Name: Md Touhidul Islam	Server Technology part 2	Topic: Secure Apache with let's Encrypt on Ubuntu
Date: 05/04/2021		

Step 1: Installing Certbot

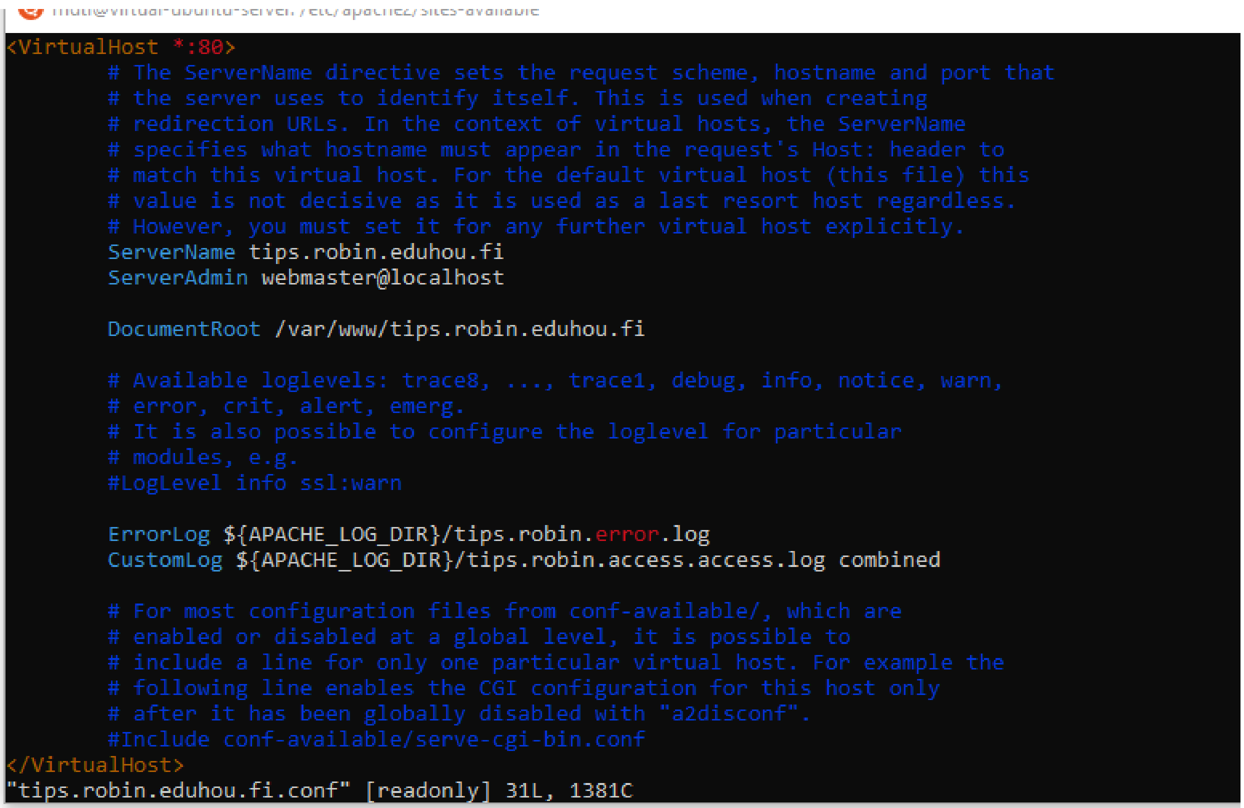
- Command: `sudo apt install certbot python3-certbot-apache`

Step 2: Checking your Apache Virtual Host Configuration

Checked VirtualHost block setup :

- Command: `sudo nano /etc/apache2/sites-available/tips.robin.eduhou.fi.conf`

We have to check ServerName and ServerAlias look like below.

