Mission: Permissions 2 Workout Student Instructions

Introduction:

In the first addition of Mission: Permissions, you learned about the Windows file system and how to modify permissions for users and user groups on a folder or file. In the greatly anticipated sequel to Mission: Permission, we will introduce you to the Linux file system! For this one, you'll be using the terminal and the system command *chmod*. This website gives a brief rundown of chmod and appropriate values.

Logging on to Your Computer:

- Log into the Guacamole web server using the username and password provided on your Cyber Gym student landing page.
- You may have to refresh the page if a screen does not come up.
- Then, you will log in automatically.

Your Mission:

Although you stemmed the tide on the Windows system, the security team noticed that another folder was vulnerable to the world. This time it's on their Linux server! Good thing you just learned about this topic and are ready to assist them. First, open up your computer terminal by clicking second icon from the left on the at the bottom of the screen. Hovering over it should say, *Terminal Emulator*. Run the following command to move to the location of the vulnerable file:

```
cd /usr/local/etc/protect_me/
```

Now view what permissions are currently set by typing the following:

```
ls -la
```

Use the website provided earlier to figure out what access rules or permissions are currently set for the file *vulnerable.txt*.

For security purposes, the security staff wants the file to meet the following permissions:

- Only you (the owner of the file) have access to read, write, and execute
- Groups can read, *but not write or execute*
- Other users (the world) *shouldn't have any access*

To properly run each command you will need to run it as *sudo*.

Example: *sudo chmod 777 /example/file/file.txt*