Shahryar Awan

251710692

**Commands**

**Step 1: Generate a 2048-bit RSA Private Key**

openssl genrsa -out private\_key.pem 2048

**Step 2: Generate the Public Key**

openssl rsa -in private\_key.pem -pubout -out public\_key.pem

**Step 3: Create a Certificate Signing Request (CSR)**

openssl req -new -key private\_key.pem -out request.csr

**Step 4: Generate a Self-Signed Certificate**

openssl x509 -req -days 365 -in request.csr -signkey private\_key.pem -out self\_signed.crt

**Step 5: Create Directories and Files for the CA**

mkdir -p ~/myCA/{certs,private,newcerts}

touch ~/myCA/index.txt

echo 1000 > ~/myCA/serial

**Step 6: Generate the CA's Private Key**

openssl genrsa -out ~/myCA/private/ca\_key.pem 2048

**Step 7: Create the CA's Self-Signed Certificate (valid for 10 years)**

openssl req -x509 -new -days 3650 -key ~/myCA/private/ca\_key.pem -out ~/myCA/certs/ca\_cert.pem

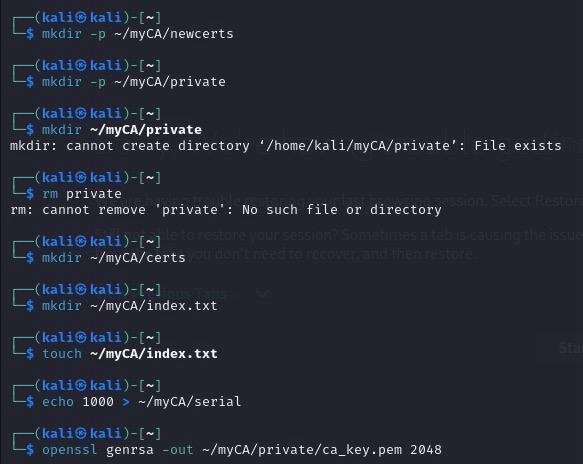
**Step 8: Sign the CSR with the CA to Issue a Certificate**

openssl x509 -req -in request.csr -CA ~/myCA/certs/ca\_cert.pem -CAkey ~/myCA/private/ca\_key.pem -CAcreateserial -out signed.crt -days 365

**Step 9: Verify the Signed Certificate**

openssl verify -CAfile ~/myCA/certs/ca\_cert.pem signed.crt

**SCREENSHOTS**

** **

****

****