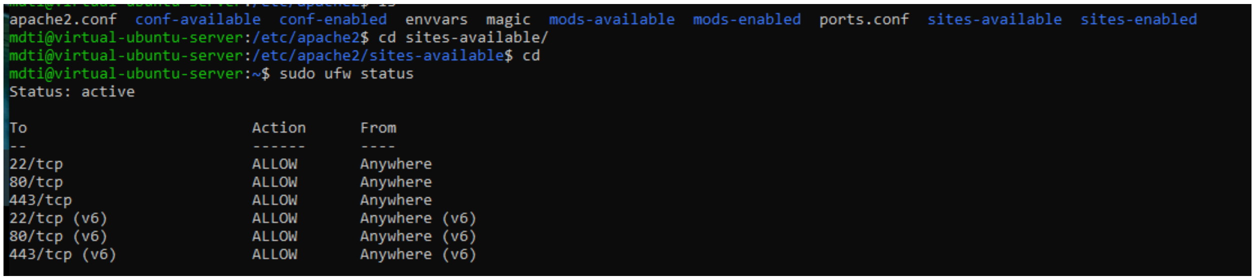


```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        ServerName tips.robin.eduhou.fi
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/tips.robin.eduhou.fi

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/tips.robin.error.log
        CustomLog ${APACHE_LOG_DIR}/tips.robin.access.access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
"tips.robin.eduhou.fi.conf" [readonly] 31L, 1381C
```

Step 3: Allowing HTTPS Through the Firewall

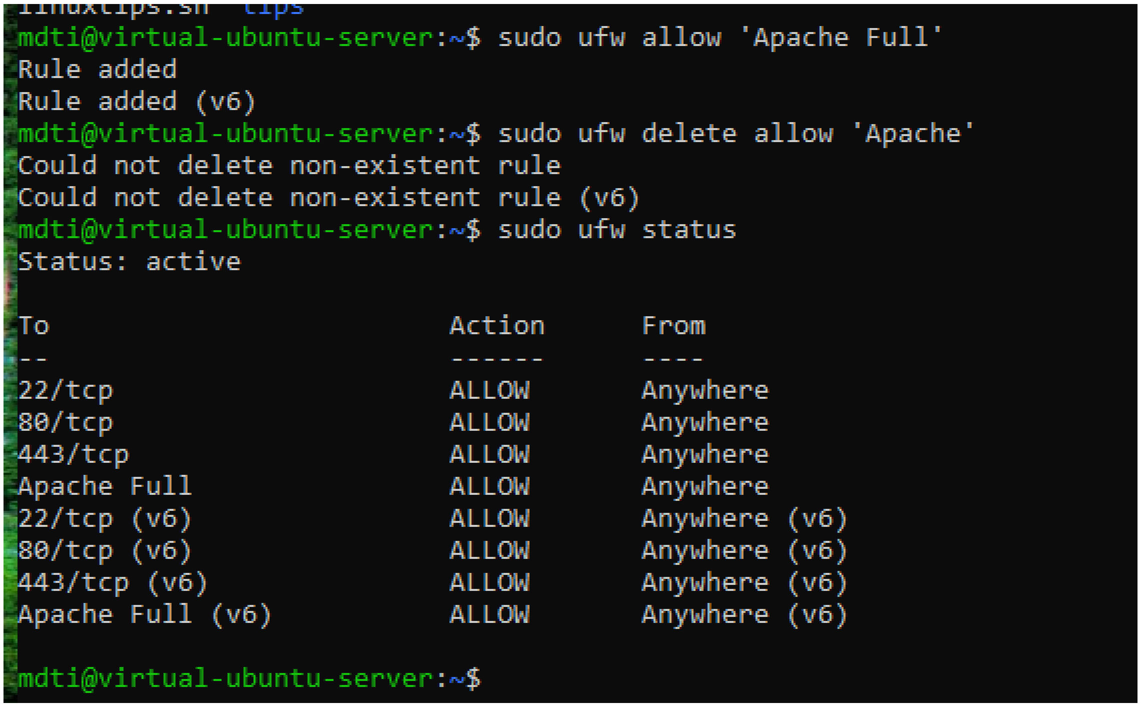
The **Apache Full** profile to allow both HTTP and HTTPS traffic on your server. Verify traffic on server.

