CMPS 3680 Guided Lab 8

Spring 2024

For this assignment you will be using the Linux server that you set up in Lab 7.

Part 1 - SSH Key Setup

1. **WARNING:** Only do this section if you are using your **OWN** laptop or computer.
   Setting up an SSH key-pair for your server will increase security and save you time!
2. First, open up a terminal application that supports the ssh-keygen command:
   - For Windows: Use **`PowerShell`** or **`WSL`**
   - For Mac/Linux: Use **`Terminal`**
3. Use the following command to generate public/private keys for your machine:

   ```
   ssh-keygen
   ```

   Note: Without any cli arguments, the default algorithm for the keys will be RSA
4. When you first enter the command above, it will ask you a few additional questions.
   You can simply press enter a few times to accept the default values.
5. Once completed, you will have a .ssh folder in your home folder with two new files: **`id_rsa`** and **`id_rsa.pub`**
6. To add your machine's public key to an existing user on an existing server you can simple run the command:

   ```
   ssh-copy-id username@server
   ```
7. Alternatively, if the command above does not work you will need to login to your remote server and manually create the .ssh folder if it doesn't already exist (and set the proper permissions):

   ```
   mkdir ~/.ssh
   chmod 700 .ssh
   ```
8. Once the .ssh folder is created, create an authorized_keys file inside it with the proper permissions:

   ```
   cd ~/.ssh
   touch authorized_keys
   chmod 600 authorized_keys
   ```
9. Finally, copy the contents of the **id_rsa.pub** file on your machine to the authorized_keys file on your server.

Part 2 - SSL/TSL With Certbot

1. If you have completed Lab 7 properly, and you already have a domain name assigned to your server, you should be able to follow the guide provided by CertBot to validate your server and reroute all traffic through https: https://certbot.eff.org/instructions?ws=apache&os=ubuntufocal
2. Type the following command to allow traffic through port 443 to apache:

   ```
   sudo ufw allow 'Apache Full'
   ```
3. Once completed, all traffic to your site will be routed through the new Apache config using SSL on port 443.
   You can test this by going to your site's URL in the browser and seeing the secure symbol next to the url.
   Depending on your browser the icon usually appears as a green checkmark or lock like this: