**Project 1**

**Name:** Tanya Peddi

**UNCC ID:** 800968024

**Aim:** To setup an Apache web server with OpenSSL enabled on it.

**Setups**

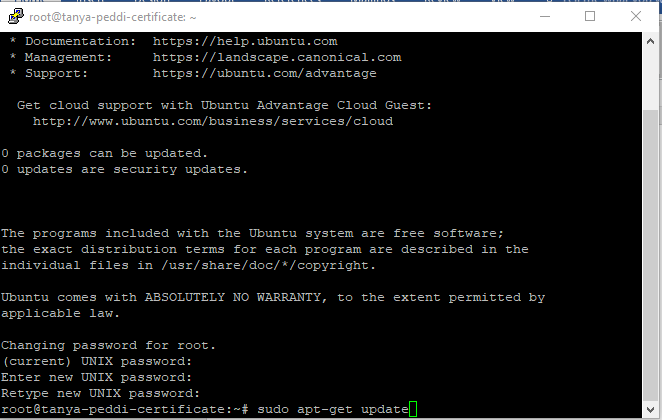
* We created an Ubuntu droplet and use it as an instance using DigitalOcean’s cloud sources
* We downloaded Putty serve to telnet the Ubuntu server

**Steps performed**

* Opened the instance using the IP address through Putty
* Login was done using the username root and passowrd provided by DigitalOcean. We then changed the password.

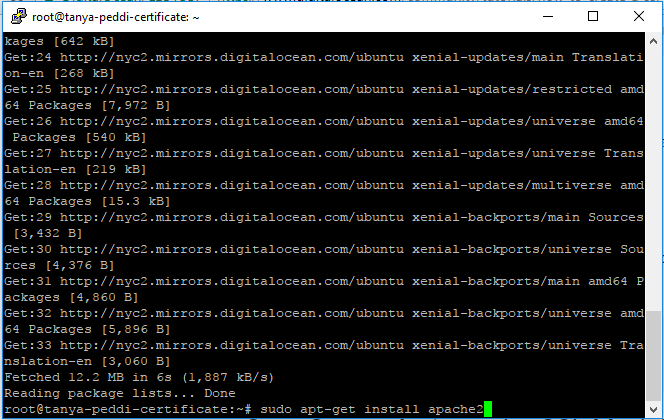
1. **Update all the packages**

*sudo apt-get update*



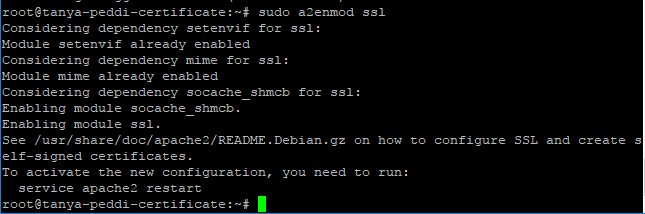
1. **Install Apache**

*sudo apt-get install apache2*



1. **Enable SSL module for Apache2**

*sudo a2enmod ssl*



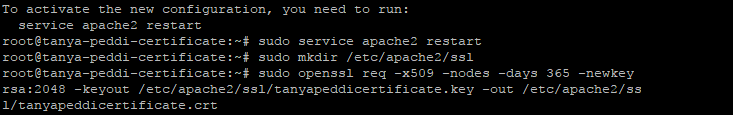
1. **Restart Apache server to apply all the configurations if any**.

*sudo service apache2 restart*

1. **Create self-signed Certificate**

*sudo mkdir /etc/apache2/ssl*

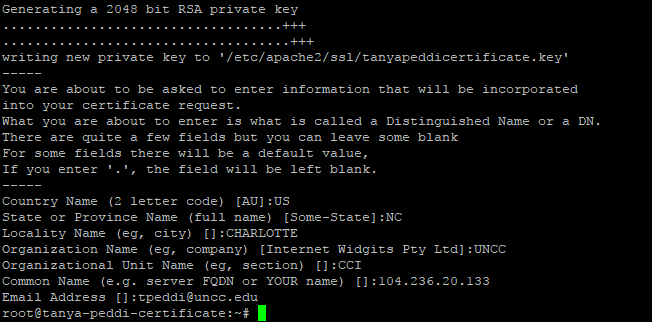
*sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/tanyapeddicertificate.key -out /etc/apache2/ssl/tanyapeddicertificate.crt*