- Command: `sudo ufw status`



```
apache2.conf  conf-available  conf-enabled  envvars  magic  mods-available  mods-enabled  ports.conf  sites-available  sites-enabled
mdti@virtual-ubuntu-server:/etc/apache2$ cd sites-available/
mdti@virtual-ubuntu-server:/etc/apache2/sites-available$ cd
mdti@virtual-ubuntu-server:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
```

Apache full allowed

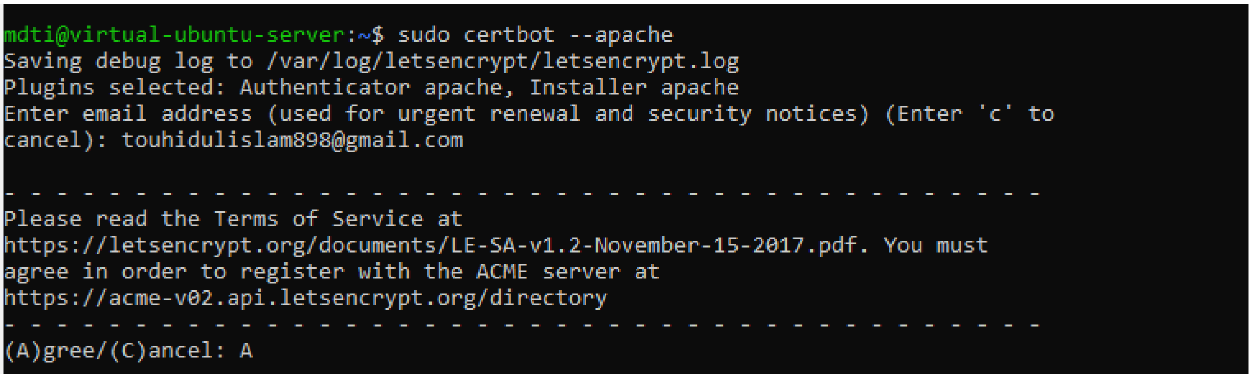


```
linuxtips.sh  tips
mdti@virtual-ubuntu-server:~$ sudo ufw allow 'Apache Full'
Rule added
Rule added (v6)
mdti@virtual-ubuntu-server:~$ sudo ufw delete allow 'Apache'
Could not delete non-existent rule
Could not delete non-existent rule (v6)
mdti@virtual-ubuntu-server:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
Apache Full                ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
Apache Full (v6)           ALLOW       Anywhere (v6)

mdti@virtual-ubuntu-server:~$
```

Step 4: Obtaining an SSL Certificate

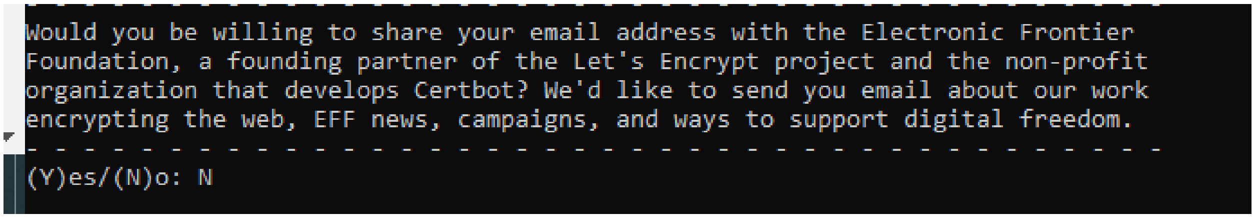
Command: sudo certbot --apache

First will ask for valid e-mail address. This email used for renewal notifications and security notices. And it will ask about terms and condition.



