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.

Resources

- Cisco Packet Trace
- CSE-LABVM installed in VirtualBox

Instructions

Part 1: Discover the FTP Account Credentials for Mary

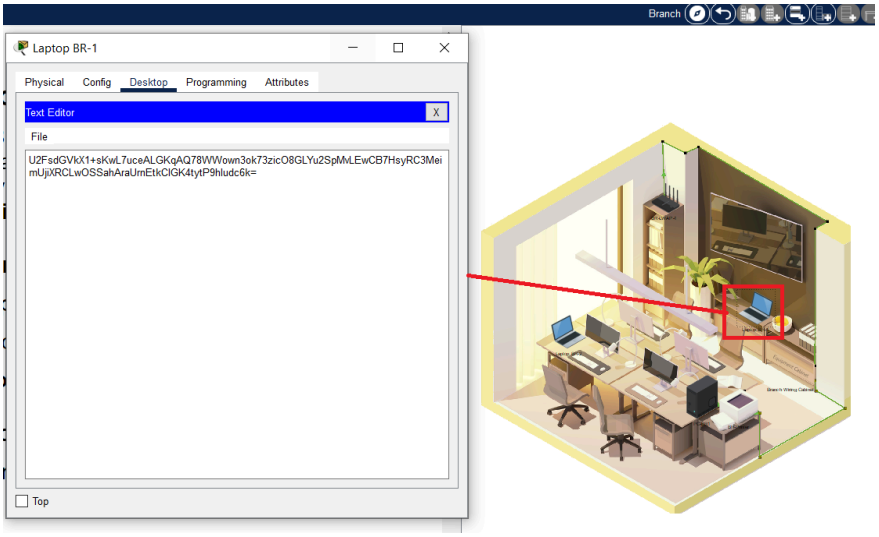
Mary's laptop is named Laptop BR-1 in the Branch Office. Mary has a text document on her laptop that contains her FTP login information in encrypted form. The contents must be decrypted to enable access to the BR Server which is located in the Branch Wiring Closet.

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.

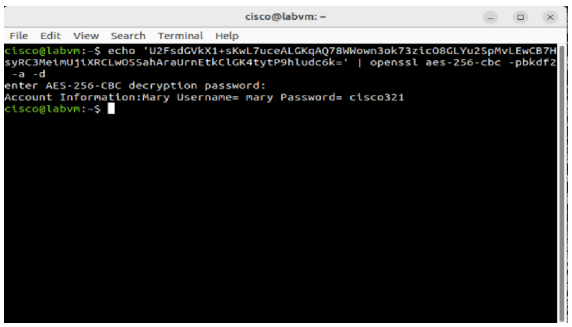
d. Use the following command to decrypt the contents of the file and reveal the FTP login information for Mary:

```
cisco@labvm:~$ echo
'U2FsdGVkX1+sKwL7uceALGKqAQ78WWown3ok73zicO8GLYu2SpMvLEwCB7Hsy
RC3MeimUjiXRCLwOSSahAraUrnEtkClGK4tytP9hludc6k=' | openssl
aes-256-cbc -pbkdf2 -a -d
```

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

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

R: *Username= mary Password= cisco321*



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?

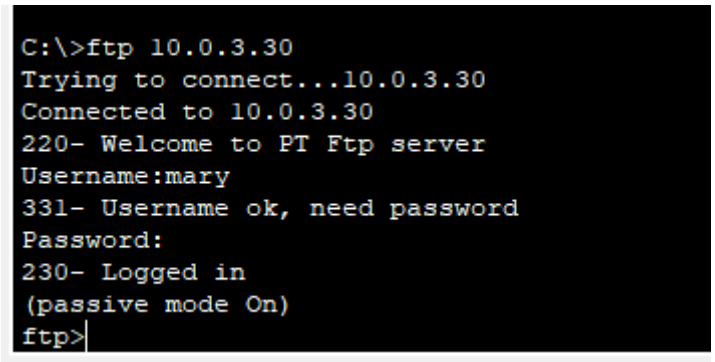
R: The data is encrypted.

