

## Network Operating Systems Experience – Part 2

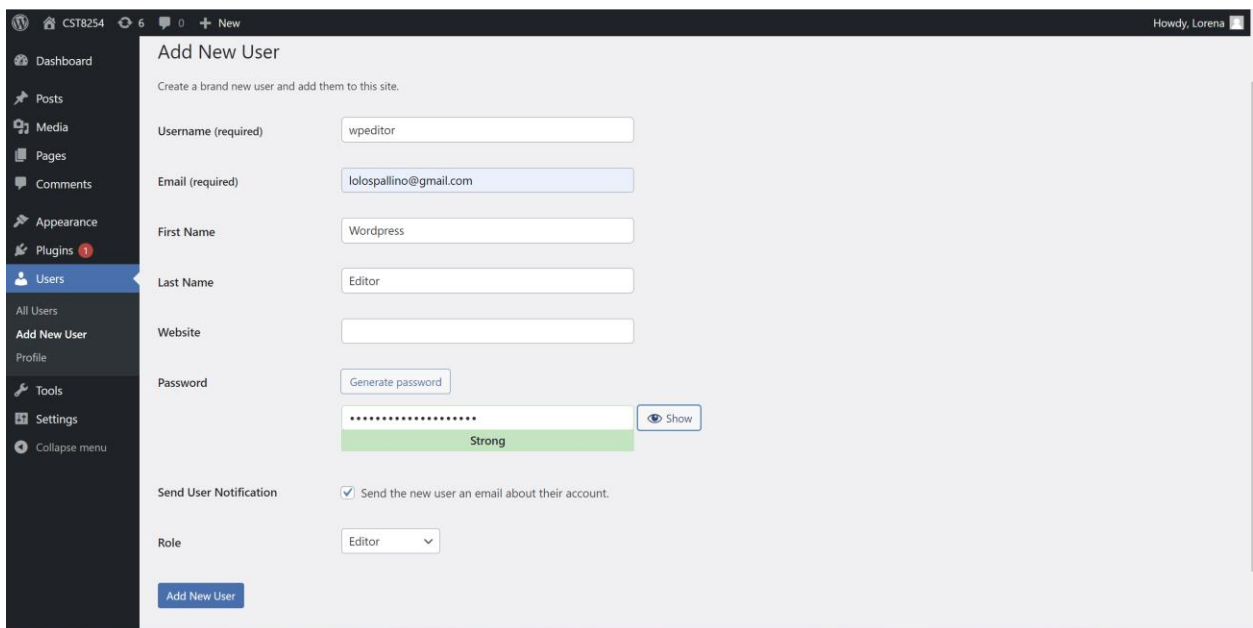
### Part A

Login to Wordpress on the Ubuntu server with your admin account to perform the following tasks.

1. Create 2 WordPress users with the following properties.

a. username : wpeditor, password : (you choose one), First Name :

WordPress, Last Name : Editor, Role : Editor

A screenshot of the WordPress administration interface showing the 'Add New User' form. The left sidebar contains navigation links: Dashboard, Posts, Media, Pages, Comments, Appearance, Plugins (with a red notification icon), Users (highlighted), All Users, Add New User, Profile, Tools, Settings, and Collapse menu. The main content area is titled 'Add New User' and includes the instruction 'Create a brand new user and add them to this site.' The form fields are: Username (required) with value 'wpeditor', Email (required) with value 'lolospallino@gmail.com', First Name with value 'Wordpress', Last Name with value 'Editor', Website (empty), Password (with a 'Generate password' button and a strength indicator showing 'Strong'), Send User Notification (checked), and Role (dropdown menu set to 'Editor'). A blue 'Add New User' button is at the bottom left. The top of the interface shows the site name 'CST8254', a user profile picture, and the text 'Howdy, Lorena'.

b. username : wpcontributor, password : (you choose one), First Name :

WordPress, Last Name : Contributor, Role : Contributor

**Add New User**

Create a brand new user and add them to this site.

