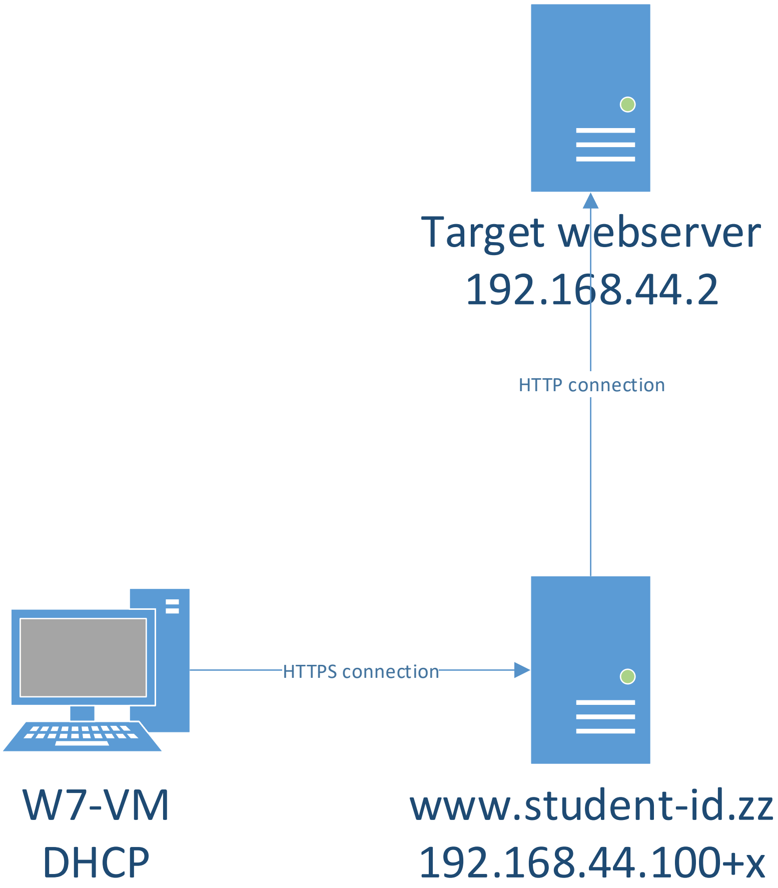
Lab3 – TLS Hardening

You can use this lab manual for your personal documentation. Use screenshots for your own documentation, there will be questions later on that may point to this lab manual. Take care to check if you need to collect some information from the lab for the answers.

\ at the end of the line is used to mark that the command needs to be on one line. Replace **student-id** with your own student-id and **x** or **y** as your VMs correct IP in the labs.

The labs use the following topology:



All VMs in this lab are in VirtualBox ***Bridged*** network. The machines that have static IP need to have an offset, check the topology image for reference. USE YOUR WIN7 WORKSTATION IP ADDRESS AS **x**.

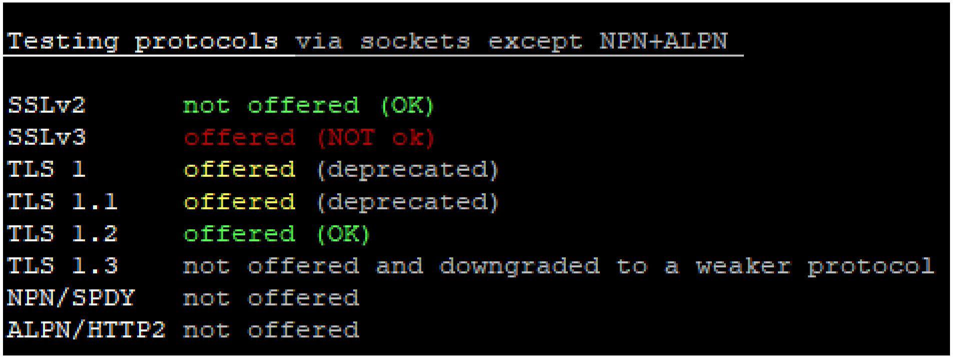
All templates for VMs can be found in \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\

- ### TestSSL.sh

Before and after hardening, check results with testssl.sh (https://testssl.sh/). Download it to the proxy server and run against localhost:

```
yum install git
git clone --depth 1 https://github.com/drwetter/testssl.sh.git
cd testssl.sh
./testssl.sh https://www.student-id.zz/
```

Take note of at least the lines printed in RED and ORANGE, as they are critical. These should be mitigated.