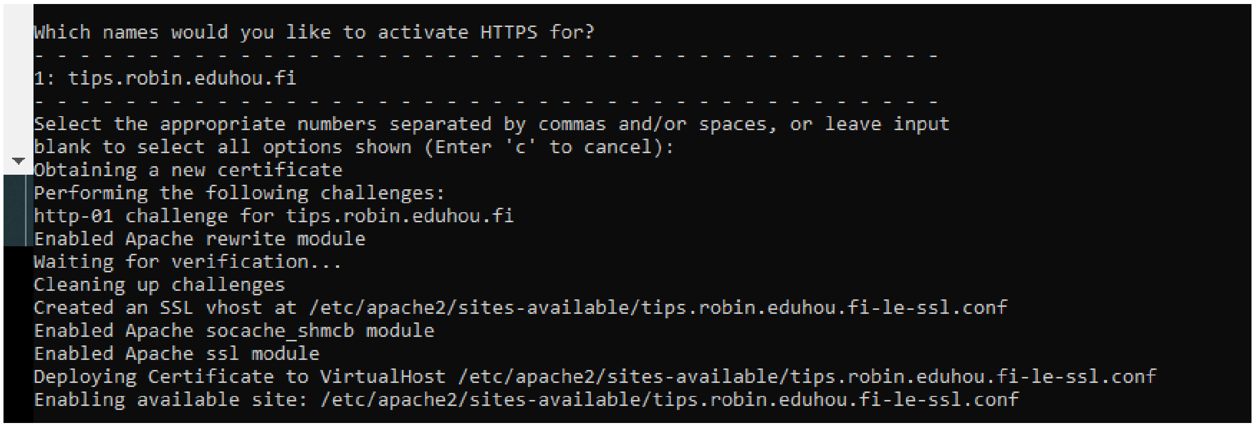
```
mdti@virtual-ubuntu-server:~$ sudo certbot --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): touhidulislam898@gmail.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)ancel: A
```

Next, you'll be asked if you would like to share your email with the Electronic Frontier Foundation to receive news and other information. If you do not want to subscribe to their content, type N. Otherwise, type Y. Then, hit ENTER to proceed to the next step.



```
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: N
```

