**FORMAN CHRISTIAN COLLEGE (A CHARTERED UNIVERSITY)**

****

**Comp 421**

**Fall 2024**

**Assignment 2**

**Information security**

**Hajra Mujahid 251707426**

Demonstration of Public Key Infrastructure (PKI) using OpenSSL

**Objective**

To demonstrate the use of Public Key Infrastructure (PKI) by completing the following tasks using the OpenSSL tool:

1. Generate a private and public key.

2. Generate a Certificate Signing Request (CSR).

3. Create a self-signed certificate.

4. Act as a Certification Authority (CA) to issue certificates.

Steps and Commands

**Checking if openssl is installed in Kali**

****

**1. Generate a Private and Public Key**

**Command:**



**Description:**

This command generates a 2048-bit RSA private key and saves it in the file private.key.

**Output:**

File created: private.key

**Verification:**

Display the contents of the private key:

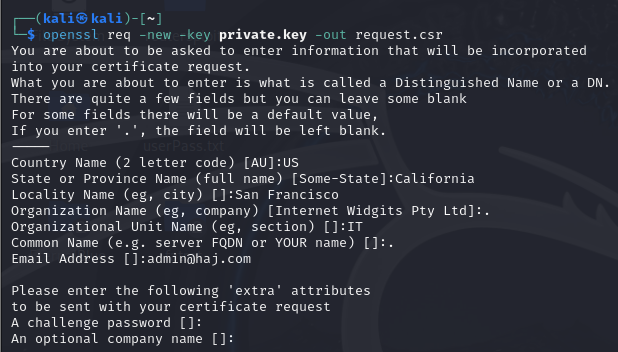


The file should begin with:

-----BEGIN RSA PRIVATE KEY-----

**2. Generate a Certificate Signing Request (CSR)**

**Command:**



**Description:**

This command generates a CSR using the private key private.key.

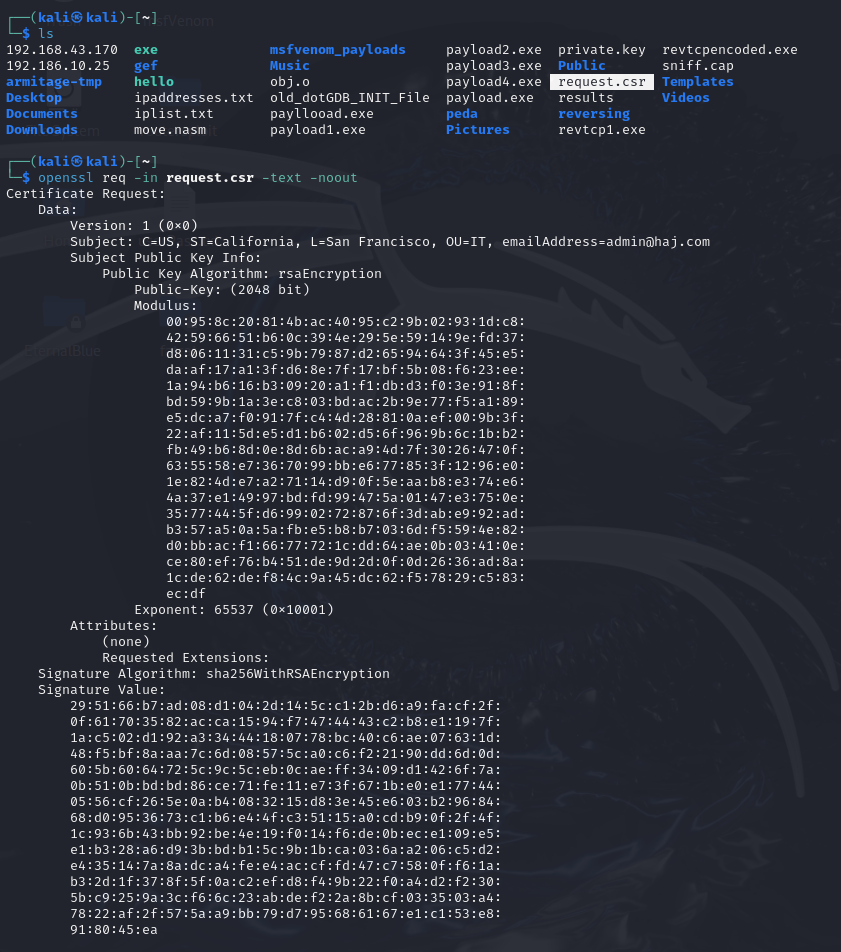
User is prompted to enter details like Country, State, Organization, Common Name, etc.