Username (required): wpcontributor

Email (required): lorenna.spallino01@gmail.com

First Name: WordPress

Last Name: Contributor

Website:

Password:  [Generate password](#) [Show](#)

Send User Notification: ☒ Send the new user an email about their account.

Role: Contributor

[Add New User](#)

Click users in the left hand menu and place a screenshot of the users including the newly created ones.

**Users** [Add New User](#)

This theme recommends the following plugins: [Instagram Widget by WPZOOM](#), [One Click Demo Import](#), [Social Icons Widget by WPZOOM](#), [Video Popup Block by WPZOOM](#), [WPZOOM Forms](#) and [WPZOOM Portfolio](#). [Begin installing plugins](#) | [Dismiss this notice](#)

All (3) | Administrator (1) | Editor (1) | Contributor (1)

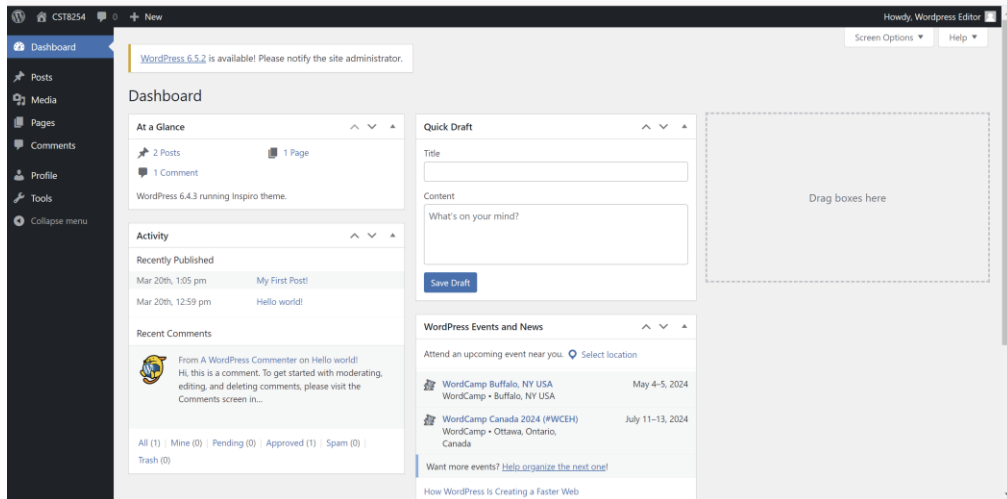
Bulk actions  [Apply](#) [Change role to...](#) [Change](#) [Search Users](#) 3 items

<input type="checkbox"/>	Username	Name	Email	Role	Posts
<input type="checkbox"/>	Lorena	—	spal0013@algonquinlive.com	Administrator	2
<input type="checkbox"/>	wpcontributor	WordPress Contributor	lorena.spallino01@gmail.com	Contributor	0
<input type="checkbox"/>	wpeditor	WordPress Editor	lolospallino@gmail.com	Editor	0

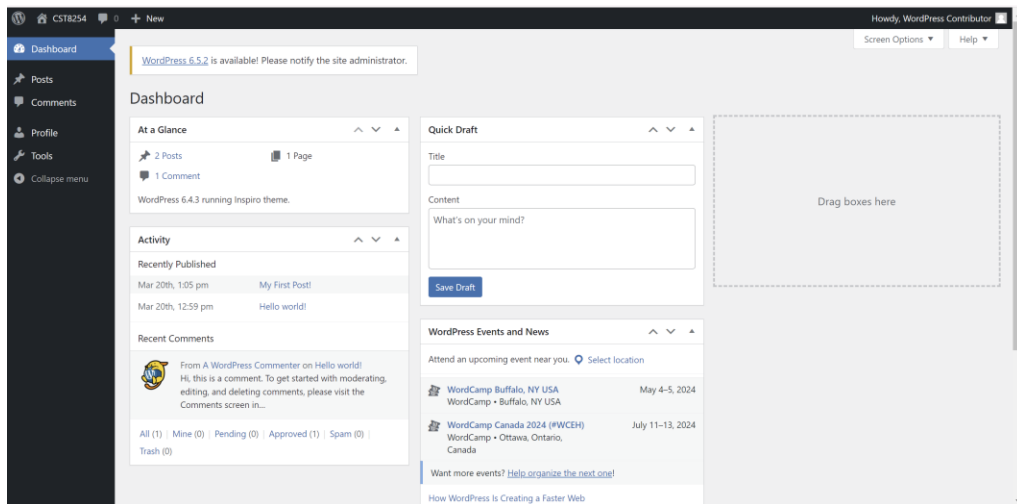
Bulk actions  [Apply](#) [Change role to...](#) [Change](#) 3 items

