Lab 8: SSH and SSL

Parth Kalkar

Q1. Generate ssh key pairs different from the exercise encryption algorithm. Use those keys to access a remote machine (VM for example). Provide all necessary secure configuration.

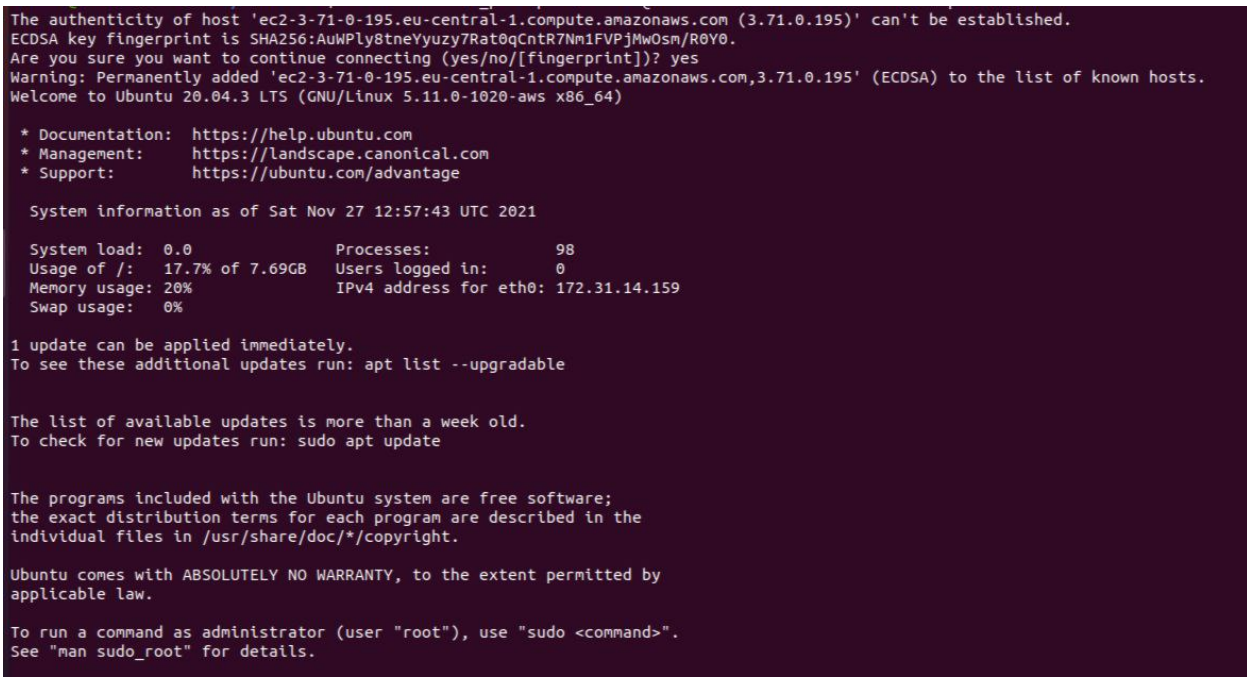
- SSH key pair to access an instance in AWS will be generated, later will connect to this instance using SSH from the local machine

  The steps mentioned below should be followed:

