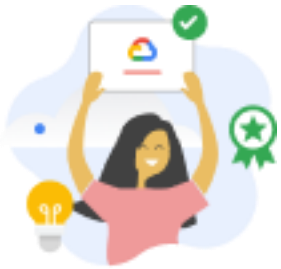
Activity - Decrypt an encrypted message

experimentLabschedule1 houruniversal_currency_altNo costshow_chartIntroductory

Lab instructions and tasks

- Activity overview
- Scenario
- Start your lab
- Task 1. Read the contents of a file
- Task 2. Find a hidden file
- Task 3. Decrypt a file
- Conclusion
- End your lab



This content is not yet optimized for mobile devices.
For the best experience, please visit us on a desktop computer using a link sent by email.

Activity overview

Previously, you learned about cryptography and how encryption and decryption can be used to secure information online. You were also introduced to the Caesar cipher, one of the earliest cryptographic algorithms used to protect people's privacy.

As a security analyst, it’s important that you understand the role of encryption to secure data online and that you’re familiar with the right security controls to do so.

In this lab activity, you’ll be guided through some basic cryptographic activities using Linux commands to decrypt files and reveal hidden messages.

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.

Here’s how you’ll do this task: **First**, you’ll explore the contents of the home directory and read the contents of a file. **Next**, you’ll find a hidden file and decrypt the Caesar cipher it contains. **Finally**, you’ll decrypt the encrypted data file to recover your data and reveal the hidden message.

OK, it's time to decrypt some messages in Linux!

Note: *The lab starts with you logged in as user* `analyst`*, with your home directory,* `/home/analyst`*, as the current working directory.***Disclaimer:** For optimal performance and compatibility, it is recommended to use either **Google Chrome** or **Mozilla Firefox**browsers while accessing the labs.

Start your lab

Before you begin, you can review the instructions for using the Qwiklabs platform under the **Resources** tab in Coursera.

If you haven't already done so, click **Start Lab**. This brings up the terminal so that you can begin completing the tasks!

When you have completed all the tasks, refer to the **End your Lab** section that follows the tasks for information on how to end your lab.

Task 1. Read the contents of a file

The lab starts in your home directory, `/home/analyst`, as the current working directory.

In this task, you need to explore the contents of your home directory and read the contents of a file to get further instructions.

1. Use the `ls` command to list the files in the current working directory.

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

```
Q1.encrypted  README.txt caesar
```

The `README.txt` file contains an important message with instructions you need to follow.

2. 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.

In the next task, you'll need to find the hidden file and solve the Caesar cipher that protects it. The file contains instructions on how to recover your data.

Click **Check my progress** to verify that you have completed this task correctly.

You have completed this task and discovered the encrypted files in your home directory.

Read the contents of a file

You have completed this task and discovered the encrypted files in your home directory.

Task 2. Find a hidden file

In this task, you need to find a hidden file in your home directory and decrypt the Caesar cipher it contains. This task will enable you to complete the next task.

1. First, use the `cd` command to change to the `caesar` subdirectory of your home directory:

```
cd caesar
```

Copied!

2. Use the `ls -a` command to list all files, including hidden files, in your home directory. This will display the following output:

```
.  ..  .leftShift3
```

Hidden files in Linux can be identified by their name starting with a period (.).

3. Use 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".

4. You can decrypt the Caesar cipher in the `.leftshift3` file by using the following command:

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

Copied!

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".*

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"`.

Note: *The output provides you with the command you need to solve the next task!*
You don't need to copy the command revealed in the output. It will be provided in the next task.

5. Now, return to your home directory before completing the next task:

```
cd ~
```

Copied!

Click **Check my progress** to verify that you have completed this task correctly.

You have completed this task.You identified the hidden file in your home directory and decrypted the Caesar cipher contained in the hidden file.

Find a hidden file

You have completed this task.You identified the hidden file in your home directory and decrypted the Caesar cipher contained in the hidden file.