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.enc file is now on the server.

```
ftp>put clientinfo.enc

Writing file clientinfo.enc to 10.0.3.30:
File transfer in progress...

[Transfer complete - 564 bytes]

564 bytes copied in 0.111 secs (5081 bytes/sec)
ftp>dir

Listing /ftp directory from 10.0.3.30:
0    : asa842-k8.bin                                5571584
1    : asa923-k8.bin                                30468096
2    : c1841-advipservicesk9-mz.124-15.T1.bin       33591768
3    : c1841-ipbase-mz.123-14.T7.bin                13832032
4    : c1841-ipbasek9-mz.124-12.bin                 16599160
5    : c1900-universalk9-mz.SPA.155-3.M4a.bin       33591768
6    : c2600-advipservicesk9-mz.124-15.T1.bin       33591768
7    : c2600-i-mz.122-28.bin                        5571584
8    : c2600-ipbasek9-mz.124-8.bin                  13169700
9    : c2800nm-advipservicesk9-mz.124-15.T1.bin     50938004
10   : c2800nm-advipservicesk9-mz.151-4.M4.bin      33591768
11   : c2800nm-ipbase-mz.123-14.T7.bin              5571584
12   : c2800nm-ipbasek9-mz.124-8.bin                15522644
13   : c2900-universalk9-mz.SPA.155-3.M4a.bin       33591768
14   : c2950-i6q412-mz.121-22.EA4.bin               3058048
15   : c2950-i6q412-mz.121-22.EA8.bin               3117390
16   : c2960-lanbase-mz.122-25.FX.bin               4414921
17   : c2960-lanbase-mz.122-25.SEE1.bin             4670455
18   : c2960-lanbasek9-mz.150-2.SE4.bin             4670455
19   : c3560-advipservicesk9-mz.122-37.SE1.bin      8662192
20   : c3560-advipservicesk9-mz.122-46.SE.bin       10713279
21   : c800-universalk9-mz.SPA.152-4.M4.bin         33591768
22   : c800-universalk9-mz.SPA.154-3.M6a.bin        83029236
23   : cat3k_caa-universalk9.16.03.02.SPA.bin       505532849
24   : cgr1000-universalk9-mz.SPA.154-2.CG          159487552
25   : cgr1000-universalk9-mz.SPA.156-3.CG          184530138
26   : clientinfo.enc                               564
27   : ir800-universalk9-bundle.SPA.156-3.M.bin     160968869
28   : ir800-universalk9-mz.SPA.155-3.M             61750062
29   : ir800-universalk9-mz.SPA.156-3.M             63753767
30   : ir800_yocto-1.7.2.tar                        2877440
31   : ir800_yocto-1.7.2_python-2.7.3.tar           6912000
32   : pt1000-i-mz.122-28.bin                       5571584
33   : pt3000-i6q412-mz.121-22.EA4.bin              3117390
ftp>
```

d. Enter quit to end the FTP session.

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

R: 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

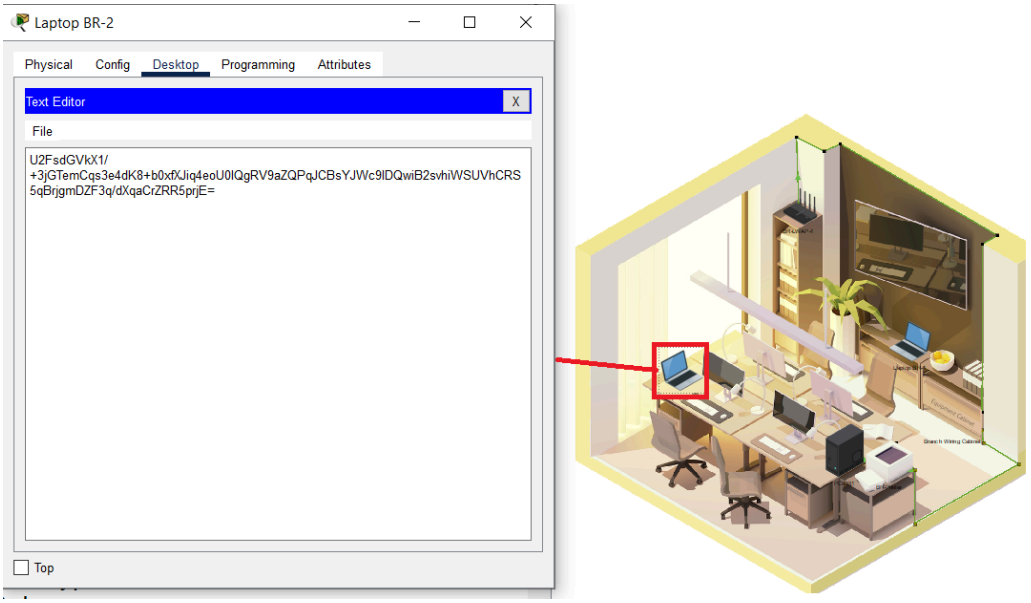
Bob needs to access the contents of the file Mary stored on the BR Server to verify some customer information. Like Mary, Bob needs to decrypt his FTP login information in order to access the BR Server and download the file.