2. Log in as both of the new users and click the Dashboard in the menu on the left hand side to open the users' Dashboard. Take a screenshot of the both users dashboard.

### a) Wpeditor



### b) Wpcontributor



3. Name 2 differences in the tasks that both users are able to perform from the menu on the left hand side?

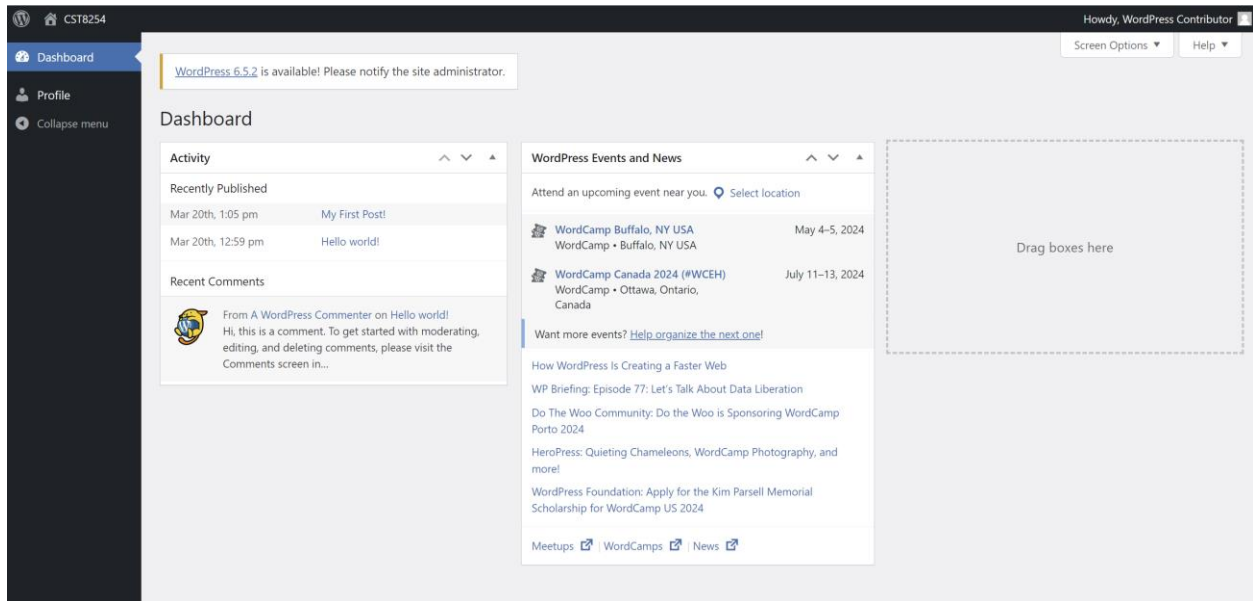
As evidently seen in the left-hand sides of the previous two screenshots, the possible and available tasks that these users are able to perform is

different from each other, and they are both very different from my administrator account. The first difference between the wpeditor and the wpcontributor accounts is that the editor account has access to the “media” tab while the contributor account does not. This means that the editor can upload media and view the media library while the contributor does not have access to this task. Additionally, the second difference in tasks is that the editor account has access to the “pages” tab on the left-hand side, allowing this user to view the current pages, edit them and add additional pages. On the other hand, the contributor account does not have access to this tab and is not permitted to perform these tasks on the site’s pages. While these accounts are different in their own ways, they are both similar when comparing to the administrative user. While the admin user has access to add edit and delete users in the users tab, they have access to control the site’s settings in the settings tab they can control plugins in the plugins tab and can change the appearance in the appearance tab.

