Open SSL Encrypt and Decrypt Files

Estimated time needed: 15 minutes

In this lab, you will learn to encrypt files into an unreadable, incomprehensible format using special hashing techniques and also decrypt an encrypted file.

Learning Objectives

After completing this lab, you will be able to:

- Perform download and then decrypt an encrypted file
- Create special and secret keys to encrypt your files
- Perform decryption of the encrypted files
- Apply encryption with 2500 iterations that strengthen the encryption standard.

Prerequisites (optional)

Familiar with using the Linux command prompt.

Task 1: Decrypting a simple file

Step 1:

Run the following command in the terminal on the right to get an encrypted secret file.

```
wget https://cf-courses-data.s3.us.cloud-object-storage.appdomain.cloud/IBM-CD0267EN-SkillsNetwork/labs/module1/encrypted_secretfile
```

This will download the file into your local environment.

Step 2:

View the file content from the explorer menu on the left.

You will see that the content is not readable, and is all encrypted. This has been encoded using aes-256-cbc cipher. Each cipher has its own algorithm. aes-256-cbc is one of the older and simpler ciphers, and there are now much better algorithms to encrypt the data.

Step 3:

Run the following command to decrypt the file.

```
openssl aes-256-cbc -d -a -pbkdf2 -in encrypted_secretfile -out secrets.txt
```

Command option	**Meaning**
aes-256-cbc	The cipher algorithm
-d	Decrypt
-a	Base64 decode
-pbkdf2	Use password-based key derivation function 2
-in encrypted_secretfile	Input file
-out secrets.txt	Output file

Step 4:

It will prompt you for a password. When the file was encrypted, it was done so with the aes-256-cbc cipher using a password. You need to type the password into the prompt to decrypt the file. The file has been encrypted with the password `adios`. The same needs to be given to decrypt it.

Type the password and press enter. Note that the password will not appear on the terminal.

Step 5:

The decrypted file will be viewable through the explorer with decrypted contents.

Task 2: Encrypt the file

Now that you have decrypted the file, take it further and encrypt the file.

Step 1:

Make changes, as you require, to the secret.txt file and encrypt it with a new password. It will prompt you to enter and renter the same password to verify. Make sure you remember the password.

```
openssl aes-256-cbc -a -pbkdf2 -in secrets.txt -out secrets.txt.enc
```

Step 2:

Now, if you see the file secrets.txt.enc, it will have encrypted contents.

Step 3:

Remove the original `secret.txt` from the system by running the following command.

```
rm secrets.txt
```

Challenge:

Follow the instructions outlined in **Task 1** starting from **Step 3**, and then continue with the subsequent steps to decrypt the file and view its contents.

> Note: Here you are required to establish a new password, distinct from the one provided in *Step 4*.

Task 3: Changing the Encrypt options

1. To encrypt the file in a manner that is not easily decryptable, we can also set the iterations to higher numbers. Many iterations increase the time required to brute-force the encrypted file.

   ```
   openssl aes-256-cbc -a -pbkdf2 -iter 2500 -in secrets.txt -out secrets_2500.txt.enc
   ```

You will observe a change in the content of the encrypted file when you use a different number of iterations.

Conclusion

Congratulations! You have now learned to encrypt and decrypt files.

Next Steps

You can optionally explore the cipher algorithms available with OpenSSL by typing the following command in the terminal.

```
openssl enc --list
```

Author(s)

Lavanya T S

Changelog

Date	Version	Changed by	Change Description
2023-12-20	0.5	Sowmyaa Gurusamy	Updated the instructions
2023-09-18	0.4	Dania Kulsum	Added output screenshot
2023-08-09	0.3	Mary Stenberg	QA Pass with edits
2023-08-07	0.2	Gagandeep Singh	ID review
2023-07-31	0.1	Lavanya T S	Initial version created