

Relatório sobre descoberta de arquivo encriptado

Cenário: Os arquivos e um determinado dispositivo estão encriptados. Sabe-se que um dos arquivos que está com as informações fora de ordem foi encriptado utilizando a cifra de César.

Os arquivos estão na página home do usuário “analyst”. Listando os arquivos da pasta, pode-se visualizar dois arquivos “Q1.encrypted” e “README.txt” e o diretório “caesar”.

```
analyst@7f27f596cddb:~$ ls
Q1.encrypted  README.txt  caesar
analyst@7f27f596cddb:~$ cat Q1.encrypted
U2FsdGVkX1/nxHZY2p53/6gRmQ9alkNrVwOwPOgpTeB09rdnvKnydLPQsnOYHjgR
42Mwdv0ye94Im+u100F12+Bx3SHjJ7wZjOxA7Jew1x7g3LcRsRnFcFLyfAnn0f3u
xMIH/y+Y4HfVb6NUFueXM43M5Cn/Gz9JqIxpw+tZaaJsrtZrsoEwenZEND1Ya6AY
rnVCjCFdTmSVG9EnzGxFT40DOW0yIhEAW5WqfBzjwgNSfz+p44Bnb3jUHsJt38gw
analyst@7f27f596cddb:~$
analyst@7f27f596cddb:~$ 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@7f27f596cddb:~$
```

Listando o conteúdo do arquivo Q1.encrypted, que como o nome já diz, está encriptado e não possui conteúdo que possa ser lido. Já o arquivo README.txt exibe a mensagem: Todos os seus dados foram encriptados. Para recuperá-los, você terá que resolver uma cifra. Para iniciar encontre o arquivo escondido no subdiretório caesar.

Acessando o subdiretório caesar, inicialmente não é possível visualizar nenhum arquivo, mas usando o comando ls -a que lista todos os arquivos da pasta até mesmo os que estão escondidos.

```
analyst@7f27f596cddb:~/caesar$ ls
analyst@7f27f596cddb:~/caesar$ ls -a
.  ..  .leftShift3
analyst@7f27f596cddb:~/caesar$
```

Acessando o conteúdo do arquivo .leftShift3 que estava escondido no diretório caesar, percebe-se que o conteúdo está criptografado com a cifra de César, o que impossibilita a leitura.

```
analyst@7f27f596cddb:~/caesar$ cat .leftShift3
Lq rughu wr uhfryhu brxu ilohv brx zloo qhhg wr hqwhu wkh iroorzlqj frppdgg:

rshqvvo dhv-256-fef -sengi2 -d -g -lq T1.hqfubswhg -rxw T1.uhfryhuhg -n hwwxeuxwh
analyst@7f27f596cddb:~/caesar$
```

A cifra de César é um algoritmo de encriptação que desloca as letras de lugar para encobrir mensagens. Usando a lógica do nome do arquivo que traduzindo é “deslocamento para esquerda 3”. É possível usar o comando “tr” do Linux para realizar essa troca de caracteres, os parâmetros desse comando é o caractere atual pelo caractere desejado. No caso desse arquivo, como são 3 caracteres à esquerda o caractere atual foi setado como d para ser iniciada a modificação a partir da letra d, isso possibilita a mudança para até 3 caracteres anteriores, exemplo: dado = aaao.

Nesse caso, os primeiros caracteres descritos e começados em d são traduzidos para caracteres começados em a, tanto em letra maiuscula quanto letra minúscula.

```
analyst@7f27f596cddb:~/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@7f27f596cddb:~/caesar$
```

Decifrando a mensagem encriptada pela cifra de César, foi possível ler o conteúdo do arquivo e nele é descrito um comando para decifrar o arquivo Q1.encrypted que está na pasta home.

Retornando a pasta home, é possível visualizar o arquivo Q1.encrypted novamente.

O comando que estava listado no conteúdo do arquivo .leftShift3 é possível encontrar o comando “ **openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute**” que indica que o arquivo está encriptado com o programa OpenSSL e usa a criptografia aes com de 256 “aes-256”, usando “cbc ” que indica o modo de operação Cipher Block Chaining. Usa a função “-pbkdf2” que significa password-based key derivation function 2, e é utilizado para derivar a chave a partir da senha fornecida. O parâmetro “-a” é usado para habilitar a codificação em Base64, ou seja, o arquivo cifrado pode ser representado em texto legível, o parâmetro “-d” indica a operação que está sendo realizada, nesse caso a descryptografia. Os

parâmetros seguintes são para o arquivo que será modificado e o outro especifica em qual arquivo que a saída do comando será anexado. O último parâmetro é a função “-k ettubroute” define a senha de descritografia como ettubroute.

Após usar o comando para descritografar o arquivo, e listando o conteúdo da pasta novamente, é possível ver o novo arquivo que foi indicado como saída. Q1.recovered.

```
analyst@7f27f596cddb:~$ ls
Q1.encrypted  README.txt  caesar
analyst@7f27f596cddb:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubroute^C
analyst@7f27f596cddb:~$ ls
Q1.encrypted  README.txt  caesar
analyst@7f27f596cddb:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubroute
analyst@7f27f596cddb:~$ ls
Q1.encrypted  Q1.recovered  README.txt  caesar
```

Ao acessar o conteúdo do arquivo, dá para visualizar o conteúdo do arquivo que estava encriptado.

```
analyst@7f27f596cddb:~$ 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!
analyst@7f27f596cddb:~$
```