**a. What role is the most restrictive role in Wordpress? When would you use this role?**

The most restrictive role in wordpress is the role known as Subscriber. This user does not have access to edit or contribute to anything, they simply have access to view the news in the dashboard and view the preview of the site. I have changed the wpcontributor’s role from contributor to subscriber to demonstrate this. As shown in the screenshot below, the subscriber has limited

to no tasks available at all. On the left-hand side the only tabs available are dashboard and profile. Additionally, they are only able to view the site and not make any changes to it.



#### 4. What is a plugin in WordPress?

Plugins in WordPress are pieces of software geared towards performing specific tasks. These plugins or pieces of software can be downloaded and activated by the administrator on the WordPress account, and can then be applied to the WordPress site. These plugins can give the site additional functionality and extend on previous functionalities on your site. These allow for WordPress to create any kind of website, including ecommerce stores, online presence, blogs or anything else.

#### 5. Give 2 steps that can be taken to diagnose WordPress plugins that are not working?

The first step that can be taken to diagnose a Plugin that may not be working is by deactivating the current theme that may be applied to the site and changing it to a very neutral theme such as the default or “Twenty-Twenty”. Often, the theme may be limiting or restricting certain capabilities that the plugin offers, and therefore will not work properly if at all. If the issue resolves after changing to a neutral theme, it is reasonable to conclude that the theme was the issue and try to find a more suitable theme that fits the needs of the site. Additionally, a second step to take if the problem still persists is to manually deactivate all plugins in order to determine which one specifically is causing an issue. In the plugins tab, you can manually and temporarily deactivate all plugins installed onto your site. That would likely solve the plugin related problem. Then to determine which individual plugin is causing the problem you can activate one plugin at a time, checking at which one the issue reappears. Then you will know which plugin is giving you issues and can contact wordpress support from there. Additionally, if WordPress needs to update, it is a good idea to update it as soon as possible, this may solve plugin related issues as well.

## **Part B**

### **1. Log on to your Ubuntu server locally and list the firewall rules in Iptables.**

**Place a screenshot of the rules.**

After logging in locally to the Ubuntu server, I used the command `sudo iptables -L` to show the current iptables which act as firewalls in ubuntu. The image below shows the iptables firewall rules on my server.

```
Last login: Tue Apr 16 12:38:02 UTC 2024 from 192.168.1.174 on pts/0
lorena@raspberrypi:~$ sudo iptables -L
[sudo] password for lorena:
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
lorena@raspberrypi:~$ _
```

