Packet Tracer - Explore File and Data Encryption

Objectives

Part 1: Discover the FTP Account Credentials for Mary

Part 2: Upload Confidential Data using FTP

Part 3: Discover the FTP Account Credentials for Bob

Part 4: Download Confidential Data using FTP

Part 5: Decrypt the Contents of a Sensitive File

Background

In this Packet Tracer activity, you will access the encrypted content of multiple files and transfer a file to an FTP server. Then, in the role of another user, you will download the file from the FTP server and decrypt the file contents. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices to transfer a file with encrypted data to another device.

To decrypt text and files in this activity, you will use OpenSSL. 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.

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

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

This activity should be used as a learning tool only. The methods presented here should NOT be used to secure truly sensitive data.

Resources

The **CSE-LABVM** installed in VirtualBox

Note: It is recommended that you use the **CSE-LABVM** for the decryption tasks in this activity. The **CSE-LABVM** was installed during the **Lab - Install a Virtual Machine on a Personal Computer**.

Instructions

Part 1: Discover the FTP Account Credentials for Mary

Mary's laptop is named **Laptop BR-1** in the **Branch Office**. Mary has a text document on her laptop that contains her FTP login information in encrypted form. The contents must be decrypted to enable access to the **BR Server** which is located in the **Branch Wiring Closet**.

Step 1: Access the text document on Mary's Laptop.

a. Click **Laptop BR-1** > **Desktop** tab > **Text Editor**.

b. In the **Text Editor** window, click **File > Open**.

c. Click the document **maryftplogin.txt** and click **OK**.

Step 2: Decrypt Mary’s FTP account information.

a. Highlight all the text from the **maryftplogin.txt** file and copy it.

b. Start the **CSE-LABVM**.

c. Double click the **Terminal** icon on the desktop to open a terminal.

d. Use the following command to decrypt the contents of the file and reveal the FTP login information for Mary.

```
cisco@labvm:~$ echo
'U2FsdGVkX1+sKwL7uceALGKqAQ78WWown3ok73zicO8GLYu2SpMvLEwCB7HsyRC3MeimUjiXRCLw
OSSahAraUrnEtkClGK4tytP9hludc6k=' | openssl aes-256-cbc -pbkdf2 -a -d
```

This command sends the encrypted text to the OpenSSL application. The **aes-256-cbc** option tells OpenSSL to use the Advanced Encryption System with a 256 bit key length and Cipher Block Chaining. The **pbkdf2** option enables Password-Based Key Derivation Function 2 which applies a hash-based message authentication code or HMAC to the password along with salt. The **-a** option tells OpenSSL to encode the encrypted message using a different encoding method of Base64. The **-d** option tells the application to decrypt the data.

e. When you are asked for the decryption password, use **maryftp123**.

```
enter aes-256-cbc decryption password: maryftp123
```

What is the username and password for Mary’s FTP account?

Part 2: Upload Confidential Data using FTP

Mary works for a credit card agency and needs to send the agency a file that contains the data of some customers. In Part 2, you will verify that the data is encrypted before uploading it to the **BR Server**.

Step 1: View the confidential document on Laptop BR-1

a. Return to **Laptop BR-1**. Open the **Text Editor**, if necessary, and click **File** > **Open**.

b. Click the document **clientinfo.enc** and click **OK**.

What form is the data in?

Step 2: Connect to the BR Server.

a. Close the **Text Editor** window, and then click **Command Prompt**.

b. At the prompt, enter the **ftp 10.0.3.30** command to connect to the **BR Server**.

c. Use Mary's credentials that you decrypted early to authenticate.

Step 3: Upload a file to the FTP server.

a. At the **ftp>** prompt, enter the command **dir** to view the current files stored on the server.

b. Use the **put** command to upload the **clientinfo.enc** file to the server.

c. At the **ftp>** prompt, enter the command **dir** and verify the **clientinfo.en**c file is now on the server.

d. Enter **quit** to end the FTP session.

If threat actors were to capture the file transfer, what would be in clear text?

Part 3: Discover the FTP Account Credentials for Bob

Bob needs to access the contents of the file Mary stored on the **BR Server** to verify some customer information. Like Mary, Bob needs to decrypt his FTP login information in order to access the **BR Server** and download the file.

Step 1: Access the text document on Bob's Laptop.

a. In **Branch Office**, click **Laptop BR-2**, and then open the **Text Editor**.

b. In the **Text Editor** window, click **File** > **Open**.

c. Click the document **bobftplogin.txt** and click **OK**.

