Lab Assignment 6

1. Implement SSL/TLS certificates on a website to ensure secure communication between the server and the client.

With Real Website:

Step: 1 A Linux server such as Apache or Nginx with root or sudo access.

sudo apt install apache2 -y **or** sudo apt install nginx -y

Step: 2 Update your server.

```
sudo apt update && sudo apt upgrade -y
```

Step: 3 Install Certbot

Certbot is a tool to get free SSL certificates from Let's Encrypt.

- For Apache:

```
sudo apt install certbot python3-certbot-apache -y
```

- For Nginx:

```
sudo apt install certbot python3-certbot-nginx -y
```

Step: 4 Get the SSL Certificate

Replace study.com with your domain.

- For Apache:

```
sudo certbot --apache -d study.com -d www.study.com
```

- For Nginx:

```
sudo certbot --nginx -d study.com -d www.study.com
```

Certbot will ask for email and agree to terms. It will then automatically configure HTTPS.

Step: 5 Verify HTTPS

Open your browser and go to:

https://study.com

You should see the padlock icon in the address bar.

Step: 6 Test Auto-Renewal

Let's Encrypt certificates expire every 90 days. Auto-renewal is typically enabled by default.

Test it with:

```
sudo certbot renew --dry-run
```

Step: 7 Force HTTPS(Optional)

If not automatically done, redirect all HTTP traffic to HTTPS.

- For Apache:

In your virtual host file (/etc/apache2/sites-available/000-default.conf), add:

```
<VirtualHost *:80>
   ServerName example.com
   Redirect permanent / https://study.com/
</VirtualHost>
```

Then reload Apache:

```
sudo systemctl reload apache2
```

With Local Server

Step: 1 Install Apache Web Server

Run the following command in the terminal:

```
sudo apt install apache2 -y
```

Step: 2 Generate a Self-Signed Certificate

Run the following command to create a self-signed SSL certificate and private key:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -
keyout/etc/ssl/private/selfsigned.key -out /etc/ssl/certs/selfsigned.crt
```

Step: 3 Enable SSL Module and Default SSL Site

Execute the following commands:

```
sudo a2enmod ssl
sudo a2ensite default-ssl.conf
```

Step: 4 Configure Apache to Use SSL Certificate

Edit the default SSL virtual host configuration file:

```
sudo nano /etc/apache2/sites-available/default-ssl.conf
```

Update the following lines to match the paths to your certificate and key:

```
SSLCertificateFile /etc/ssl/certs/selfsigned.crt
SSLCertificateKeyFile /etc/ssl/private/selfsigned.key
```

Step: 5 Restart Apache

Apply the changes by restarting Apache:

```
sudo systemctl restart apache2
```

Step: 6 Test HTTPS on Localhost

Open a browser and navigate to: https://localhost

You will see a warning about the certificate being untrusted. This is expected for a self-signed certificate.