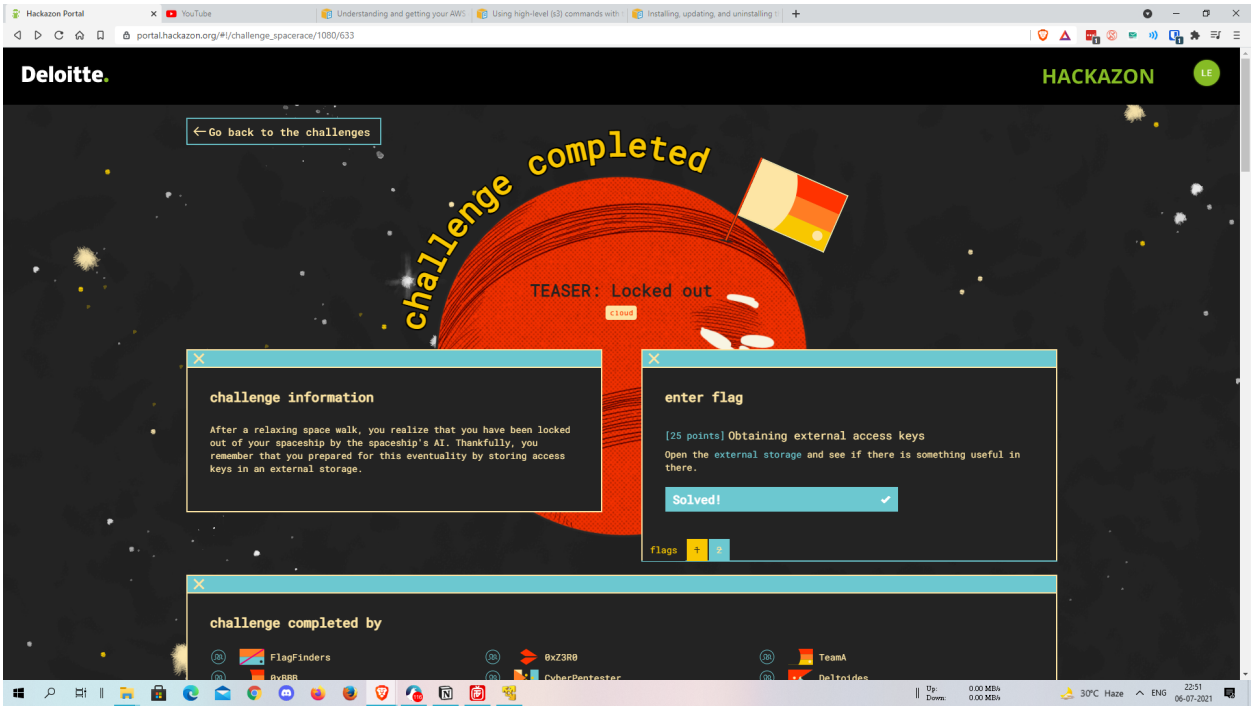
TEASER: Locked out

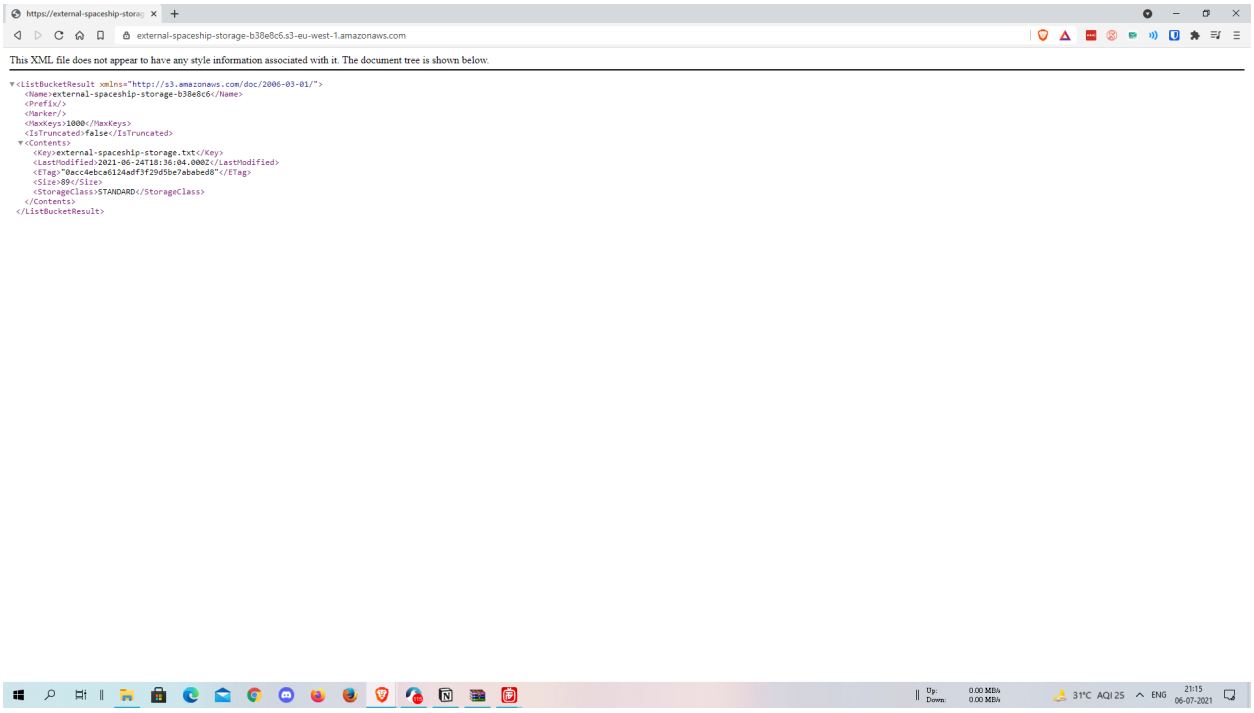
1> Obtaining external access keys

Open the external storage and see if there is something useful in there.



- Points :- [25 points]
- We are provided with the following Link When clicked on the link we get a standard xml output it also lists the content of the AWS bucket it has the external-spaceship-storage.txt file.
- Link

```