Step 2: Decrypt Bob’s FTP account information.

a. Highlight all the text from the **bobftplogin.txt** file and copy it.

b. Return to the terminal window in the **CSE-LABVM**.

c. Use the following command to decrypt the contents of the file and reveal the FTP login information for Bob.

```
cisco@labvm:~$ echo
'U2FsdGVkX1/+3jGTemCqs3e4dK8+b0xfXJiq4eoU0lQgRV9aZQPqJCBsYJWc9lDQwiB2svhiWSUV
hCRS5qBrjgmDZF3q/dXqaCrZRR5prjE=' | openssl aes-256-cbc -pbkdf2 -a -d
```

d. When you are asked for the decryption password, use **bobftp123**.

```
enter aes-256-cbc decryption password: bobftp123
```

What is the username and password for Bob’s FTP account?

Part 4: Download Confidential Data using FTP

In this Part, you will download and decrypt the confidential data stored on the **BR Server**.

Step 1: Connect to the BR Server.

a. In Branch Office on Laptop BR-2, close the **Text Editor** window, and then click **Command Prompt**.

b. At the prompt, enter the **ftp 10.0.3.30** command to connect to the **BR Server**.

c. Use Bob's credentials that you decrypted early to authenticate.

Step 2: Download the file to Bob’s PC.

a. At the **ftp>** prompt, enter the command **dir** to view the current files stored on the **BR Server**.

b. Use the **get** command to download the **clientinfo.enc** file from the server.

c. Enter **quit** to end the FTP session.

d. At the **C:\>** prompt, enter the command **dir** and verify the **clientinfo.enc** file is now on **Laptop BR-2**.

If threat actors were to capture the file transfer crossing the internet, what would be in clear text?

Part 5: Decrypt the Contents of a Sensitive File

In this Part, you will decrypt the **clientinfo.enc** file.

Step 1: Get the decryption key.

Now that Bob has the file, he needs to decrypt it so that he can read it. Earlier, Mary sent Bob an email with the decryption key for the file. Use the email program to retrieve the encryption key for the **clientinfo.enc** file.

a. Close the **Command Prompt** window, and then click **Email**.

b. Click the Email with the subject **Decryption Key** and record the decryption key below.

   What is the decryption key to access the confidential information in the **clientinfo.enc** file?

Step 2: Decrypt the contents of the clientinfo.enc file.

a. Close the Email window, and the click **Text Editor**.

b. In the Text Editor window, click **File** > **Open**, click the document **clientinfo.enc**, and then click **OK**.

c. Highlight all the text in the **clientinfo.enc** file and copy it.

d. In the **CSE-LABVM**, click the **Menu** button and click **Text Editor Pluma**.

e. Click **Edit** > **Paste**, and then click **File** > **Save**.

f. Save the file with the name **clientinfo.enc**.

g. Close **Pluma**.

h. In the terminal, enter the **ls** command to verify that **clientinfo.enc** is in the current directory. If not, navigate to the directory where **clientinfo.enc** is stored.

i. Use the following command to decrypt the **clientinfo.enc** file.

```
cisco@labvm:~$ openssl aes-256-cbc -pbkdf2 -a -d -in clientinfo.enc -out
clientinfo.txt
```

j. When prompted for the decryption password, use the password you discovered in the email from Mary.

```
enter aes-256-cbc decryption password:
cisco@labvm:~$
```

k. Enter the **ls** command to see that a new file, **clientinfo.txt**, has been added to the directory.

l. Use any method you wish to open the **clientinfo.txt** file to see the decrypted contents.

   What is the first name listed in the **clientinfo.txt** file?

Answer Key

Part 1: Discover the FTP Account Credentials for Mary

Step 1: Access the text document on Mary's Laptop.

Step 2: Decrypt Mary’s FTP account information.

What is the username and password for Mary’s FTP account?

username: mary   password: cisco321

Part 2: Upload Confidential Data using FTP

Step 1: View the confidential document on Laptop BR-1

What form is the data in?

Encrypted form

Step 2: Connect to the BR Server.

Step 3: Upload a file to the FTP server.

If threat actors were to capture the file transfer, what would be in clear text?

The username: mary   password: cisco321 for the FTP connection are in clear text but the contents of the document are encrypted.

Part 3: Discover the FTP Account Credentials for Bob

Step 1: Access the text document on Bob's Laptop.

Step 2: Decrypt Bob’s FTP account information.

What is the username and password for Bob’s FTP account?

username: bob   password: ninja123

Part 4: Download Confidential Data using FTP

Step 1: Connect to the BR Server.

Step 2: Download the file to Bob’s PC.

If threat actors were to capture the file transfer crossing the internet, what would be in clear text?

The username: bob   password: ninja123 for the FTP connection are in clear text but the contents of the document are encrypted.

Part 5: Decrypt the Contents of a Sensitive File

Step 1: Get the decryption key.

What is the decryption key to access the confidential information in the **clientinfo.enc** file?

cisco123

Step 2: Decrypt the contents of the clientinfo.enc file.

What is the first name listed in the **clientinfo.txt** file?

Drew N. Stark