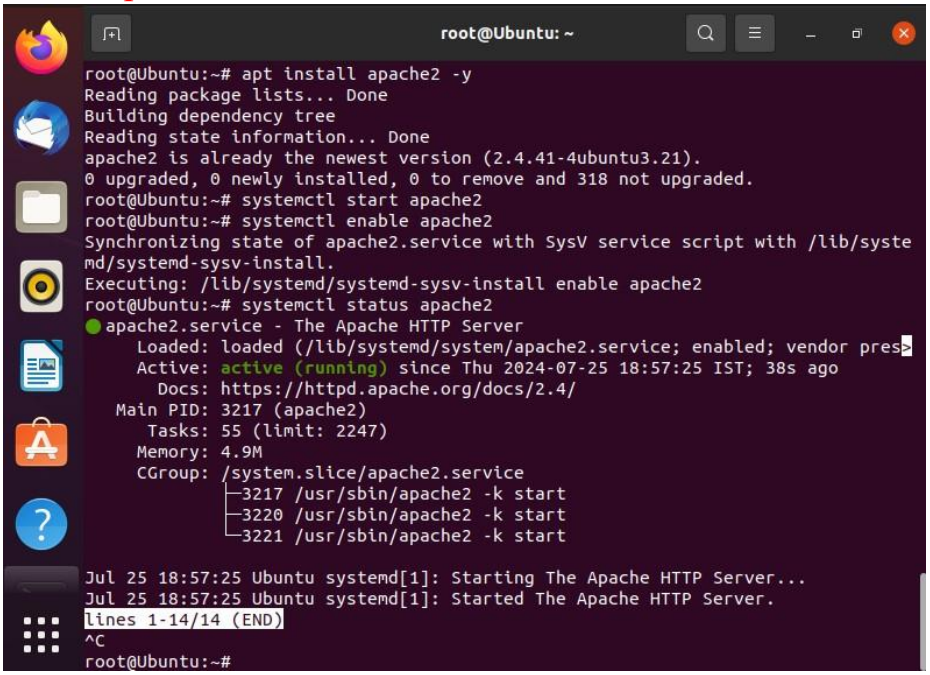
Implementing basic HTTP authentication to protect the website with a username and password

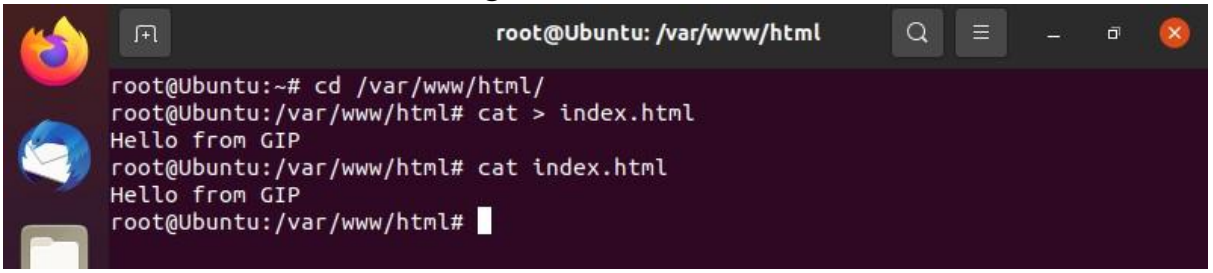
An Ubuntu 20.04 VM must be installed on your machine.

Solution:

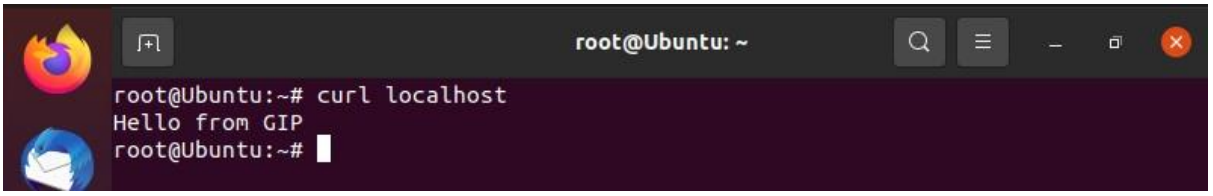
Step 1: Install the apache2 package using the apt install apache2 -y command. Start and enable the apache2 service using the systemctl start apache2 and systemctl enable apache2 commands. Check the status of the service using the systemctl status apache2 command.



Step 2: Go to the location /var/www/html and create a file named index.html. Add the content "Hello from GIP" using the cat > index.html command. Check whether the content is there using the cat index.html command.

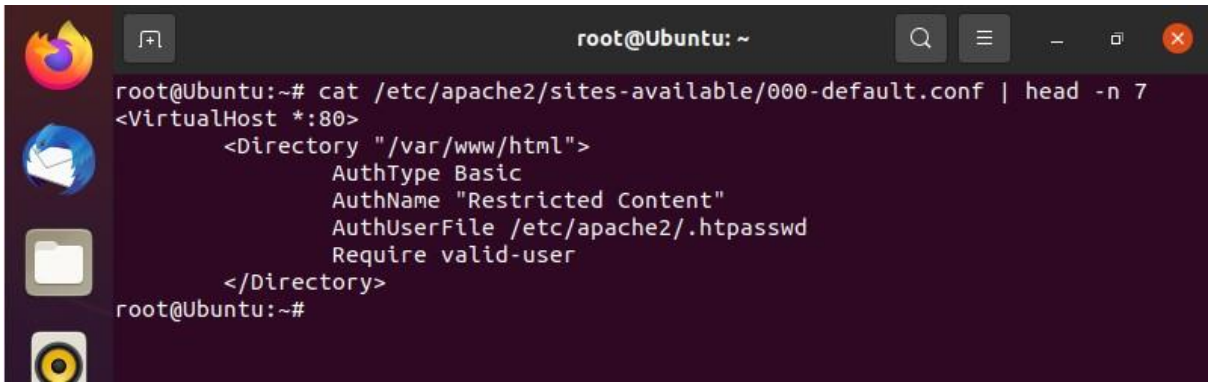


Step 3: Run the curl localhost command to check if a successful exchange occurs between the device and the server.