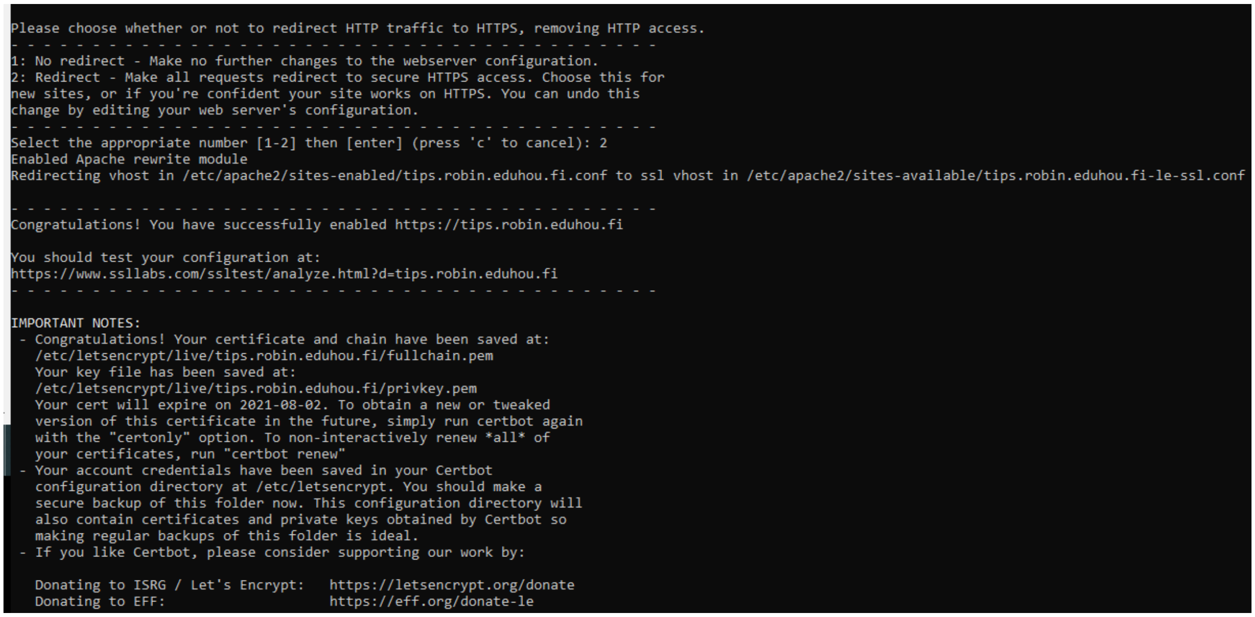
The next step will prompt you to inform Certbot of which domains you'd like to activate HTTPS for. The listed domain names are automatically obtained from your Apache virtual host configuration, that's why it's important to make sure you have the correct `ServerName` and `ServerAlias` settings configured in your virtual host. If you'd like to enable HTTPS for all listed domain names (recommended), you can leave the prompt blank and hit `ENTER` to proceed. Otherwise, select the domains you want to enable HTTPS for by listing each appropriate number, separated by commas and/ or spaces, then hit `ENTER`.



```
Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: tips.robin.eduhou.fi
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel):
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for tips.robin.eduhou.fi
Enabled Apache rewrite module
Waiting for verification...
Cleaning up challenges
Created an SSL vhost at /etc/apache2/sites-available/tips.robin.eduhou.fi-le-ssl.conf
Enabled Apache socache_shmcb module
Enabled Apache ssl module
Deploying Certificate to VirtualHost /etc/apache2/sites-available/tips.robin.eduhou.fi-le-ssl.conf
Enabling available site: /etc/apache2/sites-available/tips.robin.eduhou.fi-le-ssl.conf
```

