CS4600 Homework 5 – Public Key Infrastructure

Task 1: Becoming CA authority

1. Set up directory and files as mentioned

Text

Description automatically generated

Task 2: Create a Certificate for SEEDPKLab2020.com

1. Generate self-signed certificate for CA. PEM passphrase - Ucla

A picture containing chart

Description automatically generated

1. Generate keys

Text

Description automatically generated

Text

Description automatically generated

1. Generate certificate signing request

Text

Description automatically generated

1. Generate certificate

Text

Description automatically generated

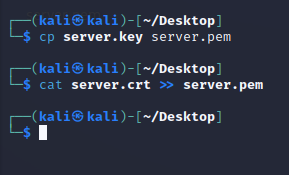
Task 3: Deploy Certificate in HTTPS Web Server

1. Configure DNS through vi/etc/host

Graphical user interface, text

Description automatically generated

1. Combine secret key and certificate into permission file



Text

Description automatically generated

1. Configure browser to accept CA certificate

Graphical user interface, text, application

Description automatically generated

1. When 1 bit is changed in server.pem, website can’t launch

Text

Description automatically generated

1. Connection to <https://localhost:4433> leads to the same website

Graphical user interface, text, application

Description automatically generated

Note: this is done on a Kali VM and may not have the “secured” padlock if it was done on the same SeedLab VM specifically configured.

Task 4: Deploying Certificate in an Apache-based HTTPS Website

1. First, copy server certificate and key and move it to /etc/apache2/ssl

Text

Description automatically generated

Text

Description automatically generated

1. Add the following section to /etc/apache2/default-ssl.conf

Text

Description automatically generated

1. Configure html file for “Hello World” and successful browse below

Graphical user interface, application

Description automatically generated