**HW-7-SECURITY**

**Questions**:

Design and build a PKI infrastructure that includes Root CA, Signing CA, and TLS Certificate,

E.g., as described here: [http Links to an external site.://pki-tutorial.readthedocs.io/en/latest/simple Links to an external site./Links to an external site.](http://pki-tutorial.readthedocs.io/en/latest/simple/)

Use the TLS certificate to install a web server, e.g. tomcat, [https:// Links to an external site.tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html](https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html)

**Group Name: 4musks**

**Team members:**

* Utsav Rawat
* Nihal Kaul
* Jaya Krishna Thupili

**Answer:**

Step 1: Clone the github repository <https://bitbucket.org/stefanholek/pki-example-1>. Proceed with the instructions given in: <https://pki-tutorial.readthedocs.io/en/latest/simple/> to construct the PKI.

Text

Description automatically generated

Step 2: Configure Root CA

* 1. Configure Directories type, below mentioned commands:

The ‘ca’ directory holds CA resources, the ‘crl’ directory holds CRLs, and the ‘certs’ directory holds user certificates

Text

Description automatically generated

* 1. Configure Database, type below mentioned commands:

Text

Description automatically generated

* 1. Create CA Request



* 1. Create CA Certificate

Text

Description automatically generated

Step 3: Create Signing CA

3.1 Create Directories

Text

Description automatically generated

3.2 Create Database

Text

Description automatically generated with medium confidence

3.3 Create CA Request

A picture containing text

Description automatically generated

3.4 Create CA Certificate

Text

Description automatically generated

Step 4: Operate Signing CA

4.1 Create email Request

A picture containing text

Description automatically generated

4.2 Create email Certificate

Text

Description automatically generated

4.3 Create TLS Server Request

Text

Description automatically generated

4.4 Create TLS Service Certificate

Text

Description automatically generated

4.5 Create CRL

Text

Description automatically generated

Step 5: Output Formats

5.1 Create DER Certificate

Text

Description automatically generated

5.2 Create DER CRL

Text

Description automatically generated

5.3 Create PKCS#7

Text

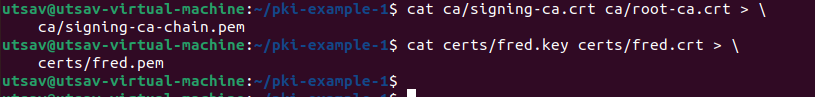
Description automatically generated

5.4 Create PKCS#12

Text

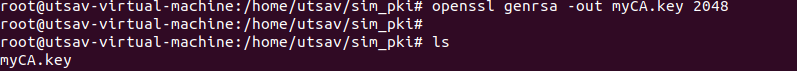
Description automatically generated

5.5 Create PEM Bundle



Step 6: Install the web server Tomcat through link: <https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html>

Follow the Below commands:

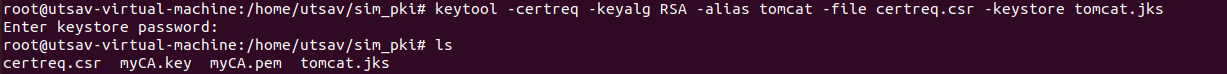


Text

Description automatically generated

Text

Description automatically generated



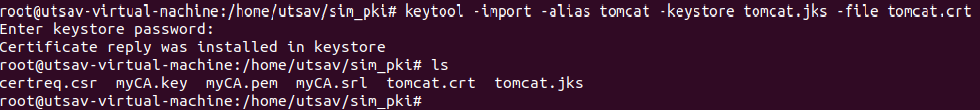
Using the root certificate, Sign the certificate for Tomcat:



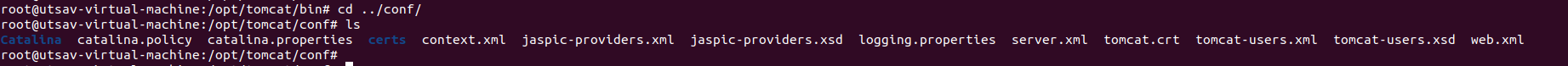
Import Tomcat certificate and Root certificate:

Text

Description automatically generated



Copy the ‘certs’ folder to /opt/tomcat/conf folder

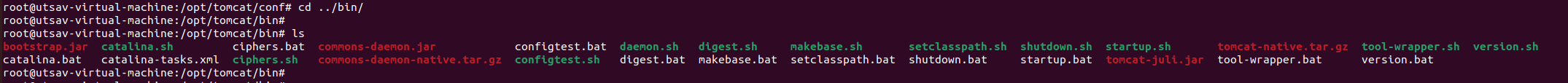


Update server.xml for the Tomcat Connector

Text

Description automatically generated

Start-Up Tomcat



**Validate TLS**

Graphical user interface, text, application

Description automatically generated