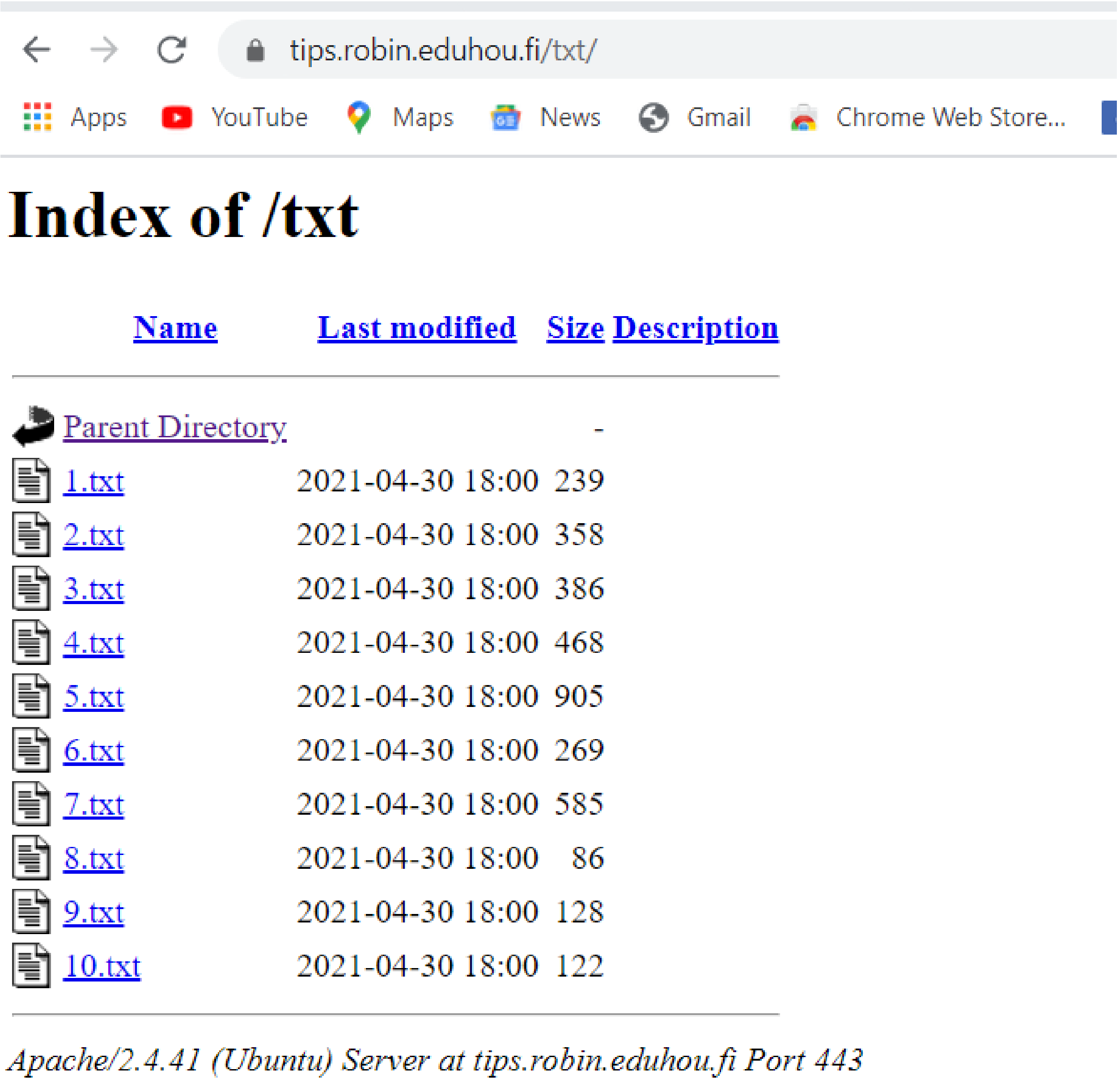
Next, you'll be prompted to select whether or not you want HTTP traffic redirected to HTTPS. In practice, that means when someone visits your website through unencrypted channels (HTTP), they will be automatically redirected to the HTTPS address of your website. Choose `2` to enable the redirection, or `1` if you want to keep both HTTP and HTTPS as separate methods of accessing your website.

