

Homework_Lesson16_Report

Цель: установить и настроить Certbot на своем сервере и затем получить и установить SSL-сертификат для вашего веб-сайта.

Задание:

Шаги:

1. Установите Certbot на свой сервер, используя инструкции, предоставленные на сайте Certbot.
2. Запустите Certbot и запросите новый SSL-сертификат для вашего веб-сайта. Certbot автоматически создаст CSR (запрос на подпись сертификата) и отправит его на подпись.
3. Получите подписанный SSL-сертификат от своего провайдера сертификатов или используйте Certbot для создания самоподписанного сертификата.
4. Установите SSL-сертификат на вашем веб-сервере. Способ установки зависит от конфигурации вашего сервера, но обычно это включает добавление SSL-сертификата в конфигурацию вашего веб-сервера и настройку HTTPS-соединения.
5. Проверьте работу вашего SSL-сертификата, используя браузер. Убедитесь, что ваш веб-сайт открывается по HTTPS и что ваш SSL-сертификат правильно настроен.
6. Настройте автоматическое продление SSL-сертификата с помощью Certbot, чтобы убедиться, что ваш сертификат всегда актуален и не истекает.

Устанавливаем и запускаем nginx.

```
ubuntu@ip-172-31-38-174:~$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: en>
   Active: active (running) since Tue 2024-12-10 08:21:31 UTC; 52s ago
     Docs: man:nginx(8)
  Process: 1863 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_proce>
  Process: 1864 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (c>
 Main PID: 1866 (nginx)
   Tasks: 2 (limit: 1130)
  Memory: 1.7M (peak: 1.9M)
     CPU: 13ms
   CGroup: /system.slice/nginx.service
           └─1866 "nginx: master process /usr/sbin/nginx -g daemon on; master>
             └─1867 "nginx: worker process"

Dec 10 08:21:31 ip-172-31-38-174 systemd[1]: Starting nginx.service - A high pe>
Dec 10 08:21:31 ip-172-31-38-174 systemd[1]: Started nginx.service - A high pe>
lines 1-16/16 (END)
```

Подкинем свою html и проверим что она не защищена.

← → ↻ Не защищено | 35.158.211.111

Information

Levchenko Alexey Viktorovich

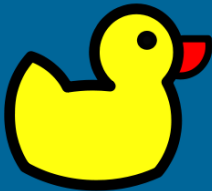
Group: DOS24-onl

Topic: webserver

IP Address: [192.168.1.213:8080](#)

Зайдем на duckdns.org и создадим запись для нашего сайта.

Duck DNS spec about why install faqs logout logged in with alex1436183@gmail.com



Duck DNS


account alex1436183@gmail.com
type free
token d06ce0ae-d8c0-4d60-88ad-df6e6b65d882
token generated 10 minutes ago
created date 10 Dec 2024, 09:02:35

domains 1/5

http:// sub domain .duckdns.org add domain

domain	current ip	ipv6	changed
tms-avl	35.158.211.111 update ip	<input type="text" value="ipv6 address"/> update ipv6	3 minutes ago delete domain

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

[Donate](#) [Bitcoin 16gHnv3NTjpf5ZavMi9QY8FxFUKNchdicUS](#) [patreon](#) 

Устанавливаем Certbot.

```
ubuntu@ip-172-31-38-174:~$ sudo apt install python3-certbot-nginx -y
```

Запустим Certbot для вашего домена

```
ubuntu@ip-172-31-38-174:~$ sudo certbot --nginx --agree-tos --redirect --hsts --staple-ocsp --email alex1436183@gmail.com -d tms-avl.duckdns.org
Saving debug log to /var/log/letsencrypt/letsencrypt.log

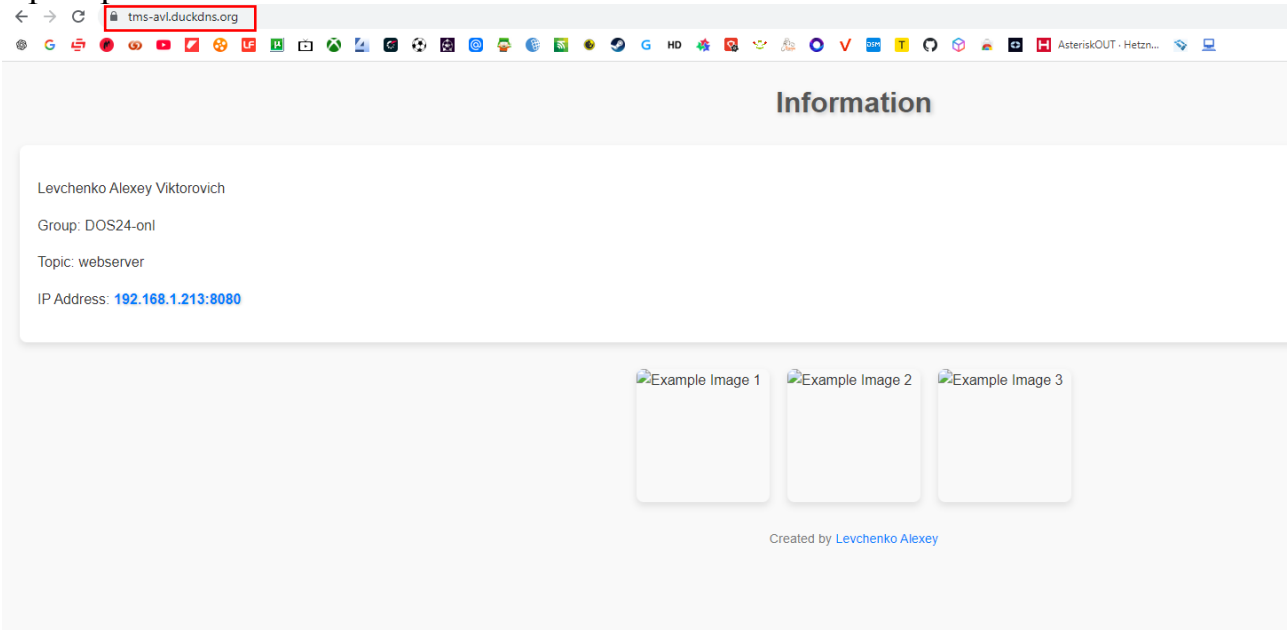
-----
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: y
Account registered.
Requesting a certificate for tms-avl.duckdns.org

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/tms-avl.duckdns.org/fullchain.pem
Key is saved at: /etc/letsencrypt/live/tms-avl.duckdns.org/privkey.pem
This certificate expires on 2025-03-10.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for tms-avl.duckdns.org to /etc/nginx/sites-enabled/default
Congratulations! You have successfully enabled HTTPS on https://tms-avl.duckdns.org

-----
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
-----
ubuntu@ip-172-31-38-174:~$
```

Проверим сайт.



Проверим сертификат.



Для автоматического продления сертификатов добавим в cron команду что бы она выполнялась каждый понедельник.

0 0 * * 1 certbot renew --quiet