Assignment 2

Due: 5 December 2023 by 23:59:59 EST

Grade: 5% of final mark

Description:

This assignment requires you to build a Certificate Authority (CA) on your virtual machine or personal computer, and then sign and return a certificate request using your CA's private key.

There are many different ways to create a Certificate Authority. Ideally you would use the OpenSSL tool directly to create your private and public keys, and to sign certificate requests. However, the principles are more important for this assignment, so you can use a tool called Easy-RSA to manage all of the cryptographic operations for you.

CA Setup

Follow the steps in this tutorial to create your CA: How To Set Up and Configure a Certificate Authority On Ubuntu 22.04.

Be sure to read through this assignment first, before running any of the commands in the tutorial.

If you need to start again, you can run the following command:

```
rm -rf ~/easy-rsa
```

And then resume the tutorial at Step 2 — Preparing a Public Key Infrastructure Directory.

Notes

The tutorial assumes that you are working as a non-privileged user named `sammy`. Be sure to substitute in your `itec2210` user instead of `sammy` when you come to commands that require a username or path.

The steps below correspond to the steps in the tutorial, and indicate additional steps or configuration options that you should choose where applicable.

Step 1: Installing Easy-RSA

1. Run the commands as instructed.

Step 2: Preparing a Public Key Infrastructure Directory

1. Run the commands as instructed. Look around the `easy-rsa` directory to see what it created for you. Use a command like `ls -laR ~/easy-rsa`.

Step 3: Creating a Certificate Authority

1. You **MUST** use a different Common Name (CN) for your CA than the default “Easy-RSA CA” in this step.

   Use the following format for your CN: 31415926.itec2210.ca

   Substitute in your student number in place of ***31415926***.

   Then complete the steps as instructed. If you do not complete this step then your submission will not be associated with your student number and it will not be graded.

Step 4: Distributing your Certificate Authority’s Public Certificate

1. Run the `cat` command, and record the output somewhere. This is the public key for your CA. A good place to store it is in a message to yourself in Mattermost. You will need to send it to me at the end of the assignment.
2. Skip the rest of the steps in this section after the initial `cat` command.

Step 5: (Optional) — Creating and Signing a Practice Certificate Request

1. Practice creating your own certificate and signing it with your CA. Use your existing class virtual machine instead of a new second system.
2. You won’t be graded on this step, it is just for you to get familiar with your CA.

Step 6: (Optional) — Signing a CSR

1. Sign the following Certificate Signing Request (copy and paste everything that is grey):

```
-----BEGIN CERTIFICATE REQUEST-----
MIH/MIGyAgEAMH8xCzAJBgNVBAYTAkNBMRAwDgYDVQQIDAdPbnRhcmlvMRAwDgYD
VQQHDAdUb3JvbnRvMRgwFgYDVQQKDA9Zb3JrIFVuaXZlcnNpdHkxETAPBgNVBAsM
CElURUMyMjEwMR8wHQYDVQQDDBZpbnN0cnVjdG9yLml0ZWMyMjEwLmNhMCowBQYD
K2VwAyEA1BFy2kgz4kTj4IpmUyym/ZHsjtgroPzFOdCi1F9IOZ6gADAFBgMrZXAD
QQBagxfxE8snk2DS38UHe6w0UCyLGU6ToPolx1g+95999Bfjo+rFz//ZWW58e9Ll
ur/vnqAAHRlar+Pjthhj0V0C
-----END CERTIFICATE REQUEST-----
```

2. To complete this step you will need to copy the CSR onto your server in a file called `/tmp/itec2210-server.req`. Use `nano /tmp/itec2210-server.req` to open the file, then paste in the CSR from above. Exit nano by entering CTRL+X, then press Enter when you are prompted to save the file.
3. Sign the CSR and again use the `cat` command to output the contents of the resulting file. It should be in: `/home/itec2210/easy-rsa/pki/issued/itec2210-server.crt`
4. Copy the contents somewhere. A good place to store it is in a message to yourself in Mattermost.

Submitting:

1. Verify your CA certificate and signed request using the following command: `openssl verify -CAfile pki/ca.crt pki/issued/itec2210-server.crt`

   You should receive: `pki/issued/itec2210-server.crt: OK`

2. Visit https://assignment2.itec2210.ca. Verify your CA using the form. Verify my signed certificate using the form. When you are happy with the results, submit your ca.crt file and the signed itec2210-server.crt file.

Evaluation Criteria:

Requirement	Test case	Grade
A Certificate Authority	You have Easy-RSA installed, or created your own CA using OpenSSL	1
Your CA's public key	The contents of your CA's `ca.crt` file.	2
A Signed Certificate Request	A signed certificate for my instructor signing request.	2

Final notes:

If you would like to use OpenSSL to create your CA please let me know. I'm happy to guide you through it.