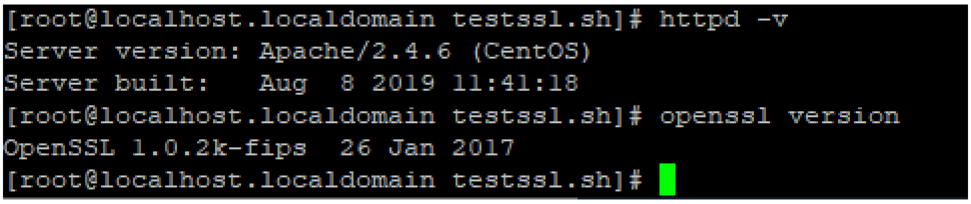
```
Testing protocols via sockets except NPN+ALPN

SSLv2      not offered (OK)
SSLv3      offered (NOT ok)
TLS 1      offered (deprecated)
TLS 1.1    offered (deprecated)
TLS 1.2    offered (OK)
TLS 1.3    not offered and downgraded to a weaker protocol
NPN/SPDY   not offered
ALPN/HTTP2 not offered
```

- ### Mozilla TLS

Mozilla has a nice TLS configuration generator in https://mozilla.github.io/server-side-tls/ssl-config-generator/

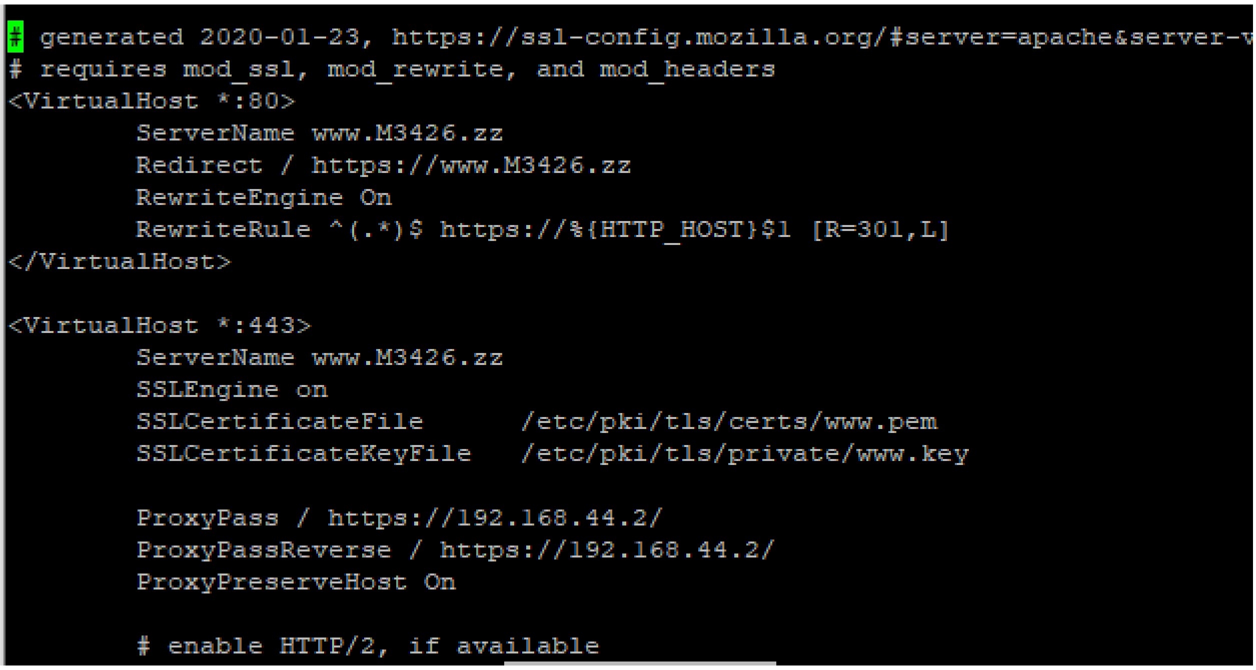
Find out from your server:

