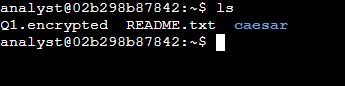
We start in our home directory, /home/analyst.

1. I used ls command to list the files in the current working directory.

Two files, Q1.encrypted and README.txt, and a subdirectory, caesar, are listed:



1. We then proceeded to use the cat command to list the contents of the README.txt file.

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

A black background with white text

Description automatically generated

**Finding a hidden file**

We now need to find a hidden file in our home directory and decrypt the Caesar cipher it contains.

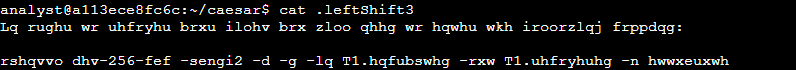
* First, I use the cd command to change to the caesar subdirectory of our home directory:
* I then proceeded to Use the ls -a command to list all files, including hidden files, in our home directory.

The following output is displayed:

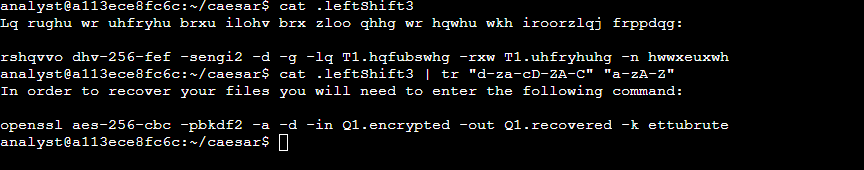


1. I then used the cat command to list the contents of the .leftShift3 file.

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".



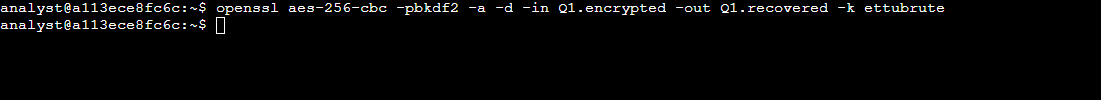
1. We can decrypt the Caesar cipher in the .leftshift3 file by using the following command:



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".

**Decrypting a file**

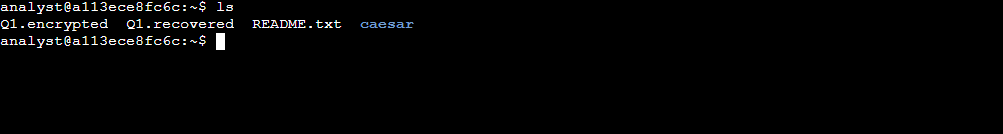
1. We then use the command revealed above to decrypt the encrypted file:



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.

1. We then use the ls command to list the contents of our current working directory again.

The new file Q1.recovered in the directory listing is the decrypted file and contains a message.



1. We then use the cat command to list the contents of the Q1.recovered file.