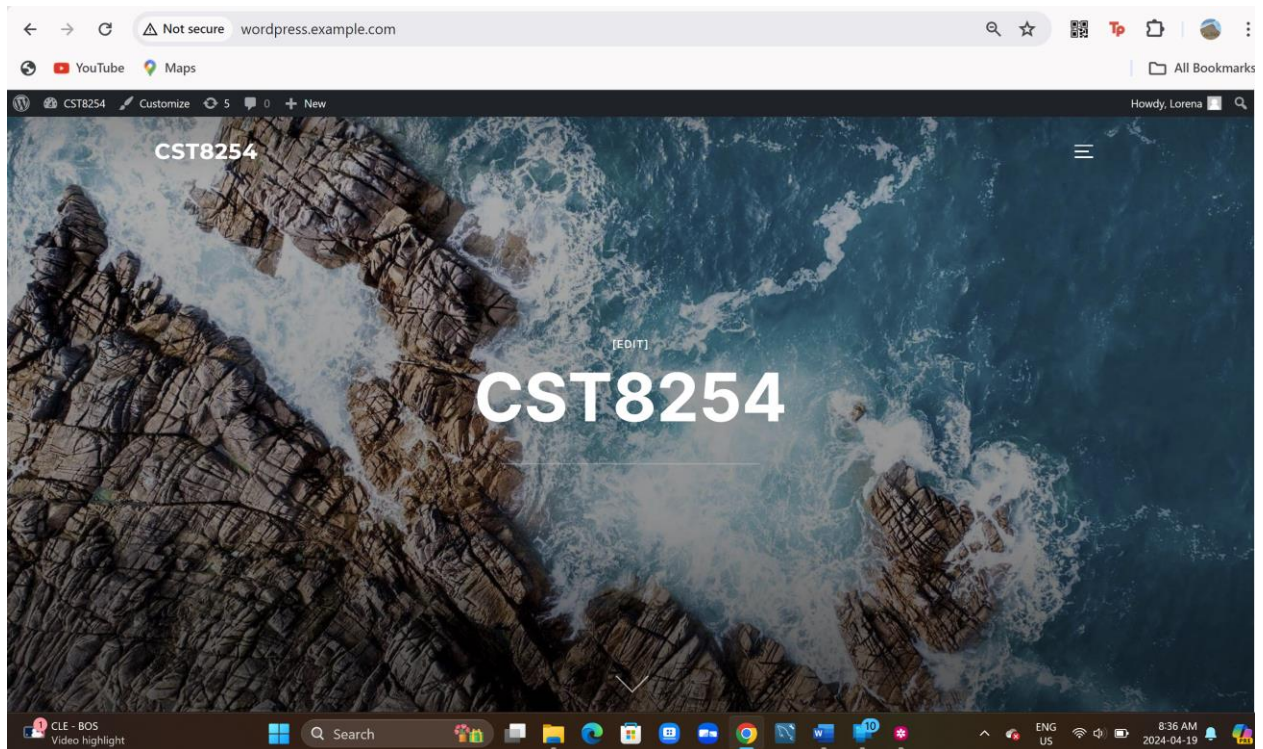
**2. Go to your laptop and ensure that you can connect to the Apache Website on the Ubuntu server**

On my laptop, after typing in my Server’s IP address into the browser’s search bar, I access one of the webpages I made on the Apache webserver. Evidently, from the screenshot below I have access to the Apache website, as well as Wordpress, which is also running on the apache webserver.

After typing the IP address:



Wordpress site:



3. We will now use the firewall to block access to the webserver. Enter the appropriate command to drop http and https traffic. Put the command you used here.

The command I use to drop http and https traffic on my server is: `sudo iptables -I INPUT 1 -p tcp --dport 80 -j DROP` This drops port 80, which is the port used by http and https. The image below shows the command on the server's terminal.

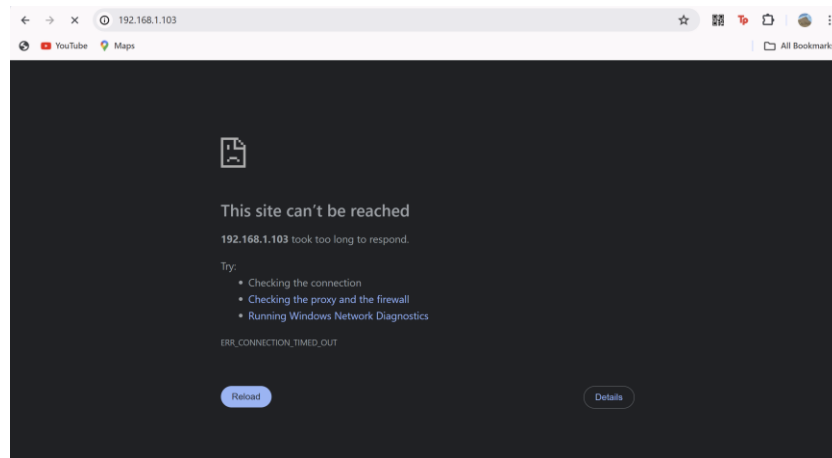
```
target      port      opt      source      destination
lorena@raspberrypi:~$ sudo iptables -I INPUT 1 -p tcp --dport 80 -j DROP
lorena@raspberrypi:~$ _
```