Task 3. Decrypt a file

Now that you have solved the Caesar cipher, in this task you need to use the command revealed in `.leftshift3` to decrypt a file and recover your data so you can read the message it contains.

1. Use the exact command revealed in the previous task to decrypt the encrypted file:

```
openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -kettubrute
```

Copied!

Although you don't need to memorize this command, to help you better understand the syntax used, let's break it down.

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`.

2. Use the `ls` command to list the contents of your current working directory again. The new file `Q1.recovered` in the directory listing is the decrypted file and contains a message.

3. Use the `cat` command to list the contents of the `Q1.recovered`file.

Click **Check my progress** to verify that you have completed this task correctly.

You have completed this task by decrypting the Q1.encrypted file, recovering your data, and reading the message in the Q1.recovered file.

Decrypt a file

You have completed this task by decrypting the Q1.encrypted file, recovering your data, and reading the message in the Q1.recovered file.

Conclusion

Great work! You now have practical experience in using basic Linux Bash shell commands to

- list hidden files,
- decrypt a Caesar cipher, and
- decrypt an encrypted file.

This is an important milestone on your journey towards understanding encryption and decryption.

analyst@3354023ff175:~$ pwd

/home/analyst

analyst@3354023ff175:~$ ls -al

total 40

drwxr-xr-x 3 analyst analyst 4096 May 9 02:02 .

drwxr-xr-x 1 root   root   4096 May 9 01:27 ..

-rw------- 1 analyst analyst   10 May 9 02:03 .bash_history

-rw-r--r-- 1 analyst analyst 220 Apr 18 2019 .bash_logout

-rw-r--r-- 1 analyst analyst 3574 May 9 01:27 .bashrc

-rw-r--r-- 1 analyst analyst 3574 May 9 01:27 .profile

-rw-r--r-- 1 root   root   260 May 9 01:27 Q1.encrypted

-rw-r--r-- 1 root   root   165 May 9 01:27 README.txt

drwxr-xr-x 2 root   root   4096 May 9 01:27 caesar

analyst@3354023ff175:~$ cat R*

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@3354023ff175:~$

analyst@3354023ff175:~$ 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@3354023ff175:~$ cd caesar

analyst@3354023ff175:~/caesar$ ls -al

total 12

drwxr-xr-x 2 root   root   4096 May 9 01:27 .

drwxr-xr-x 3 analyst analyst 4096 May 9 02:02 ..

-rw-r--r-- 1 root   root   160 May 9 01:27 .leftShift3

analyst@3354023ff175:~/caesar$ cat .l*

Lq rughu wr uhfryhu brxu ilohv brx zloo qhhg wr hqwhu wkh iroorz

```
analyst@3354023ff175:~$ history
    1  clear
    2  pwd
    3  ls -al
    4  cat R*
    5  cat README.txt
    6  cd caesar
    7  ls -al
    8  cat .l*
    9  cat .leftShift3 | tr "d-za-cD-ZA-C" "a-zA-Z"
   10  cd ~
   11  ls -al
   12  cat -al
   13  cat Q*
   14  openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute
   15  ls -al
   16  clear
   17  history
analyst@3354023ff175:~$ cat Q1.encrypted
U2FsdGVkX1/nxHZY2p53/6gRmQ9alkNrVwOwPOgpTeB09rdnvKnydLPQsnOYHjgR
42Mwdv0ye94Im+u100Fl2+Bx3SHjJ7wZjOxA7Jew1x7g3LcRsRnFcFLyfAnn0f3u
xMIH/y+Y4HfVb6NUFueXM43M5Cn/Gz9JqIxpw+tZaajsrtZrsoEwenZEND1Ya6AY
rnVCjCFdTmSVG9EnzGxFT40DOw0yIhEAw5WqfBzjwgNSfz+p44Bnb3jUHsJt38gw
analyst@3354023ff175:~$ 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@3354023ff175:~$