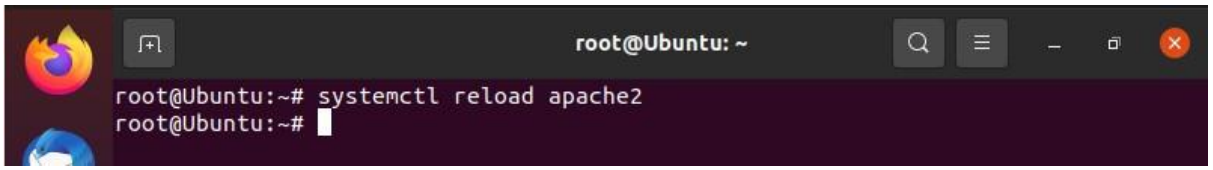


Step 4: Install the apache2-utils package using the apt install apache2-utils -y command. After that, run the htpasswd -c /etc/apache2/. htpasswd <user_name> command. This command creates a new password file for basic authentication in Apache and adds a user <user_name> to it with a password prompt. The -c option specifies that the file should be created if it does not already exist. Enter the password for that user when prompted.

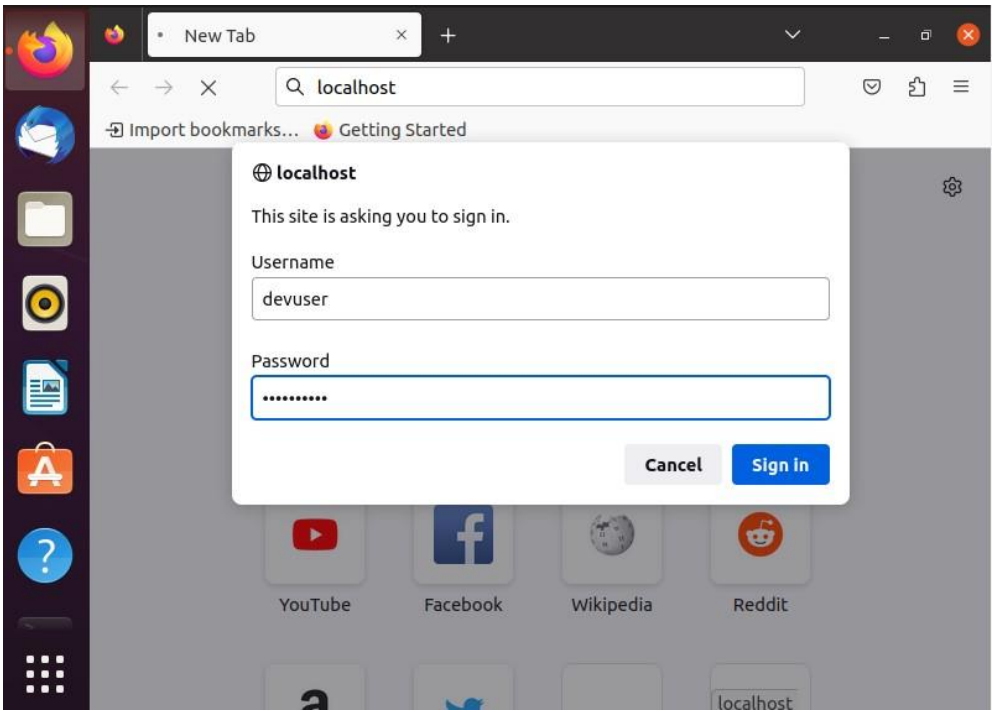
Step 5: Add the following lines to the /etc/apache2/sites-available/000-default.conf file to modify the default configuration.



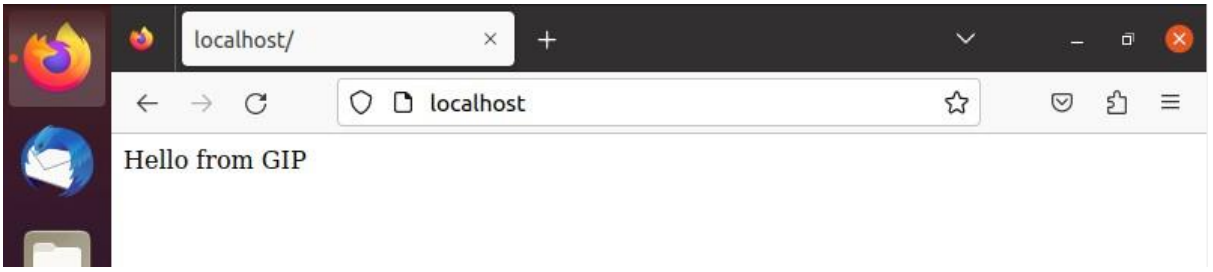
Step 6 - Reload the apache2 service to apply changes using the **'systemctl reload apache2'** command



Step 7 - On the browser, enter **http://localhost**, you will get the prompt to enter your username and password. Enter the correct username and password and click on sign in.



Step 8 - After clicking on sign in, you can see 'Hello from GIP' on the web page.



Task Successfully Completed

dasaremahir333@gmail.com