After this step, Certbot's configuration is finished, and you will be presented with the final remarks about your new certificate, where to locate the generated files, and how to test your configuration using an external tool that analyzes your certificate's authenticity:



```
Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 2
Enabled Apache rewrite module
Redirecting vhost in /etc/apache2/sites-enabled/tips.robin.eduhou.fi.conf to ssl vhost in /etc/apache2/sites-available/tips.robin.eduhou.fi-le-ssl.conf

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations! You have successfully enabled https://tips.robin.eduhou.fi

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=tips.robin.eduhou.fi
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/tips.robin.eduhou.fi/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/tips.robin.eduhou.fi/privkey.pem
   Your cert will expire on 2021-08-02. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

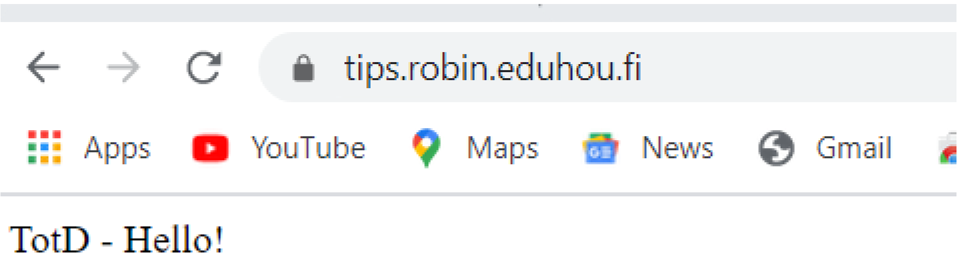
Now my server showing secure sign.



Index of /txt

Name	Last modified	Size	Description
Parent Directory		-	
1.txt	2021-04-30 18:00	239	
2.txt	2021-04-30 18:00	358	
3.txt	2021-04-30 18:00	386	
4.txt	2021-04-30 18:00	468	
5.txt	2021-04-30 18:00	905	
6.txt	2021-04-30 18:00	269	
7.txt	2021-04-30 18:00	585	
8.txt	2021-04-30 18:00	86	
9.txt	2021-04-30 18:00	128	
10.txt	2021-04-30 18:00	122	

Apache/2.4.41 (Ubuntu) Server at tips.robin.eduhou.fi Port 443

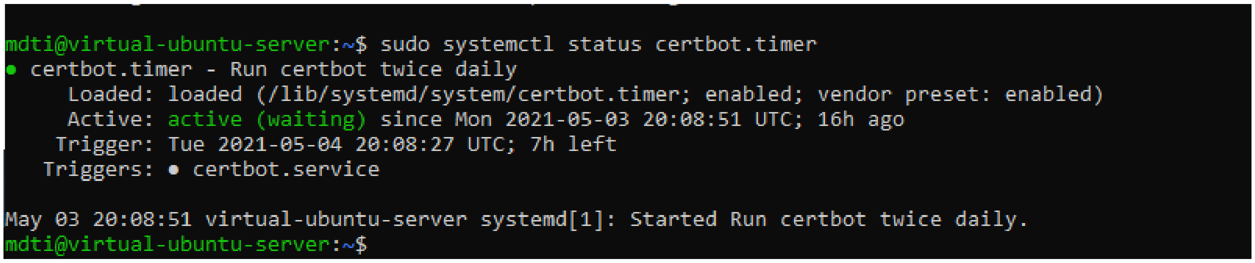


TotD - Hello!

Step 5: Verifying Certbot Auto-Renewal

Let's Encrypt's certificates are only valid for ninety days. This is to encourage users to automate their certificate renewal process, as well as to ensure that misused certificates or stolen keys will expire sooner rather than later. The `certbot` package we installed takes care of renewals by including a renew script to `/etc/cron.d`, which is managed by a `systemctl` service called `certbot.timer`. This script runs twice a day and will automatically renew any certificate that's within thirty days of expiration. To check the status of this service and make sure it's active and running, you can use:

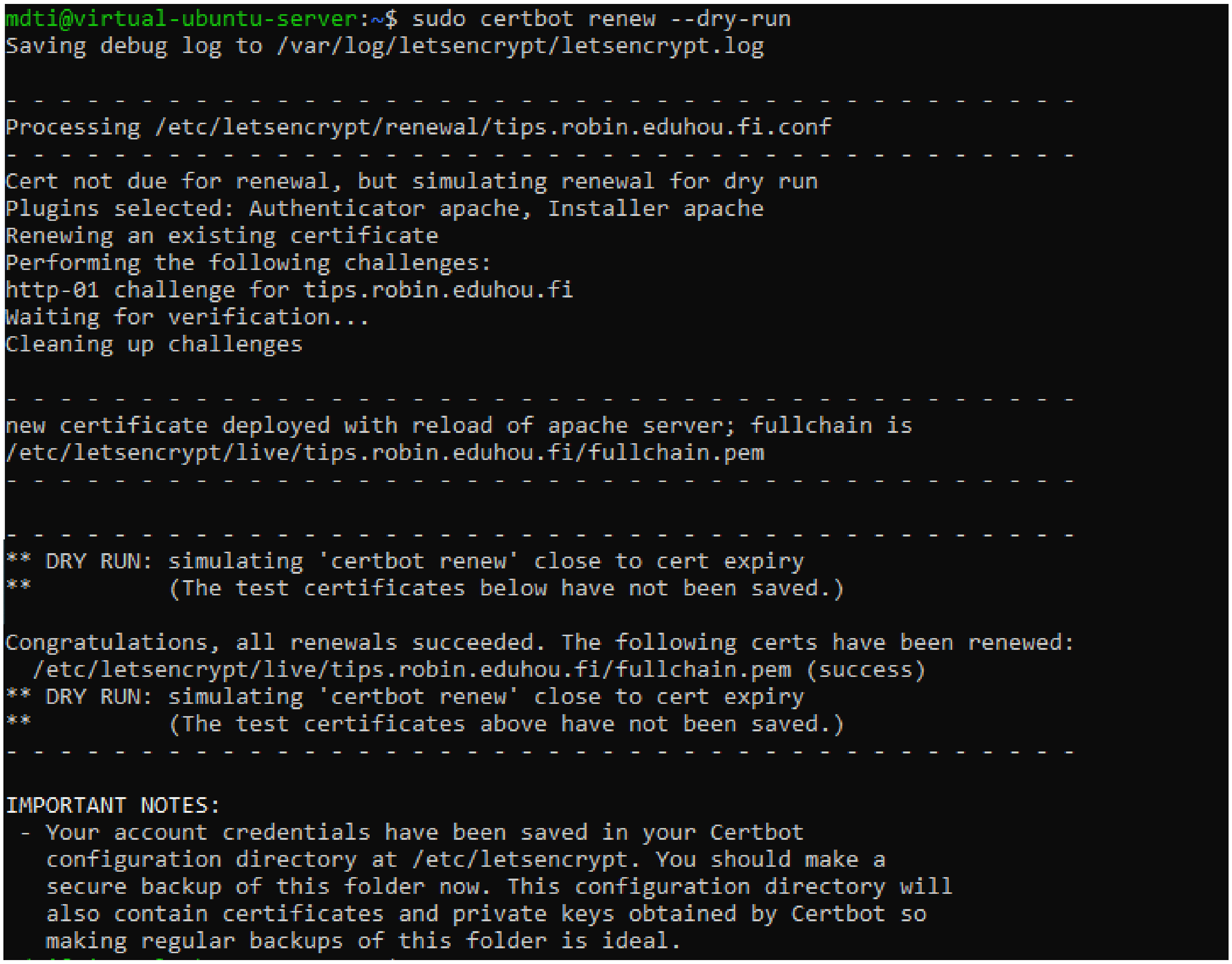
Command: sudo systemctl status certbot.timer