**Output:**

File created: request.csr

**Verification:**

Display the contents of the CSR:



The output displays the CSR details, including the public key and the subject fields.

**3. Create a Self-Signed Certificate**

**Command:**



**Description:**

This command generates a self-signed certificate valid for 365 days.

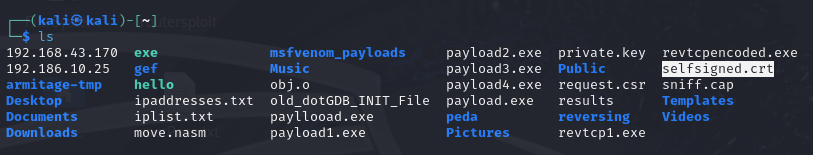
It uses the CSR (request.csr) and signs it with the private key (private.key).

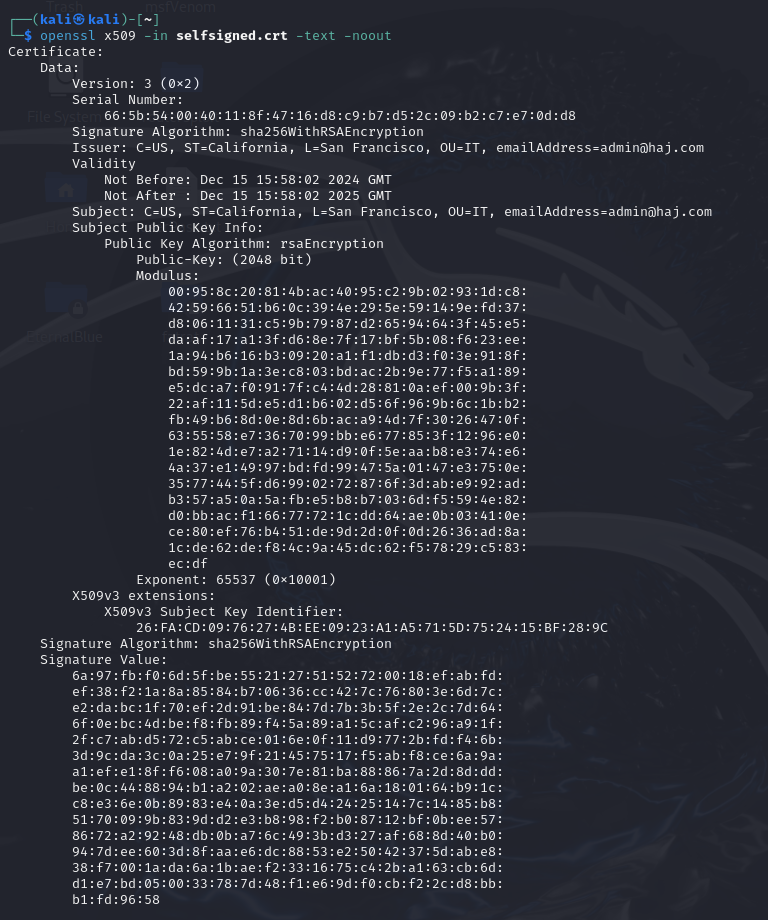
**Output:**

File created: selfsigned.crt

**Verification:**

Display the contents of the certificate:





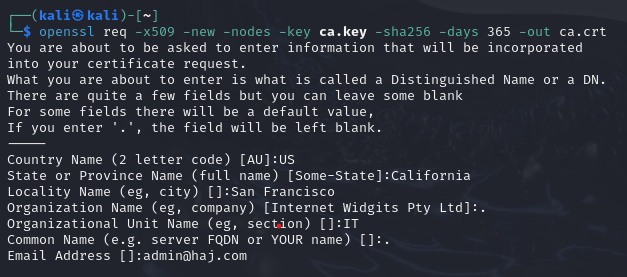
The Issuer and Subject fields are identical, confirming it is self-signed.