x509 – Public Key Standard

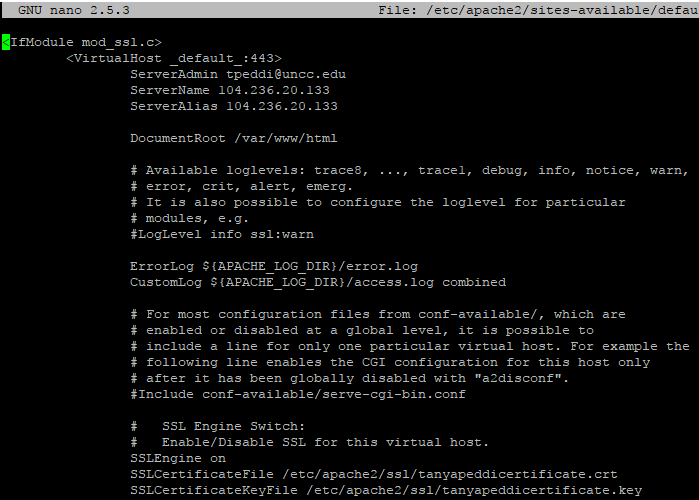
365 – Validity for certificate

RSA 2048 – Algorithm used to create key of 2048 bits



1. **Updating the configuration file of Apache to reflect created certificate**

*sudo nano etc/apache2/sites-available/default-ssl.conf*



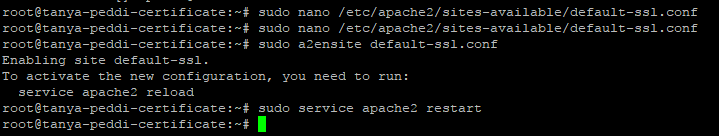
We make relevant changes to the configuration file such as adding in ServerName, ServerAlias, SSLCertificateFile and SSLCertificateKeyFile.

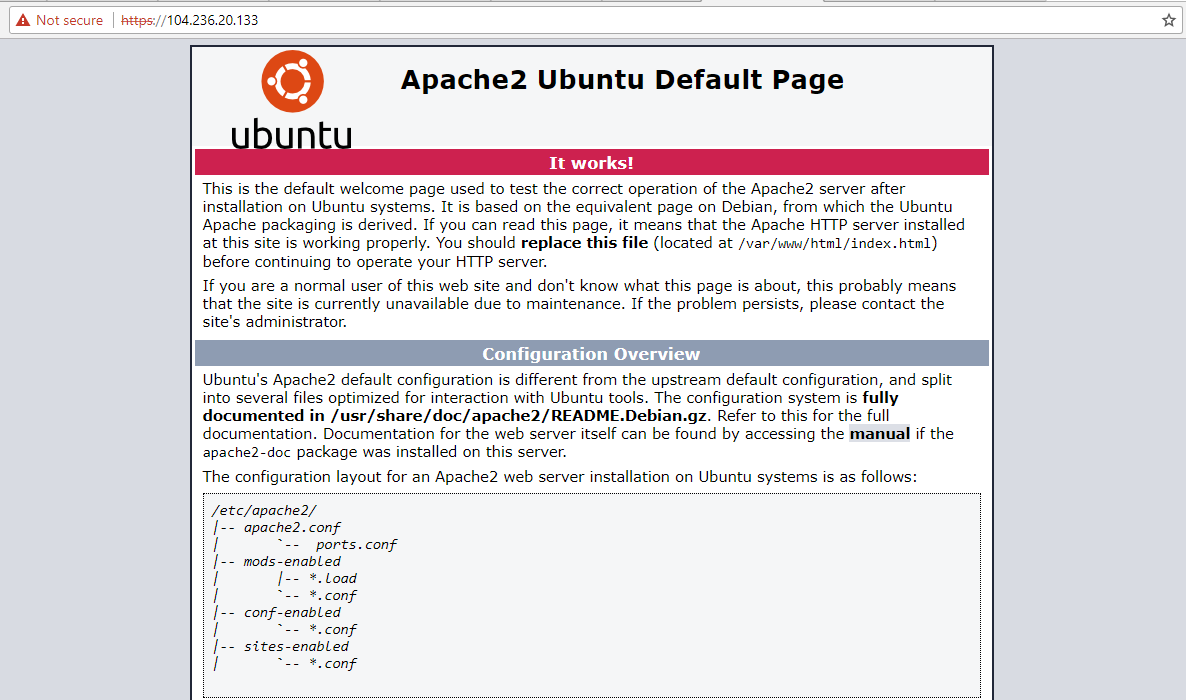
1. **Activated SSL**

*sudo a2ensite default-ssl.conf*

1. **Restarting Apache**

*sudo service apache2 restart*



1. **On browser, we typed in** [**https://104.236.20.133**](https://104.236.20.133) **i.e. our domain name. The browser deemed it unsafe so we clicked *Proceed anyway* option**

**Certificate tested for online resource:**