IN3210/4210 Exercise 5 - TLS

This exercise continues exercise 4. Use again the SEED PKI lab found here: https://seedsecuritylabs.org/Labs_16.04/PDF/Crypto_PKI.pdf

1. Perform the following tasks from the lab:
   - 2.4 Task 4: Deploying Certificate in an Apache-Based HTTPS Website

2. Install the tool *testssl*:

```
sudo apt install testssl.sh
```

3. Use *testssl* to test your HTTPS Webserver. Which weaknesses are detected?

4. Modify the configuration of your Apache Web server in the following way:
   a. *testssl* does not show any red errors anymore (except for the issuer)
   b. only "secure" TLS versions are use
   c. only symmetric encryption with GCM mode is used