**4. Act as a Certification Authority (CA) to Issue Certificates**

Step 4.1: Create a CA Private Key and Certificate

**Commands:**





**Description:**

The first command generates a private key for the CA (ca.key).

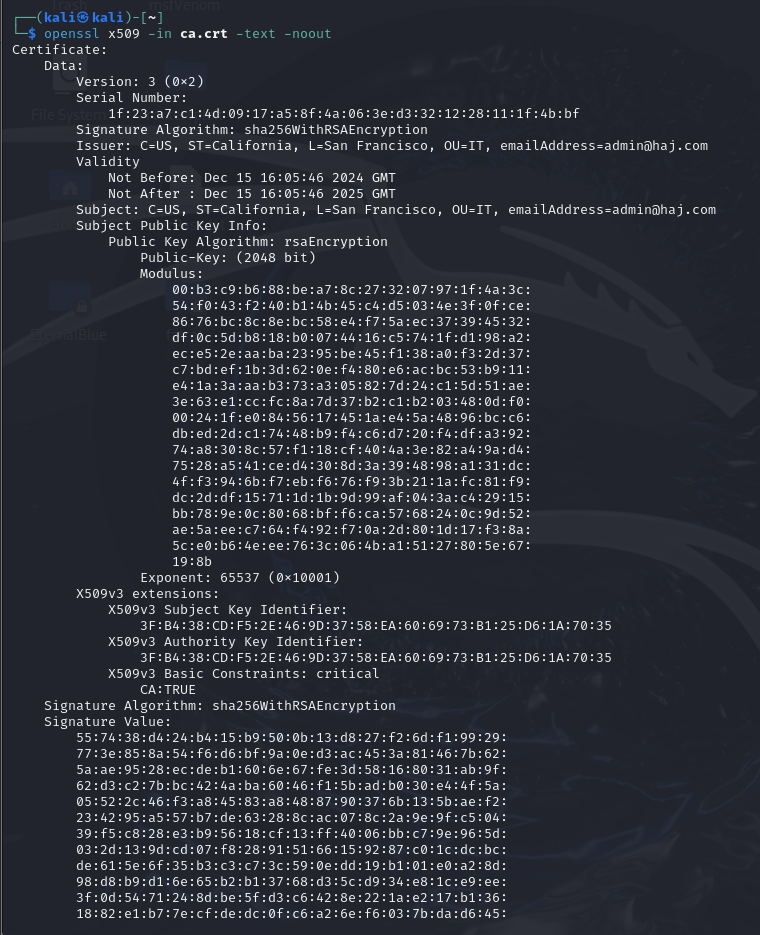
The second command creates a self-signed certificate (ca.crt) for the CA.

**Output:**

Files created: ca.key and ca.crt

**Verification:**

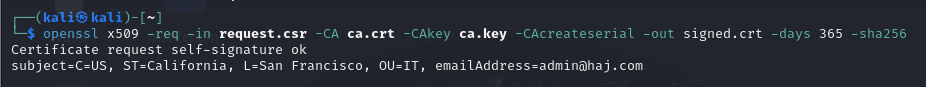
Display the contents of the CA certificate:



The Issuer and Subject fields match, indicating it is a CA certificate.

**Step 4.2: Sign a Certificate Using the CA**

**Command:**



**Description:**

This command uses the CA certificate (ca.crt) and private key (ca.key) to sign the CSR (request.csr).

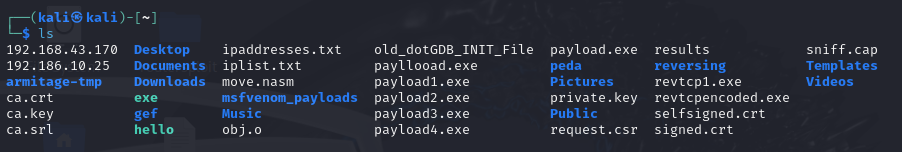
The signed certificate (signed.crt) is valid for 365 days.

**Output:**

Files created: signed.crt and ca.srl (serial number file).

**Verification:**

Display the contents of the sig ned certificate:





The Issuer field matches the CA details, and the Subject field should match the CSR details.

Full Screenshots:

