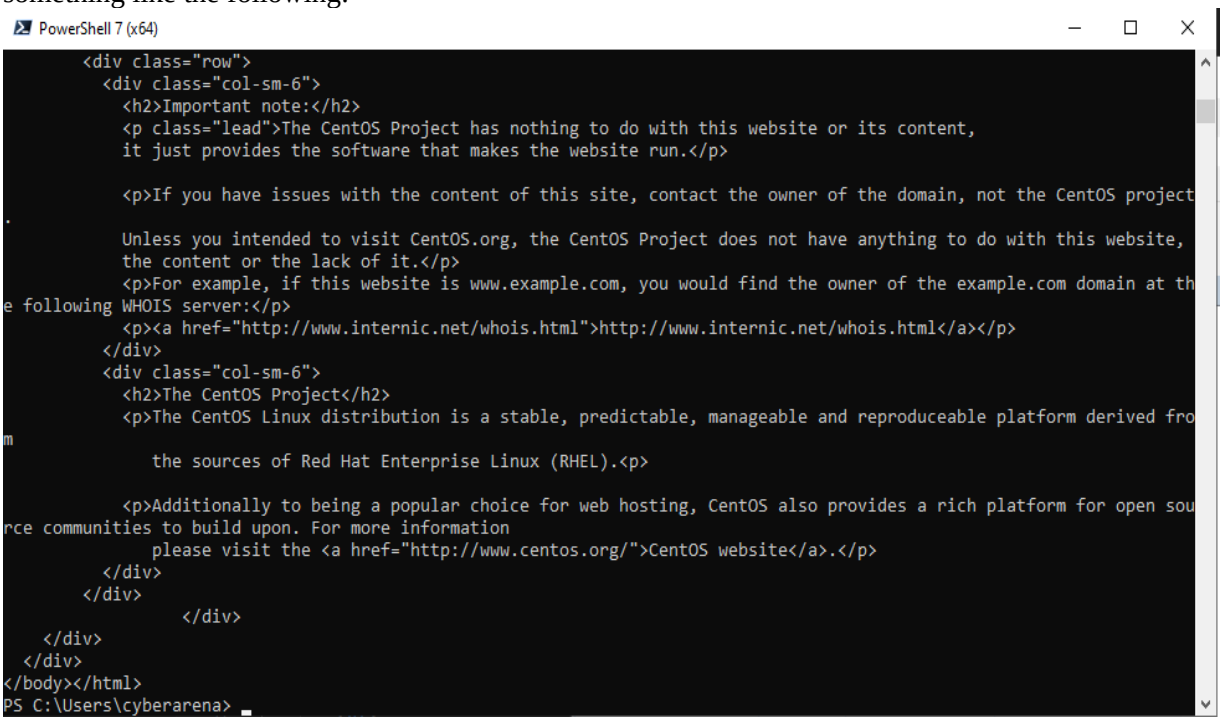
Attacking the webserver:

Preparing the test command

By this point, you should have a PowerShell window by clicking on the arrow button next to the Chrome browser icon on the taskbar.

Then run the command below:

The curl (client URL) command is like opening the website in your browser, but it allows us to have instant feedback to know if the website is responding. When you run the command, you should see something like the following:



We will use this to test the slowloris attack in a moment. Just keep the window open for now

