HW #7 - Security

Team: Four Guys++

Members: Hongru Lin

Bryan Caldera

Devi Priya Ravi

Monish Murali

Problem Statement

* Design and build a PKI infrastructure that includes Root CA, Signing CA, and TLS Certificate
* Use the TLS certificate to install a web server, e.g., tomcat

Implementation

Step 1:

Git clone <https://bitbucket.org/stefanholek/pki-example-1>

Implemented the below steps based on the instructions in <https://pki-tutorial.readthedocs.io/en/latest/simple/>

Step 2:

Creating directories and database

Text

Description automatically generated

Create CA request:

Text

Description automatically generated

Create CA certificate

Text

Description automatically generated

Create Database

Text

Description automatically generated

Create CA request

Text

Description automatically generated

Create CA certificate :

Text

Description automatically generated

Create email request and Email certificate

Text

Description automatically generated

Create TLS server request:

Text

Description automatically generated

Revoke certificate

Text

Description automatically generated

Create PKCS#7 bundle

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

View Results View Request :

Text

Description automatically generated

View Certificate:

Text

Description automatically generated

Create a new JKS store for TOMCAT:

Text

Description automatically generated

Generate a new CSR for tomcat :

Text

Description automatically generated

Sign the certificate for TOMCAT using the root:

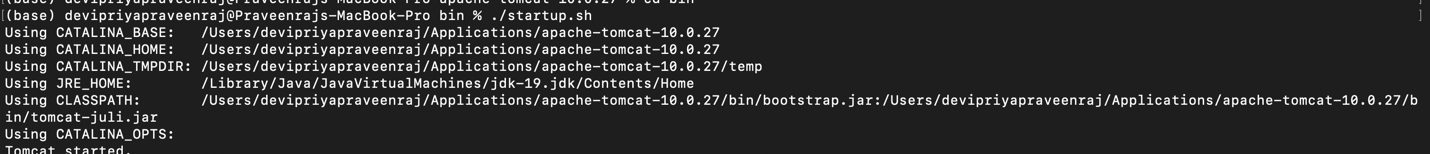


Import root certificate and tomcat certificate

Text

Description automatically generated

Edit the server.xml with the created key store and start the tomcat server.



The TOMCAT server is running with TSL/SSL enabled on port 8443:

Graphical user interface

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence