**HW#7 Application Security**

**Group Name:** Hurley Guys

Github Link: <https://github.com/artikShetty/Homework-7>

Creating a PKI Infrastructure (Signing- CA, Root-CA, and TLS certificate)

Following are the steps to create this:

1. First create the directories for the host certificates and crls which are required. We can name it as “crl” and “cert” respectively. The commands are shown in the following snapshots.

A close up of a screen

Description automatically generated

A screenshot of a cell phone screen with text

Description automatically generated

1. Now create separate folders for databases and storing the “root-ca” which is our key. The commands to do this and expected results are shown in following snapshot.

A close up of a keyboard

Description automatically generated

A screenshot of a cell phone screen with text

Description automatically generated

1. After creating the separate folders, we have to create a private key and request for the root-CA. While doing this it will ask for the PE pass phrase which is “.key”. The commands to do this and expected results are shown in following snapshot.

A screenshot of a cell phone

Description automatically generated

1. Now in this step the CA create and updates the certificate of self in the database. The commands to do this and expected results are shown in following snapshot.

A screenshot of text

Description automatically generated

A screen shot of a social media post

Description automatically generated

1. Now it’s time to create a signing CA authority. The commands to do this and expected results are shown in following snapshot.

A picture containing object

Description automatically generated

Screen of a cell phone

Description automatically generated

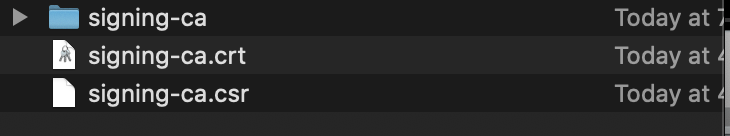
1. A close up of a sign

   Description automatically generatedIn this step we have to create a database for storing all certificates. The commands to do this and expected results are shown in following snapshot.A screenshot of a cell phone

   Description automatically generated
2. Now we have to create a request for the signing CA. The commands to do this and expected results are shown in following snapshot.

A screenshot of a cell phone

Description automatically generated



1. Now, in order to get the signing CA certificate form the root-CA we have to use the root CA private key. The commands to do this and expected results are shown in following snapshot.

A screenshot of a cell phone screen with text

Description automatically generated

A screenshot of a cell phone

Description automatically generated

1. Now its time to create a TLS-service request using following commands.

A screenshot of text

Description automatically generated

1. After creating the TLS-service request we have to create a TLS-service certificate.

A screenshot of a cell phone

Description automatically generated

