Decryption

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.

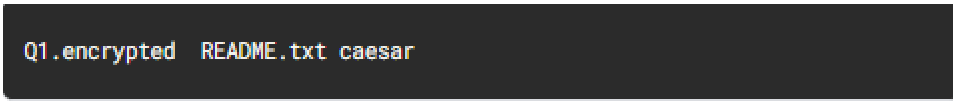
OK, it's time to decrypt some messages in Linux!

It starts with you logged in as user analyst, with your home directory, /home/analyst, as the current working directory.

Solution

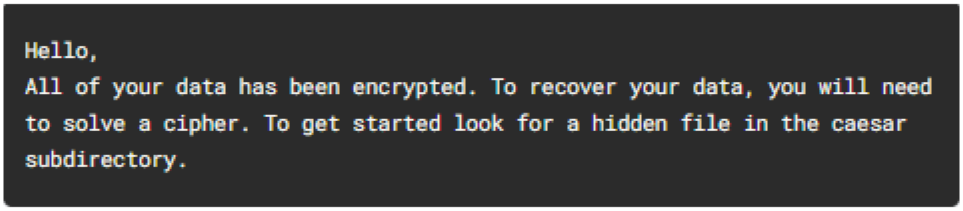
1. Read the contents of a file

- Use the ls command to list the files in the directory: ls /home/analyst.



```
Q1.encrypted  README.txt caesar
```

- List the contents of the README.txt file: cat README.txt.

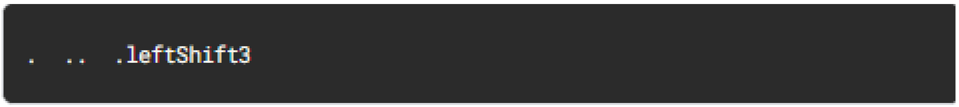


```
Hello,
All of your data has been encrypted. To recover your data, you will need
to solve a cipher. To get started look for a hidden file in the caesar
subdirectory.
```

The message in the README.txt file advises that the caesar subdirectory contains a hidden file.

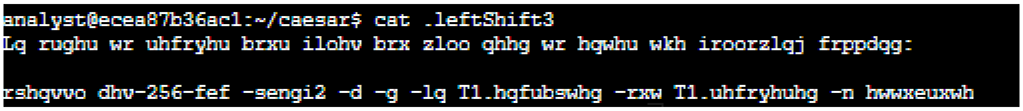
2. Find a hidden file In this task, you need to find a hidden file in your home directory and decrypt the Caesar cipher it contains.

- Use cd command to caesar subdirectory and use ls -a to list all files including hidden files: cd caesar and ls -a.



```
.  ..  .leftShift3
```

- Use the cat command to list the contents of the hidden file: cat .leftShift3.

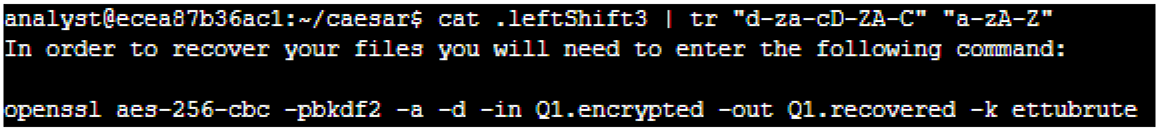


```
analyst@ecea87b36ac1:~/caesar$ cat .leftShift3
Lq rughu wr uhfryhu brxu ilohv brx zloo qhhg wr hqwhu wkh iroorzlqj frppdqg:

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

The message appears to be scrambled due to being encrypted with a Caesar cipher. The 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".

- Decrypt the Cipher using the command cat and tr: cat .leftShift3 | tr "d-za-cD-ZA-C" "a-zA-Z".



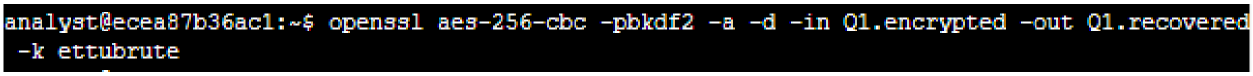
```
analyst@ecea87b36ac1:~/caesar$ cat .leftShift3 | tr "d-za-cD-ZA-C" "a-zA-Z"
In order to recover your files you will need to enter the following command:

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

The tr command translates text from one set of characters to another, using a mapping. The first parameter to the tr command represents the input set of characters, and the second represents the output set of characters. Hence, if you provide parameters “abcd” and “pqrs”, and the input string to the tr command is “ac”, the output string will be “pr".

4. Decrypt a file

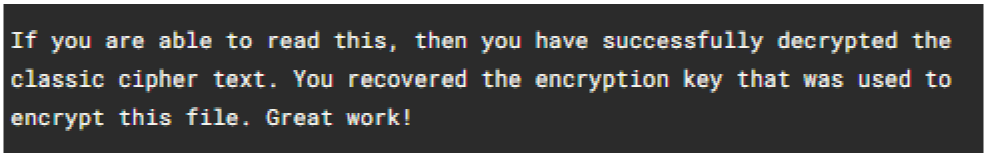
- Go back to initial working directory and run this command to decrypt a file: openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute.



```
analyst@ecea87b36ac1:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered
 -k ettubrute
```

This 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.

- Use the ls command and cat Q1.recovered.



```
If you are able to read this, then you have successfully decrypted the
classic cipher text. You recovered the encryption key that was used to
encrypt this file. Great work!
```