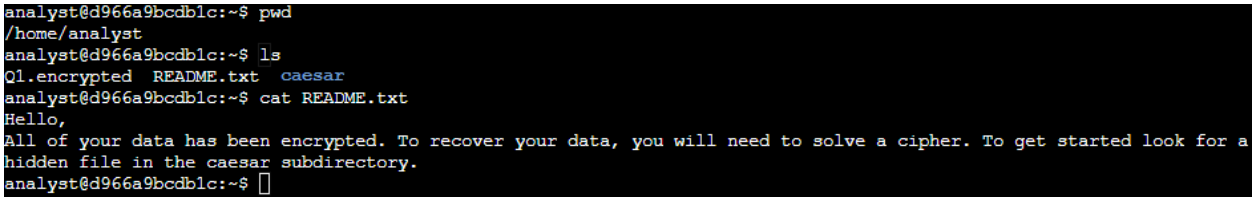
Add and manage users with Linux commands

Project description

All of the files in the 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.

Read the contents of a file



I used the `ls` command to list all files and directories in my current location (`/home/analyst`). The output showed three items:

- `Q1.encrypted` (an encrypted file)
- `README.txt` (a text file with instructions)
- `caesar` (a directory, possibly containing more files)

I used the `cat` command to display the contents of `README.txt`. This file contained a message stating that my data had been encrypted and that I needed to solve a cipher to recover it. It also hinted that a **hidden file** was inside the `caesar` subdirectory.

Find a hidden file

```
analyst@d966a9bcdb1c:~$ cd caesar/
analyst@d966a9bcdb1c:~/caesar$ ls -a
.  ..  .leftShift3
analyst@d966a9bcdb1c:~/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@d966a9bcdb1c:~/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@d966a9bcdb1c:~/caesar$ cd ~
analyst@d966a9bcdb1c:~$
```

I used `cd` (change directory) to move into the `caesar` directory since the `README.txt` file hinted that a hidden file was inside.
I listed all files in `caesar`, including hidden ones, using the `-a` flag. The output showed a hidden file called `.leftShift3`.
I used `cat` to display the contents of `.leftShift3`. The text was encoded using a **Caesar cipher** with a shift of 3 (each letter was shifted forward by 3 places).

I used the `tr` (translate) command to shift the text back by 3 places, converting it into readable English.

Decrypting an encrypted file.

```
analyst@d966a9bcdb1c:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute
analyst@d966a9bcdb1c:~$ ls
Q1.encrypted  Q1.recovered  README.txt  caesar
analyst@d966a9bcdb1c:~$ cat Q1.recovered
If you are able to read this, then you have successfully decrypted the classic cipher text. You recovered the encrypti
on key that was used to encrypt this file. Great work!
analyst@d966a9bcdb1c:~$
```

I used the `openssl` command to decrypt the file `Q1.encrypted`. Here's what each part of the command does:

- `openssl aes-256-cbc` Specifies the AES-256 encryption algorithm in CBC mode.
- `-pbkdf2` Uses a password-based key derivation function (PBKDF2) for added security.
- `-a` Tells OpenSSL that the input file is Base64 encoded.
- `-d` Specifies that I am **decrypting** the file.
- `-in Q1.encrypted` Sets `Q1.encrypted` as the input file.
- `-out Q1.recovered` Saves the decrypted output to `Q1.recovered.`
- `-k ettubrute` Uses `ettubrute` as the decryption password.

After running the decryption command, I listed the files in my home directory. I now see:

- `Q1.encrypted` (original encrypted file)
- `Q1.recovered` (newly decrypted file)
- `README.txt`
- `caesar` (directory)

This confirms that the decryption process successfully created `Q1.recovered.`

I used `cat` to read the contents of `Q1.recovered`. The message inside confirmed that I had successfully decrypted the classic cipher text and recovered the encryption key.

Summary

Listed the directory contents using `ls.` Read the `README.txt` file with `cat` to find encryption recovery instructions. Found the hidden file `.leftShift3` using `ls -a` and decoded its Caesar cipher with `tr`, revealing the decryption command. Used `openssl aes-256-cbc` to decrypt `Q1.encrypted` into `Q1.recovered`. Verified successful decryption by reading the recovered file with `cat`.