#### 4. Try connecting to the webserver

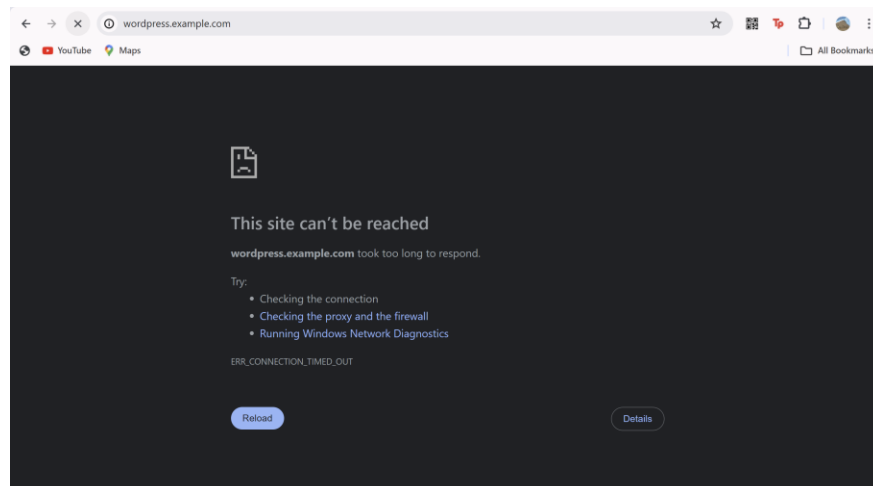
##### a. Can you connect (yes/no)?

As shown in the screenshot below, when I now try to connect to the apache site by typing the IP address, I get an error message.



##### b. Put a screenshot of you attempting to connect to the WordPress site.

After attempting to connect to the wordpress site, I get the same error, as shown below.



**c. Put a screenshot of the rules.**

The image below lists the rules of the iptables, and evidently, the tcp for http/https has been dropped, and therefore will not allow access to connect to the sites on the webserver.

```
lorena@raspberrypi:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:http
DROP      tcp  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
lorena@raspberrypi:~$ _
```

**5. Let us now reverse what we have done and allow web traffic using the following command which puts the rule at the top so that it gets executed first.**

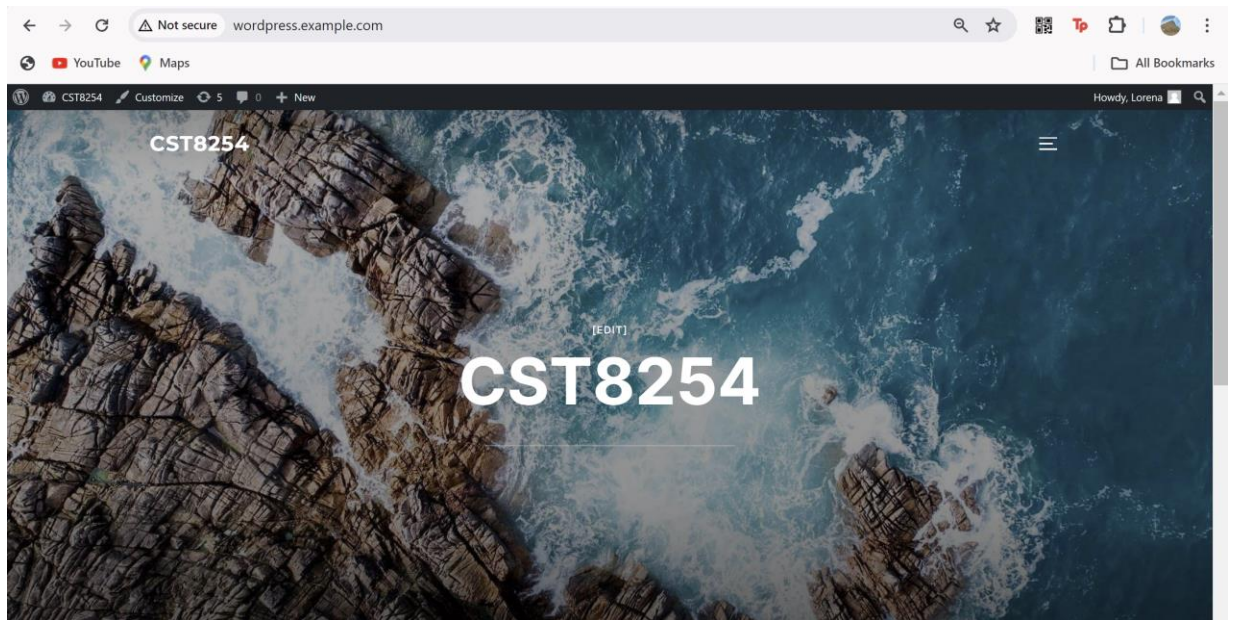
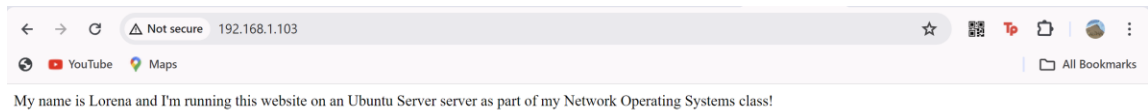
**a. Put the rule that you would use to do this.**