  1. .pem key-pair file

2. To get access:
   $ *ssh -i "center_pair.pem"*
   ubuntu@ec2-3-71-0-195.eu-central-1.compute.amazonaws.com

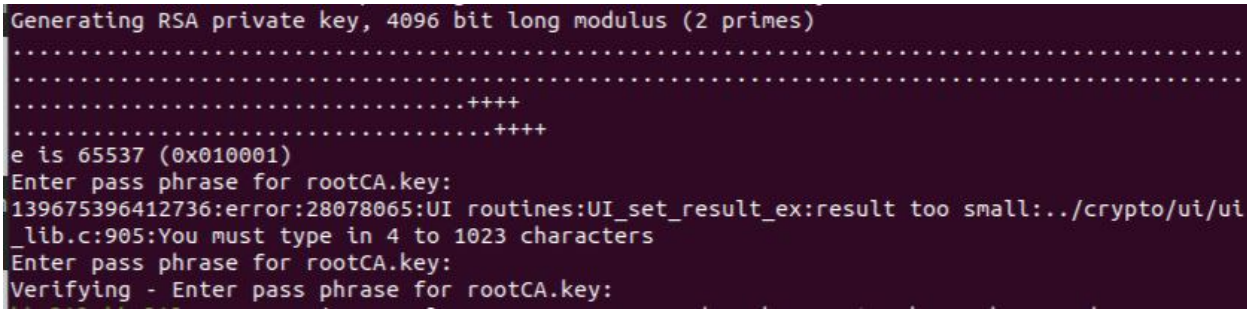
3. Output



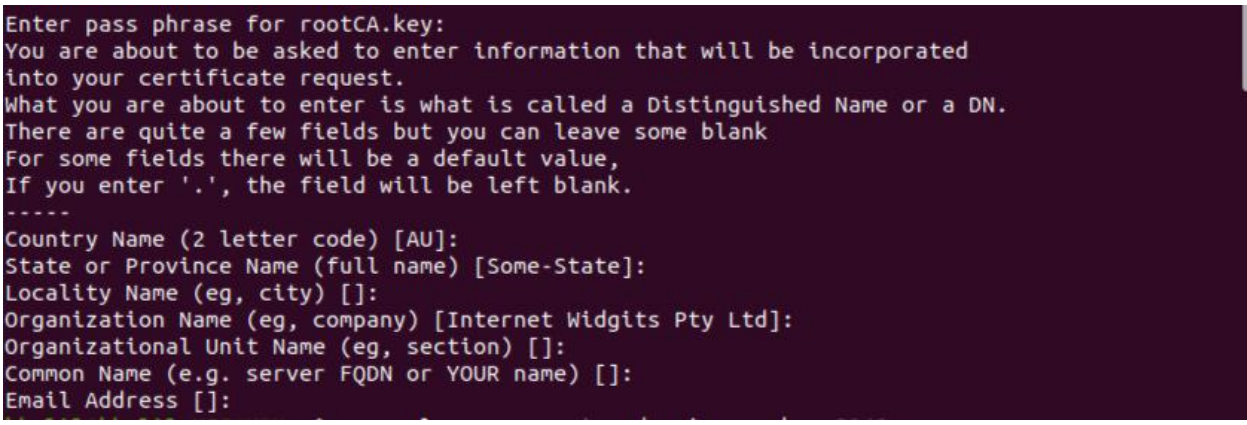
Q2. Create root certificate CA and generate your domain certificate with public and private keys. Generate a Certificate Signing Request for your domain certificate then generate your certificate with the CA's signature to form a certificate using CA certificate, set expiration days to 365. Show your content of certificate with attributes: ISSUER, Validity, Serial Number, Subject etc. Convert your certificate to DER format (install openssl tool with apt/yum). Keep these certificates, it will be used for the next LAB.

- The steps mentioned below should be followed:
  1. Create Root certificate:

$ *openssl genrsa -des3 -out rootCA.key 4096*

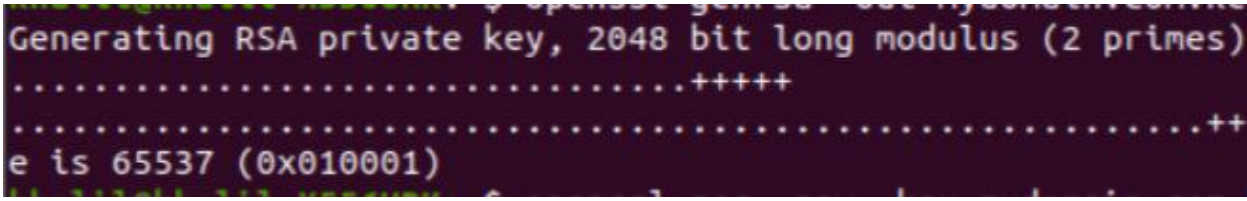


$ *openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.crt*



2. Create Domain Certificate with public/private keys:

$ *openssl genrsa -out mydomain.com.key 2048*



3. Create certificate signing request for the domain certificate:

$ *openssl req -new -key mydomain.com.key -out mydomain.com.csr*

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

4. Create certificate with CA's signature with 365 expiration days:

   $ *openssl x509 -req -in mydomain.com.csr -CA rootCA.crt -CAkey rootCA.key CAcreateserial -out mydomain.com.crt -days 365 -sha256*

5. Show content of certificate:

   $ *openssl x509 -in mydomain.com.crt -text -noout*

```
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
        Subject Public Key Info:
```

6. Convert to DER:

   $ *openssl x509 -in your_domain.crt -outform der -out your_domain.der*