```
mdti@virtual-ubuntu-server:~$ sudo systemctl status certbot.timer
● certbot.timer - Run certbot twice daily
     Loaded: loaded (/lib/systemd/system/certbot.timer; enabled; vendor preset: enabled)
     Active: active (waiting) since Mon 2021-05-03 20:08:51 UTC; 16h ago
    Trigger: Tue 2021-05-04 20:08:27 UTC; 7h left
   Triggers: ● certbot.service

May 03 20:08:51 virtual-ubuntu-server systemd[1]: Started Run certbot twice daily.
mdti@virtual-ubuntu-server:~$
```

To test the renewal process, you can do a dry run with `certbot`:

Everything ok now.



```
mdti@virtual-ubuntu-server:~$ sudo certbot renew --dry-run
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Processing /etc/letsencrypt/renewal/tips.robin.eduhou.fi.conf
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Cert not due for renewal, but simulating renewal for dry run
Plugins selected: Authenticator apache, Installer apache
Renewing an existing certificate
Performing the following challenges:
http-01 challenge for tips.robin.eduhou.fi
Waiting for verification...
Cleaning up challenges

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
new certificate deployed with reload of apache server; fullchain is
/etc/letsencrypt/live/tips.robin.eduhou.fi/fullchain.pem
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -


- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
** DRY RUN: simulating 'certbot renew' close to cert expiry
**          (The test certificates below have not been saved.)

Congratulations, all renewals succeeded. The following certs have been renewed:
  /etc/letsencrypt/live/tips.robin.eduhou.fi/fullchain.pem (success)
** DRY RUN: simulating 'certbot renew' close to cert expiry
**          (The test certificates above have not been saved.)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

IMPORTANT NOTES:
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
```

Thank You