- Your Apache version
- Your OpenSSL library version

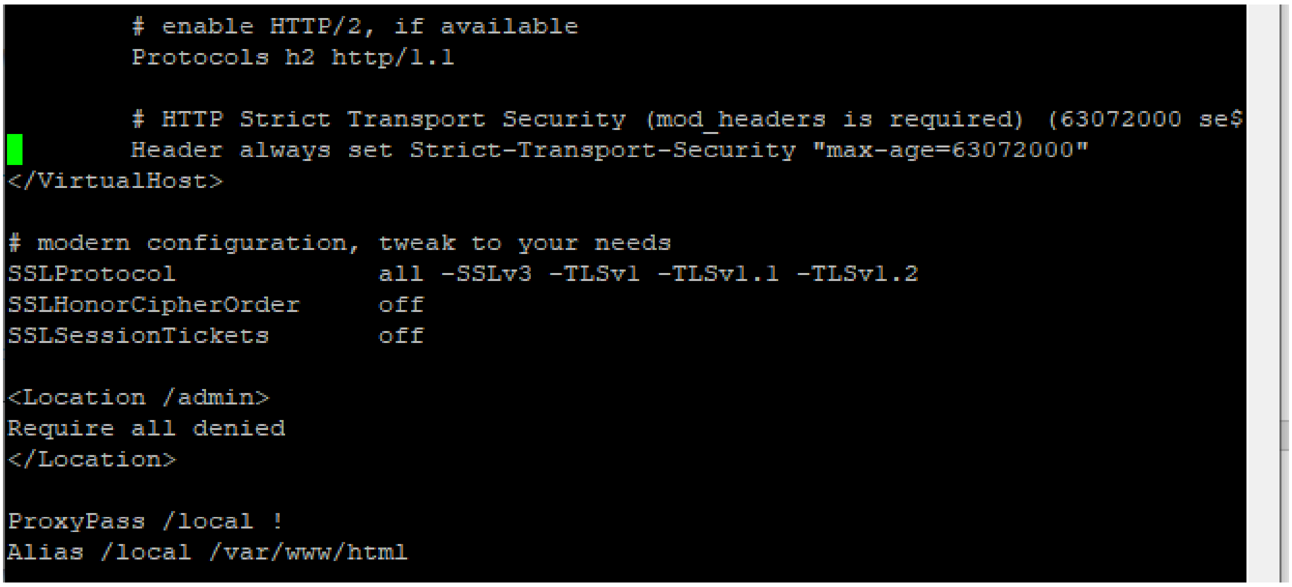


```
[root@localhost.localdomain testssl.sh]# httpd -v
Server version: Apache/2.4.6 (CentOS)
Server built:   Aug  8 2019 11:41:18
[root@localhost.localdomain testssl.sh]# openssl version
OpenSSL 1.0.2k-fips  26 Jan 2017
[root@localhost.localdomain testssl.sh]#
```

Using the Mozilla Generator, generate configuration for the server. Add this to your proxy.conf. Do not add OCSP configurations as we don’t have a valid OCSP Responder for the CA Certificate.