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+b0xfXJiq4eoU0lQgRV9aZQPqJCBsYJWc9
lDQwiB2svhiWSUVhCRS5qBrjgmDZF3q/dXqaCrZRR5prjE=' | openssl
aes-256-cbc -pbkdf2 -a -d
```

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

```
cisco@labvm:~$ echo 'U2FsdGVkX1/+3jGTemCqs3e4dK8+b0xfXJiq4eoU0lQgRV9aZQPqJCBsYJW
c9lDQwiB2svhiWSUVhCRS5qBrjgmDZF3q/dXqaCrZRR5prjE=' | openssl aes-256-cbc -pbkdf2
 -a -d
enter AES-256-CBC decryption password:
Account Information: Username= bob Password= ninja123
cisco@labvm:~$
```

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

R: *Username= bob Password= ninja123*

Part 4: Download Confidential Data using FTP

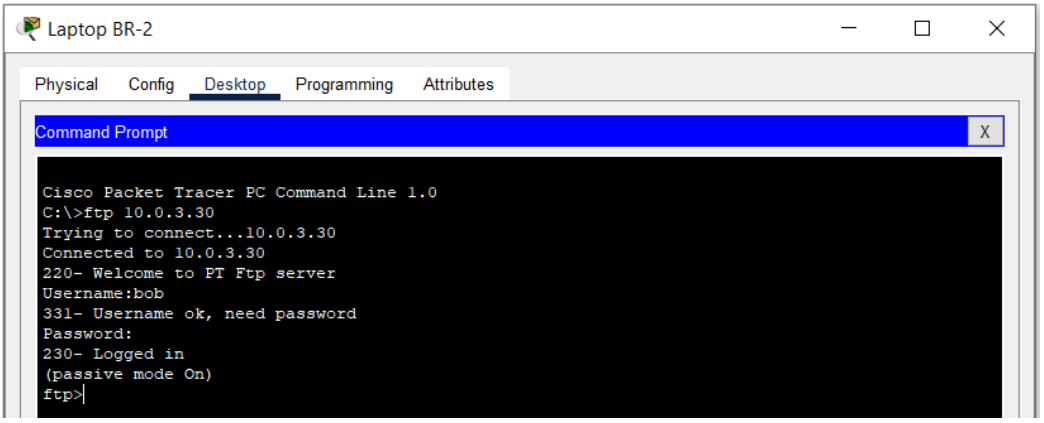
In this part, you will download and decrypt the confidential data stored on the BR Server.

Step 1: Connect to the BR Server.

a. In the Branch Office on Laptop BR-2, close the Text Editor window, and then clickCommand 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?

R: username: bob and 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

In this part, you will decrypt the clientinfo.enc file.

Step 1: Get the decryption key.

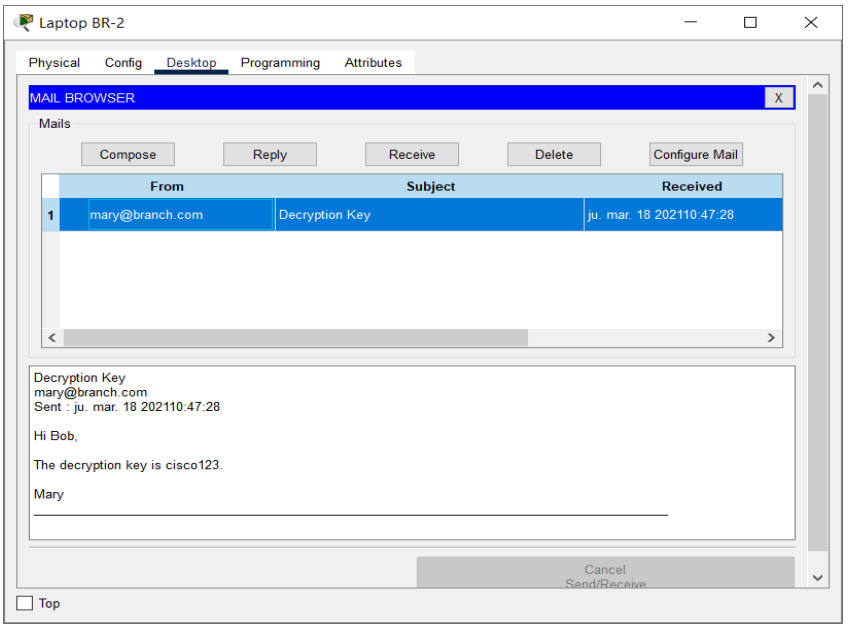
Now that Bob has the file, he needs to decrypt it so that he can read it. Earlier, Mary sent Bob an email with the decryption key for the file. Use the email program to retrieve the encryption key for the clientinfo.enc file.

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?

R: The decryption key is cisco123.



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

a. Close the Email window, and then click the 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.

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?

R: Drew N. Stark