Lab - Encrypting and Decrypting Data Using OpenSSL

.

Objectives

Part 1: Encrypting Messages with OpenSSL

Part 2: Decrypting Messages with OpenSSL

Background / Scenario

OpenSSL is an open source project that provides a robust, commercial-grade, and full-featured toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It is also a general-purpose cryptography library. In this lab, you will use OpenSSL to encrypt and decrypt text messages.

Note: While OpenSSL is the de facto cryptography library today, the use presented in this lab is NOT recommended for robust protection. Below are two security problems with this lab:

1) The method described in this lab uses a weak key derivation function. The ONLY security is introduced by a very strong password.
2) The method described in this lab does not guarantee the integrity of the text file.

This lab should be used for instructional purposes only. The methods presented here should NOT be used to secure truly sensitive data.

Required Resources

- Cybersec Workstation virtual machine

Instructions

Part 1: Encrypting Messages with OpenSSL

OpenSSL can be used as a standalone tool for encryption. While many encryption algorithms can be used, this lab focuses on AES. To use AES to encrypt a text file directly from the command line using OpenSSL, follow the steps below:

Step 1: Encrypting a Text File

a. Log into Cybersec Workstation VM.

b. Open a terminal window.

c. Find the file plaintext.txt which we created in previous lab.

d. Type the command below to list the contents of the encrypted **plaintext.txt** text file on the screen:

```
[Cybersec@ubuntu:~]$ cat plaintext.txt
This is a plaintext file
New line
[Cybersec@ubuntu :~]$
```

e. From the same terminal window, issue the command below to encrypt the text file. The command will use AES-256 to encrypt the text file and save the encrypted version as **message.enc**. OpenSSL will ask for a password and for password confirmation. Provide the password as requested and be sure to remember the password.

```
[Cybersec@ubuntu :~]$ openssl aes-256-cbc -in plaintext.txt -out message.enc
enter aes-256-cbc encryption password:
```

```
Verifying - enter aes-256-cbc encryption password:
[Cybersec@ubuntu :~]$
```

Document the password.

f. When the process is finished, use the **cat** command again to display the contents of the **message.enc** file.

```
[Cybersec@ubuntu :~]$ cat message.enc
```

Did the contents of the **message.enc** file display correctly? What does it look like? Explain.

g. To make the file readable, run the OpenSSL command again, but this time add the **-a** option. The **-a** option tells OpenSSL to encode the encrypted message using a different encoding method of Base64 before storing the results in a file.

Note: Base64 is a group of similar binary-to-text encoding schemes used to represent binary data in an ASCII string format.

```
[Cybersec@ubuntu :~]$ openssl aes-256-cbc -a -in plaintext.txt -out
message.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
```

h. Once again, use the **cat** command to display the contents of the, now re-generated, **message.enc** file:

Note: The contents of **message.enc** will vary.

```
[Cybersec@ubuntu :~]$ cat message.enc
U2FsdGVkX19ApWyrn8RD5zNp0RPCuMGZ98wDc26u/vmj1zyDXobGQhm/dDRZasG7
Mufkv+FOGn+SoEEuh7l4fk0LIPEfGsExVFB4TGdTiZQApRw74rTAZaE/dopaJn0
sJmR3+3C+dmgzZIKEHWsJ2pgLvj2Sme79J/XxwQVNpw=
[Cybersec@ubuntu :~]$
```

Is **message.enc** displayed correctly now? Explain.

Yes. While message.enc is encrypted, it is now correctly displayed because it has been converted from binary to text and encoded with Base64.

Can you think of a benefit of having **message.enc** Base64-encoded?

The encrypted message can now be copied and pasted in an email message, for example.

Part 2: Decrypting Messages with OpenSSL

With a similar OpenSSL command, it is possible to decrypt **message.enc**.

a. Use the command below to decrypt message.enc:

```
[Cybersec@ubuntu :~]$ openssl aes-256-cbc –a -d -in message.enc -out
decrypted_letter.txt
```

b. OpenSSL will ask for the password used to encrypt the file. Enter the same password again.

c. When OpenSSL finishes decrypting the **message.enc** file, it saves the decrypted message in a text file called **decrypted_letter.txt**. Use the **cat** display the contents of **decrypted_letter.txt**:

```
[Cybersec@ubuntu :~]$ cat decrypted_letter.txt
```

Was the letter decrypted correctly?

The command used to decrypt also contains -a option. Can you explain?