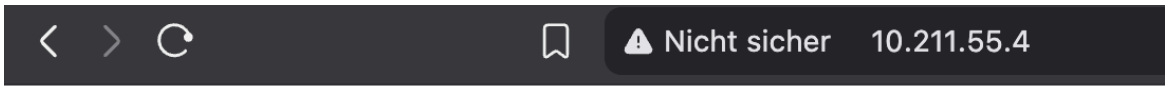
Netzwerksicherheit

Aufgabe 2

Julian Bertol

15. April 2025

Zu beginn habe ich den apache Server aufgesetzt und das gegebene Script in eine JS-Datei geschrieben. Nun wird auf der Webseite folgendes angezeigt:



TLS not used

Ich werde diese Aufgabe mit easy-rsa durchführen.

Schritt für Schritt Anleitung für das ausstellen eines Zertifikats:
Zuerst in den Ordner /usr/share/easy-rsa/ navigieren.

Dann PKI initialisieren:
./easyrsa init-pki

Nun kann ich ein CA (Certificate Authority) erstellen
Dies geht mit dem befehl:
./easyrsa build-ca

Nun muss ich ein Password und ein Common Name vergeben

Nun muss ich den private key erstellen (CSR):
./easyrsa gen-req 127.0.0.1 nopass
Mit nopass geht das ganze ohne passwort

Jetzt muss ich noch den CSR mit der CA signieren

Jetzt muss man dem Webserver mitteilen wo die generierten Dateien liegen. Das geht mit einer conf Datei die bei mir wie folgt aussieht:

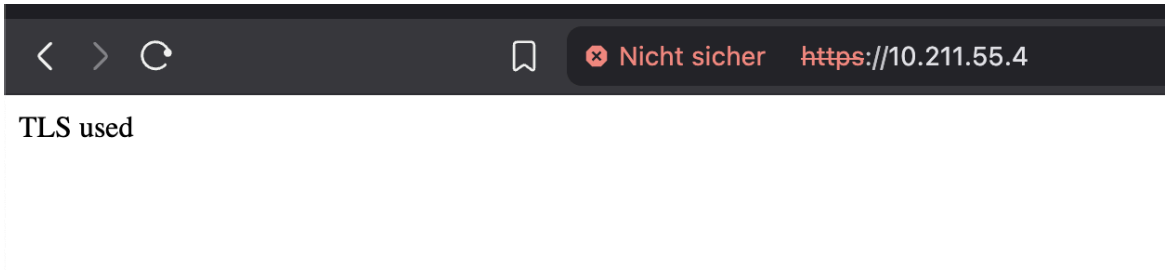
```
<VirtualHost *:443>
    ServerName 127.0.0.1
    DocumentRoot /var/www/html

    SSLEngine on
    SSLCertificateFile      /usr/share/easy-rsa/pki/issued/127.0.0.1.crt
    SSLCertificateKeyFile   /usr/share/easy-rsa/pki/private/127.0.0.1.key
    SSLCertificateChainFile /usr/share/easy-rsa/pki/ca.crt

    <Directory /var/www/html>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/127.0.0.1-ssl-error.log
    CustomLog ${APACHE_LOG_DIR}/127.0.0.1-ssl-access.log combined
</VirtualHost>
```

Diese Datei habe ich unter /etc/apache2/sites-available/127.0.0.1-ssl.conf abgelegt.



Was ist der Unterschied zwischen und HTTP und HTTPS beim Übertragen der Webseiteninhalte?

- bei HTTP werden die Daten unverschlüsselt übertragen während bei HTTPS die Daten verschlüsselt übertragen werden. Außerdem nutzen beide einen anderen Port.

Warum wird die Webseite immer noch als „Nicht sicher“ angezeigt?

Weil ich diesem Zertifikat nicht vertraue.

43	63.710958864	10.211.55.4	10.211.55.2	TLSv1.3	537 Application Data
44	63.711146072	10.211.55.2	10.211.55.4	TCP	66 53463 → 443 [ACK] Seq=2967 Ack=3489 Win=130624 Len=0 TSval=23…
45	63.813242864	10.211.55.2	10.211.55.4	SSH	150 Client: Encrypted packet (len=84)
46	63.813307739	10.211.55.4	10.211.55.2	TCP	66 22 → 53363 [ACK] Seq=2221 Ack=1801 Win=8884 Len=0 TSval=33709…
47	63.817387614	10.211.55.2	10.211.55.4	SSH	150 Client: Encrypted packet (len=84)
48	63.817414364	10.211.55.4	10.211.55.2	TCP	66 22 → 53363 [ACK] Seq=2221 Ack=1885 Win=8884 Len=0 TSval=33709…
49	65.030826323	10.211.55.4	10.211.55.2	SSH	150 Server: Encrypted packet (len=84)
50	65.031335489	10.211.55.2	10.211.55.4	TCP	66 53363 → 22 [ACK] Seq=1885 Ack=2305 Win=3586 Len=0 TSval=12080…
51	65.377703448	10.211.55.4	10.211.55.2	SSH	150 Server: Encrypted packet (len=84)
52	65.377998573	10.211.55.2	10.211.55.4	TCP	66 53363 → 22 [ACK] Seq=1885 Ack=2389 Win=3586 Len=0 TSval=12080…
53	68.712397408	10.211.55.4	10.211.55.2	TLSv1.3	90 Application Data
54	68.712540449	10.211.55.4	10.211.55.2	TCP	66 443 → 53463 [FIN, ACK] Seq=3513 Ack=2967 Win=62336 Len=0 TSva…
55	68.712848824	10.211.55.2	10.211.55.4	TCP	66 53463 → 443 [ACK] Seq=2967 Ack=3513 Win=131072 Len=0 TSval=23…
56	68.712849241	10.211.55.2	10.211.55.4	TCP	66 53463 → 443 [ACK] Seq=2967 Ack=3514 Win=131072 Len=0 TSval=23…
57	69.605397450	10.211.55.2	10.211.55.4	TCP	54 53463 → 443 [RST, ACK] Seq=2967 Ack=3514 Win=131072 Len=0

Wie man hier sehen kann ich die Übertragung jetzt verschlüsselt.