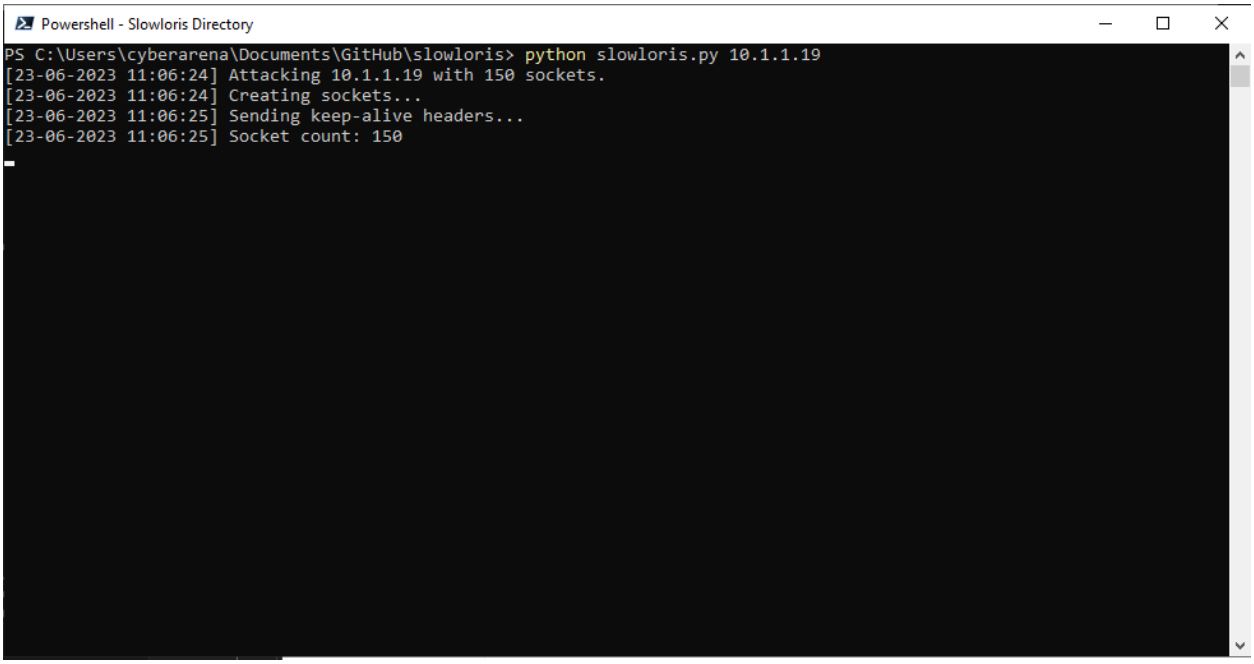
Running Slowloris

To run slowloris, go to your Tools folder and double-click on the PowerShell - Slowloris Directory shortcut file. Once PowerShell opens, you can run the following command:

Run the following commands in the box below to start Sliver.

```
Python slowloris.py 10.1.1.19
```

This will start the Slowloris attack, and you can test this, but going to your curl PowerShell window, and rerunning the command to see if the page will load.