The rule I would use is shown below. This would automatically allow web traffic to my webserver, and since it is input first, it will be executed first. This automatically accepts all policies.

**Sudo iptables -I INPUT -j ACCEPT**

**b. Can you access the webserver now? (Yes/No)**

Yes I can, as evidently seen in the following screenshots of the sites on my webserver.



**c. Put a screenshot of the rules in Iptables.**

The image below shows the command to accept web traffic and lists the rules in iptables. Evidently, now allowing web traffic.

```
lorena@raspberrypi:~$ sudo iptables -I INPUT -j ACCEPT
lorena@raspberrypi:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  anywhere               anywhere
DROP       tcp  --  anywhere               anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
lorena@raspberrypi:~$
```

6. Use the appropriate rules to prevent users from pinging the Ubuntu server.

a. Put the command that you used here.

The first thing that I would do is flush the iptables to reverse the command which sets all policies default to accept (to reverse this command: Sudo iptables -I INPUT -j ACCEPT)

Command to flush iptables: `sudo iptables -F`

Then, the command I used to prevent pinging is: `sudo iptables -A INPUT -p icmp -j DROP` This blocks the icmp protocol which allows for pinging. The screenshot of this command in the terminal is shown below.

```

lorena@raspberrypi:~$ sudo iptables -F
lorena@raspberrypi:~$ sudo iptables -A INPUT -p icmp -j DROP
lorena@raspberrypi:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      icmp -- anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
lorena@raspberrypi:~$

```

**b. Put a screenshot of an unsuccessful ping.**

```

C:\Users\lolos> ping 192.168.1.103

Pinging 192.168.1.103 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.103:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\lolos>

```

As seen in the screenshot above, now that I have blocked icmp protocol in iptables, the pings from my laptop to my server have failed and are certainly unsuccessful.

## References

Fitzgerald, A. (2021, February 18). The Ultimate Guide to WordPress Plugins: 19 Examples & How They Work. HubSpot Blog. Retrieved April 19, 2024, from <https://blog.hubspot.com/website/wordpress-plugins>

Guide, S. (2023, October 15). Troubleshooting Common WordPress Plugin Issues: A Guide to Seamless Website Maintenance. LinkedIn. Retrieved April 19, 2024, from <https://www.linkedin.com/pulse/troubleshooting-common-wordpress-plugin-issues-guide-seamless-r>

need iptables rule to accept all incoming traffic. (2013, August 20). Super User. Retrieved April 19, 2024, from <https://superuser.com/questions/634469/need-iptables-rule-to-accept-all-incoming-traffic>

Solve Problems With Plugins – WordPress.com Support. (n.d.). WordPress.com. Retrieved April 19, 2024, from <https://wordpress.com/support/plugins/solve-problems-with-plugins/>