Transport Layer Security: Lab

Christian Grothoff

14.05.2018

1 TLS lab

Obtain a TLS certificate via the "Let's encrypt" CA (you need a global DNS name!):

```
# letsencrypt -D DOMAIN.TLD --standalone certonly  # or
# letsencrypt -D DOMAIN.TLD --standalone run # may work
```

2 Configure your Apache server to use it

Edit `/etc/apache/sites-enabled/SITE.conf` to contain:

```
SSLEngine on
SSLProtocol -ALL +TLSv1.2 +TLSv1.1 +TLSv1
SSLCertificateKeyFile /etc/letsencrypt/live/example.com/privkey.pem
SSLCertificateChainFile /etc/letsencrypt/live/example.com/fullchain.pem
SSLCertificateFile /etc/letsencrypt/live/example.com/cert.pem
```

3 Check it

Verify your configuration using `https://www.ssllabs.com/ssltest/` and `https://observatory.mozilla.org/`.

4 Other services (optional)

Try to secure DNS, IMAP and SMTP with TLS as well.