Public Key Infrastructure

The goal of this assignment is to understand why unencrypted HTTP is not secure and how HTTPS addresses some of the vulnerabilities of HTTP. To this end, complete the following tasks and answer the accompanying questions.

Tasks

1. **Host a local web server**

There are many services for this. If you've done this before, you're free to use the service/software that you're comfortable with. If you're feeling adventurous, try setting up an nginx or Apache. Both are used extensively in enterprise and professional settings. Another option is to use Python's HTTP server class

2. **Identify why HTTP is not secure**

(spoiler: it is unencrypted). In your write-up, explain how an eavesdropper can "sniff" web traffic between a client and HTTP server to see what is being communicated (including which resources are being fetched and the contents of the resources). In addition, use Wireshark to capture network traffic between your local web server and a local client**.** Feel free to include screenshots from Wireshark in your explanation.

3. **Create a self-signed certificate and upgrade your web server to HTTPS**

(a) Why can't you obtain an SSL certificate for your local web server from a certificate authority?

Generate an SSL certificate for your web server, add the certificate to your list of locally trusted roots, and restart the web server with the certificate. All communications with your server should now be secured. Once again, include a network trace (captured using Wireshark) and comment on the difference between the contents of HTTP and HTTPS (TLS) traffic.

Submission Instructions

Your submission should include:

1. a write-up that documents how you did each task and answers any questions
2. a packet trace of HTTP traffic
3. a packet trace of HTTPS traffic

Please submit a zip file that contains these three files.