**Deploying SSL Certificate**

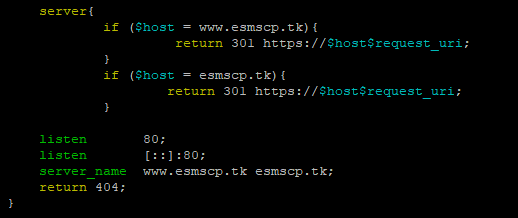
# **Objectives:**

* Obtain and installation of SSL certificate from a Certificate Authority
* Allow transmission of sensitive information with an encrypted connection

# **Prerequisites:**

* Obtain a domain name from freenom.com and point to our AWS instance’s elastic IP
* Ensure HTTPS/443 port is opened in AWS security group
* Install dependencies (yum install pip yum python-pip and pip install cryptography)

# **Installation steps:**

1. Install Let’s Encrypt(Certificate Issuer)’s client, CertBot on our instance
2. Run Certbot to install certificate with “certonly” option (certbot certonly)
3. Enter “2” for webroot installation when prompted
4. Enter domain name “[www.esmscp.tk](http://www.esmscp.tk)” when prompted
5. Enter webroot “/usr/share/nginx/html” when prompted
6. It should show that certificate has been issued. Copy the directory of “fullchain.pem” and “privkey.pem”
7. Edit nginx configuration file to include the provided files (sudo vim /etc/nginx/nginx.conf)
8. Edit settings.py to include our domain in the list of allowed hosts (cd Django\_Application/virtual\_env/ICA-1/ICA/ICA/settings.py)
9. Edit nginx configuration file to redirect requests to include ‘https’. (sudo vim /etc/nginx/nginx.conf)
10. Restart the server for changes to take effect (sudo service nginx restart)

Source: <https://pyliaorachel.github.io/blog/tech/system/2017/07/14/nginx-server-ssl-setup-on-aws-ec2-linux-with-letsencrypt.html>