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.

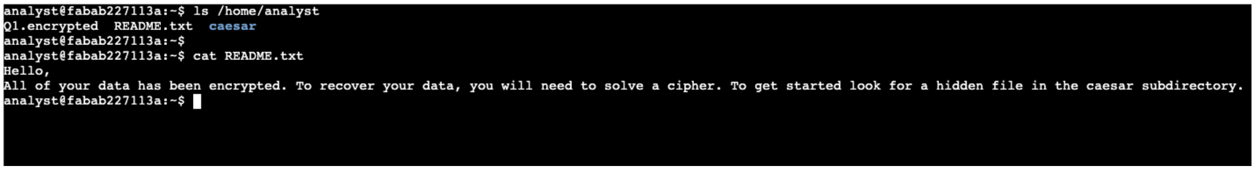
Task 1. Read the contents of a file

1.1. Command to list the files in the current working directory.

Command: ls /home/analyst

1.2. Command to list the contents of the `README.txt` file.

Command: cat README.txt

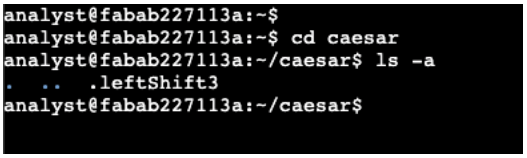


```
analyst@fabab227113a:~$ ls /home/analyst
Q1.encrypted  README.txt  caesar
analyst@fabab227113a:~$
analyst@fabab227113a:~$ cat README.txt
Hello,
All of your data has been encrypted. To recover your data, you will need to solve a cipher. To get started look for a hidden file in the caesar subdirectory.
analyst@fabab227113a:~$
```

Task 2. Find a hidden file

2.1. Command to list all files, including hidden files, in your home directory.

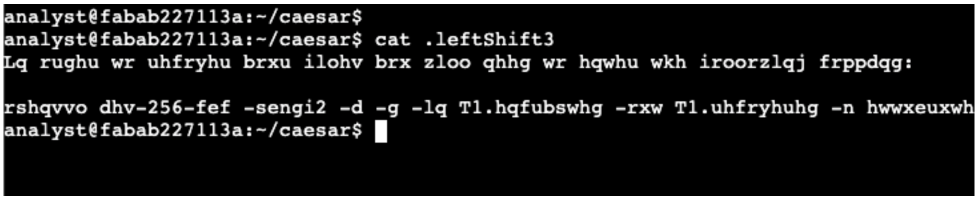
Command: ls -a



```
analyst@fabab227113a:~$
analyst@fabab227113a:~$ cd caesar
analyst@fabab227113a:~/caesar$ ls -a
.  ..  .leftShift3
analyst@fabab227113a:~/caesar$
```

2.2. Command to list the contents of the `.leftShift3` file.

Command: cat .leftShift3



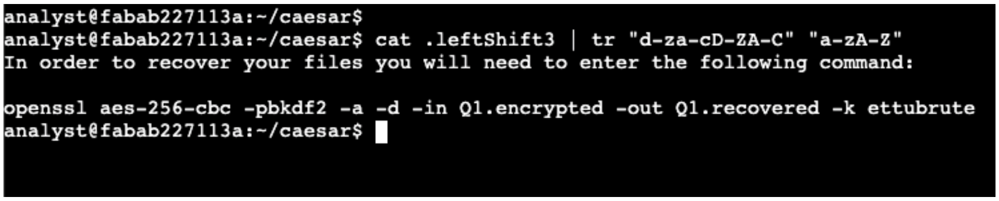
```
analyst@fabab227113a:~/caesar$
analyst@fabab227113a:~/caesar$ cat .leftShift3
Lq rughu wr uhfryhu brxu ilohv brx zloo qhhg wr hqwhu wkh iroorzlqj frppdqg:

rshqvvo dhv-256-fef -sengi2 -d -g -lq T1.hqfubswhg -rxw T1.uhfryhuhg -n hwwxeuxwh
analyst@fabab227113a:~/caesar$
```

2.3. Decrypt the Caesar cipher in the `.leftshift3` file

Command: cat .leftShift3 | tr "d-za-cD-ZA-C" "a-zA-Z"

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"`.



```
analyst@fabab227113a:~/caesar$
analyst@fabab227113a:~/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
analyst@fabab227113a:~/caesar$
```

Task 3. Decrypt a file

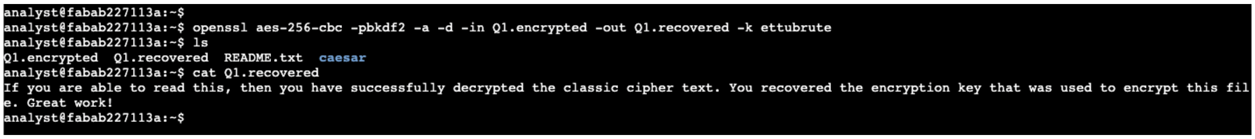
3.1. Command revealed in `.leftshift3` to decrypt a file and recover your data so you can read the message it contains.

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

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`.

3.2. Command to list the contents of the `Q1.recovered` file

Command: cat Q1.recovered



```
analyst@fabab227113a:~$
analyst@fabab227113a:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute
analyst@fabab227113a:~$ ls
Q1.encrypted  Q1.recovered  README.txt  caesar
analyst@fabab227113a:~$ 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 fil
e. Great work!
analyst@fabab227113a:~$
```