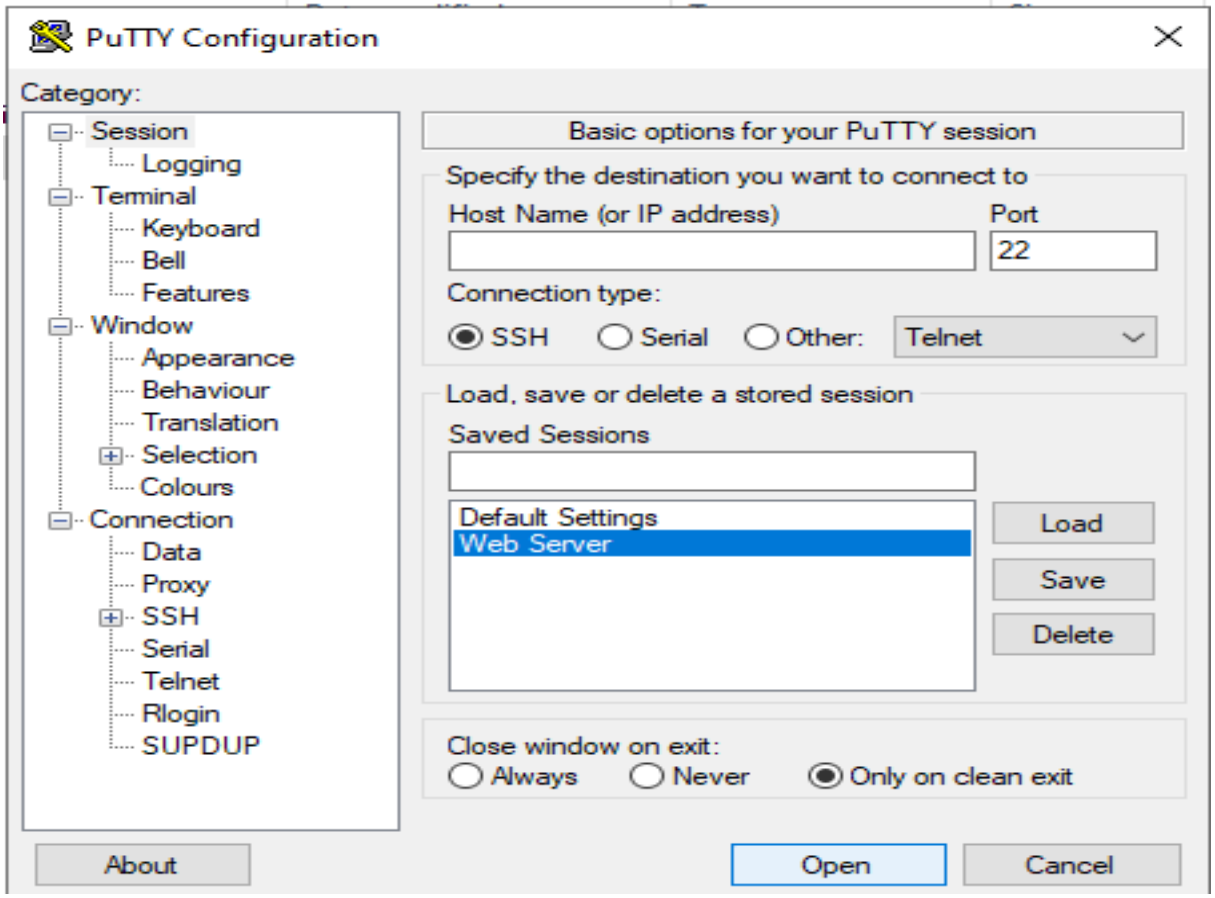


Stop the attack, type Ctrl+C (you may have to type this twice). You should be able to see that your website will quit loading during the attack. If this does not work, you can use the command line option -s to increase the number of threads that will run against the webserver.

You can show this to your instructor by asking them to pull the website on their computer and browse to the DNS that you have listed on your workout landing page

Securing the Website

To secure the website from a slowloris attack, you have a few options. Begin by opening an SSH session using the PuTTY client in your tools folder on the Desktop. Then, select the Web Server connection and click Open.



Use the following credentials

User: cyberarena Password: Let's workout !

This will be a BLIND password Prompt you will NOT see the password as it is being typed

Your first option is to set a timeout on incoming requests using the mod_reqtimeout module. If a request is not complete within the specified time, the module closes the connection. This helps to ensure that Slowloris cannot keep connections open indefinitely. To add this setting perform the following on your open SSH PuTTY connection.

1. Edit the configuration file by typing:

```
Sudo vi /etc/httpd/conf/httpd.conf
```

2. Scroll to the bottom of the file, and type the following:


```
<IfModule reqtimeout_module>

RequestReadTimeout header=20-40,MinRate=500 body=20,MinRate=500
</IFModule>
```

3. Type escape and then :wq which means write the file and quit vi). This will save the configuration file.
4. Reload the web server by typing:

```
Sudo systemctl reload httpd
```

This should reduce the effect of slowloris on your web server. You can also edit the same httpd.conf file and limit the number of connections a client can claim. To do so, you would, again, scroll to the bottom of the file and add the configuration

```
<IfModule mod_limitipconn.c>
<location />
maxConnPerIP 1
</Location>
</IfModule>
```

 Don't forget to reload httpd. *