Activity: Decrypt an encrypted message

Scenario

In this scenario, all of the files in your home directory have been encrypted. You'll need to use Linux commands to break the Caesar cipher and decrypt the files so that you can read the hidden messages they contain.

Here's how you'll do this task: **First**, you'll explore the contents of the home directory and read the contents of a file. **Next**, you'll find a hidden file and decrypt the Caesar cipher it contains. **Finally**, you'll decrypt the encrypted data file to recover your data and reveal the hidden message.

Task 1. Read the contents of a file

In this task, you need to explore the contents of your home directory and read the contents of a file to get further instructions.

1. Use the **ls** command to list the files in the current working directory.

```
analyst@bac9a5642fb5:~$ ls
Q1.encrypted  README.txt  caesar
```

2. Use the **cat** command to list the contents of the **README.txt** file.

```
analyst@bac9a5642fb5:~$ cat README.txt
Hello,
All of your data has been encrypted. To recover your data, you will need to solve a cip
her. To get started look for a hidden file in the caesar subdirectory.
```

Task 2. Find a hidden file

1. First, use the **cd** command to change to the **caesar** subdirectory of your home directory:
2. Use the **ls -a** command to list all files, including hidden files, in your home directory.

```
analyst@bac9a5642fb5:~$ cd caesar
analyst@bac9a5642fb5:~/caesar$ ls -a
.  ..  .leftShift3
```

3. Use the **cat** command to list the contents of the **.leftShift3** file.

```
analyst@bac9a5642fb5:~/caesar$ cat .leftShift3
Lq rughu wr uhfryhu brxu ilohv brx zloo qhhg wr hqwhu wkh iroorzlqj frppdqg:

rshqvvo dhv-256-fef -sengi2 -d -g -lq T1.hqfubswhg -rxw T1.uhfryhuhg -n hwwxeuxwh
```

The message in the .leftShift3 file appears to be scrambled. This is because the data has been encrypted using a Caesar cipher. This cipher can be solved by shifting each

alphabet character to the left or right by a fixed number of spaces. In this example, the shift is three letters to the left. Thus "d" stands for "a", and "e" stands for "b".

4. You can decrypt the Caesar cipher in the .leftshift3 file by using the following command:

```
analyst@bac9a5642fb5:~/caesar$ cat .leftShift3 | tr "d-za-cD-ZA-C" "a-zA-Z"
In order to recover your files you will need to enter the following command:

openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute
```

In this case, the command tr "d-za-cD-ZA-C" "a-zA-Z" translates all the lowercase and uppercase letters in the alphabet back to their original position. The first character set, indicated by "d-za-cD-ZA-C", is translated to the second character set, which is "a-zA-Z".

5. Now, return to your home directory before completing the next task:

Task 3. Decrypt a file

1. Use the exact command revealed in the previous task to decrypt the encrypted file:

```
analyst@bac9a5642fb5:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.reco
vered -k ettubrute
```

In this instance, the openssl command reverses the encryption of the file with a secure symmetric cipher, as indicated by AES-256-CBC. The -pbkdf2 option is used to add extra security to the key, and -a indicates the desired encoding for the output. The -d indicates decrypting, while -in specifies the input file and -out specifies the output file. The -k specifies the password, which in this example is ettubrute.

2. Use the **ls** command to list the contents of your current working directory again.

3. Use the **cat** command to list the contents of the **Q1.recovered** file.

```
analyst@bac9a5642fb5:~$ ls
Q1.encrypted  Q1.recovered  README.txt  caesar
analyst@bac9a5642fb5:~$ cat Q1.recovered
If you are able to read this, then you have successfully decrypted the classic cipher t
ext. You recovered the encryption key that was used to encrypt this file. Great work!
```