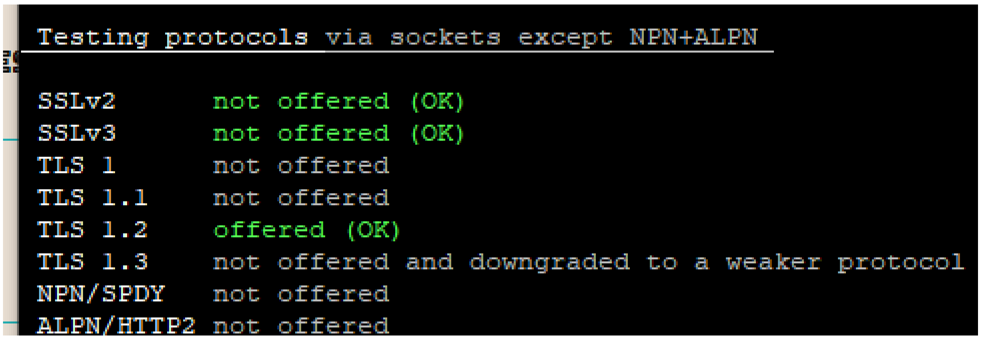


```
# generated 2020-01-23, https://ssl-config.mozilla.org/#server=apache&server-v
# requires mod_ssl, mod_rewrite, and mod_headers
<VirtualHost *:80>
        ServerName www.M3426.zz
        Redirect / https://www.M3426.zz
        RewriteEngine On
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]
</VirtualHost>

<VirtualHost *:443>
        ServerName www.M3426.zz
        SSLEngine on
        SSLCertificateFile      /etc/pki/tls/certs/www.pem
        SSLCertificateKeyFile   /etc/pki/tls/private/www.key

        ProxyPass / https://192.168.44.2/
        ProxyPassReverse / https://192.168.44.2/
        ProxyPreserveHost On

        # enable HTTP/2, if available
```



```
        # enable HTTP/2, if available
        Protocols h2 http/1.1

        # HTTP Strict Transport Security (mod_headers is required) (63072000 se$
        Header always set Strict-Transport-Security "max-age=63072000"
</VirtualHost>

# modern configuration, tweak to your needs
SSLProtocol             all -SSLv3 -TLSv1 -TLSv1.1 -TLSv1.2
SSLHonorCipherOrder     off
SSLSessionTickets       off

<Location /admin>
Require all denied
</Location>

ProxyPass /local !
Alias /local /var/www/html
```

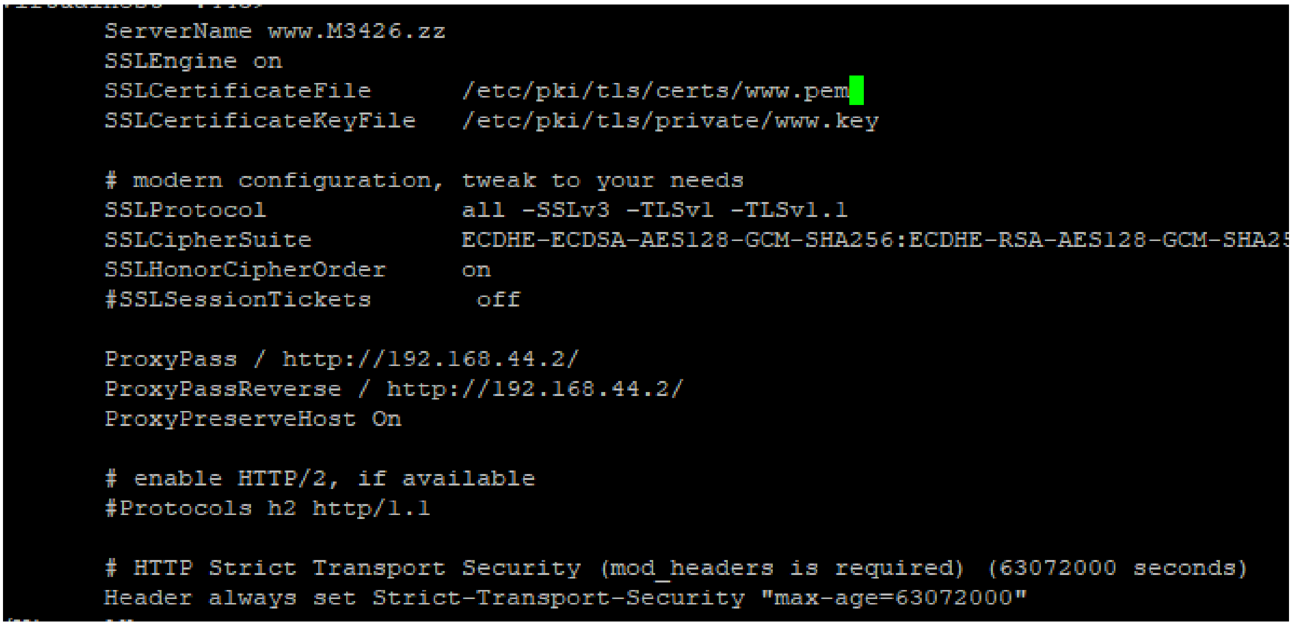
After configuring these, check again with testssl.sh



```
 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    not offered and downgraded to a weaker protocol
 NPN/SPDY   not offered
 ALPN/HTTP2 not offered
```

