Decrypt an Encrypted File in Linux

Project description

The project demonstrates how I used Caesar cipher to decrypt an encrypted file in Linux OS.

Read the contents of a file

```
analyst@b93efedb7269:~$ ls
Q1.encrypted  README.txt  caesar
analyst@b93efedb7269:~$ cat README.txt
Hello,
All of your data has been encrypted. To recover your data, you will need to solve a cipher. T
o get started look for a hidden file in the caesar subdirectory.
analyst@b93efedb7269:~$
```

The first line of the screenshot displays the command I entered, and the other lines display the output prospectively. The code lists all contents of the projects directory. I used the `ls` command to display the files and sub-directory. The output of my command indicates that there is one directory named caesar, and two files; an encrypted file Q1.encrypted and a README.txt file that contain a guideline to decrypt the encrypted file.

Find a hidden file

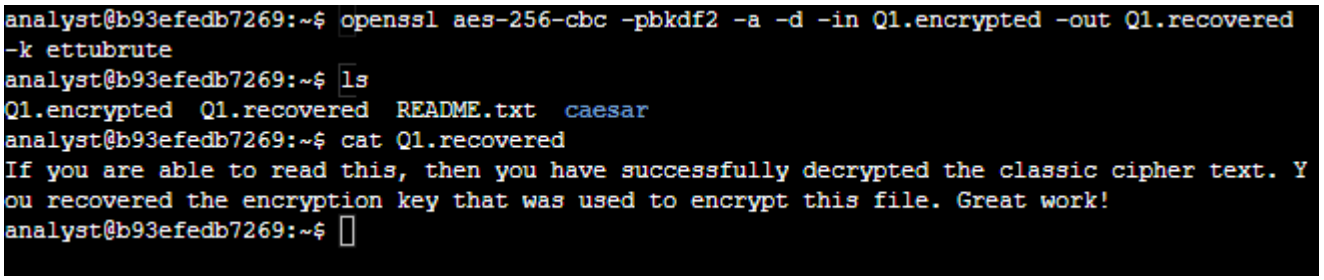
```
analyst@b93efedb7269:~$ cd caesar
analyst@b93efedb7269:~/caesar$ ls -a
.  ..  .leftShift3
analyst@b93efedb7269:~/caesar$ cat .leftShift3
Lq rughu wr uhfryhu brxu ilohv brx zloo qhhg wr hqwhu wkh iroorzlqj frppdqg:

rshqvvo dhv-256-fef -sengi2 -d -g -lq T1.hqfubswhg -rxw T1.uhfryhuhg -n hwwxeuxwh
analyst@b93efedb7269:~/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@b93efedb7269:~/caesar$ cd ~
analyst@b93efedb7269:~$
```

The first line of the screenshot displays the command I entered, and the other lines display the output prospectively. I used the `cd` command to navigate to caesar directory. I used the `ls` command with -a option to display the hidden file in the directory. The output of my command indicates that there is one hidden file named .leftShift3.

I used the cat command to read the file content and find out it was encrypted. I used the cat .leftShift3 | tr "d-za-cD-ZA-C" "a-zA-Z" caesar cipher code to decrypt the file. The output indicates that the file was decrypted and another decryption code was given which is openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute .

Note: 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".

Decrypt a file



The first line of the screenshot displays the command I entered, and the other lines display the output prospectively. I used the provided token openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute to decrypt Q1.encrypted file. The output indicates that the encrypted file has been decrypted as a result of a new file named Q1.recovered.

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.