Enable HTTPs on NginX

1. Create a directory to hold certificates and keys:

   `sudo mkdir /etc/nginx/ssl`

2. Go to folder and enter following commands to create a certificate and SSL key:

   `cd /etc/nginx/ssl`

   `sudo openssl req -x509 -nodes -days 365 \ -newkey rsa:2048 -keyout ssl.key -out ssl.crt`

3. This will prompt you to enter some information about your company and website. Enter the respective details and press Enter for each prompt:
   For example: Country Name: KH, etc.

4. Continue configuring virtual host in existing file:

   `sudo nano /etc/nginx/sites-enable/yourpreviousfilename`

The content should be similar to this:

```
server {
        listen 80;
        listen [::]:80;

        server_name ns.rathpisey.com;

        root /var/www/simpleweb;
        index index.html;

        location / {
                try_files $uri $uri/ =404;
        }
}
server {
        listen 8443 ssl;
        server_name rathpisey.com www.rathpisey.com;

        root /var/www/simpleweb;
        index index.php index.html index.htm;
        ssl on;
        ssl_certificate
        /etc/nginx/ssl/ssl.crt;

        ssl_certificate_key
        /etc/nginx/ssl/ssl.key;
        # if you have received ca-certs.pem from Certification Authority
        #ssl_trusted_certificate /etc/nginx/ssl/example.com/ca-certs.pem;
        ssl_session_cache shared:SSL:10m;
        ssl_session_timeout 5m;
        keepalive_timeout 70;
        ssl_ciphers "HIGH:!aNULL:!MD5 or HIGH:!aNULL:!MD5:!3DES";
        ssl_prefer_server_ciphers on;
        ssl_protocols TLSv1.2 TLSv1.1 TLSv1;
        add_header Strict-Transport-Security "max-age=31536000";
        location / {
                try_files $uri $uri/ /index.php;
        }
}
```