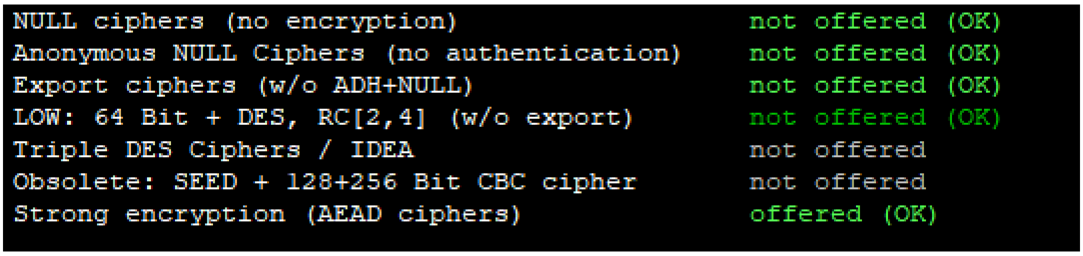
- **Extra hardening**

If critical errors still occur when testing with testssl.sh, try to find out the causes for them and mitigate. These may vary depending on the current changes in updates, new vulnerabilities, etc. If unsure, ask the teacher.

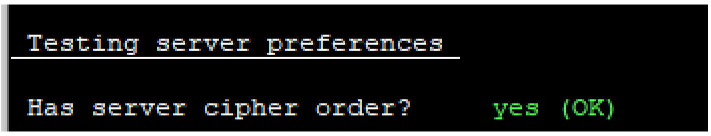


```
        ServerName www.M3426.zz
        SSLEngine on
        SSLCertificateFile      /etc/pki/tls/certs/www.pem
        SSLCertificateKeyFile   /etc/pki/tls/private/www.key

        # modern configuration, tweak to your needs
        SSLProtocol             all -SSLv3 -TLSv1 -TLSv1.1
        SSLCipherSuite          ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA2
        SSLHonorCipherOrder     on
        #SSLSessionTickets       off

        ProxyPass / http://192.168.44.2/
        ProxyPassReverse / http://192.168.44.2/
        ProxyPreserveHost On

        # enable HTTP/2, if available
        #Protocols h2 http/1.1

        # HTTP Strict Transport Security (mod_headers is required) (63072000 seconds)
        Header always set Strict-Transport-Security "max-age=63072000"
```

muutama muokkaus ja näyttää vihreää



```
 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4] (w/o export)           not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsolete: SEED + 128+256 Bit CBC cipher           not offered
 Strong encryption (AEAD ciphers)                  offered (OK)
```



```
 Testing server preferences

 Has server cipher order?     yes (OK)
```