https://external-spaceship-storage-b38e8c6.s3.eu-west-1.amazonaws.com/external-spaceship-storage.txt
```



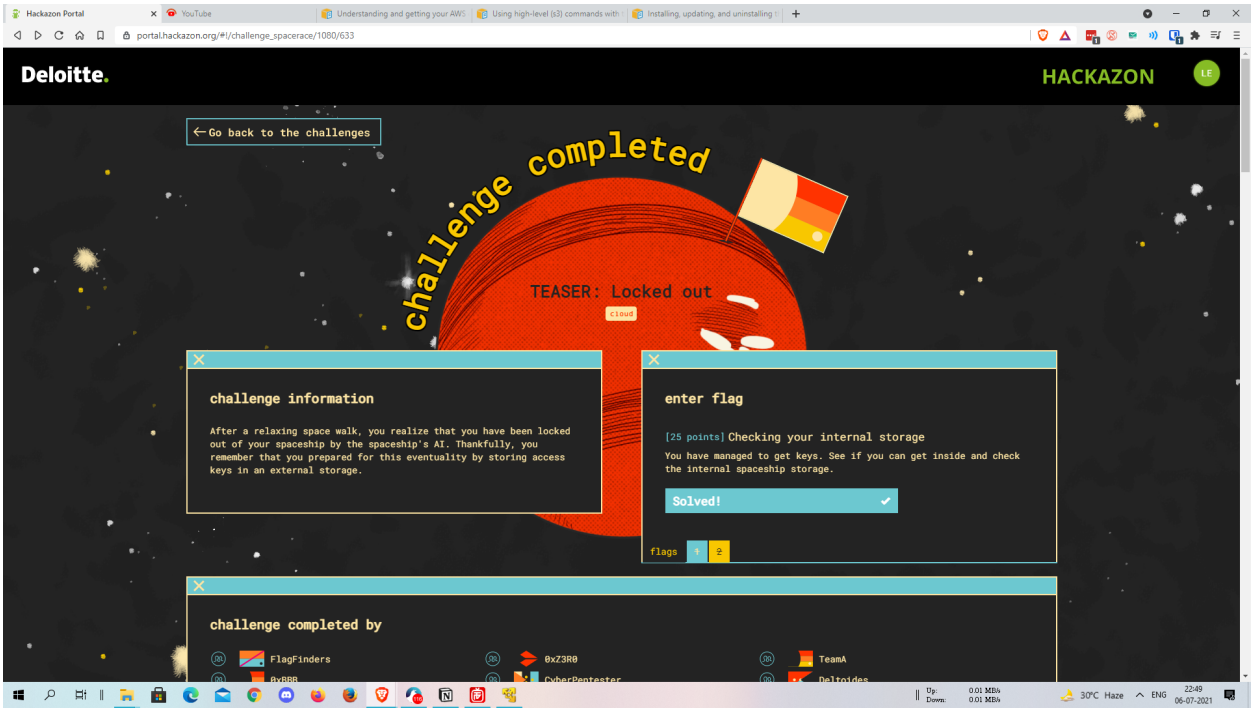
- So I added the endpoint external-spaceship-storage.txt to the link provided in order to get the file.
- The new link that I made allows me to download the external-spaceship-storage.txt file which contains the First flag and also the AWS Bucket Access key ID and secret access key.

```
https://external-spaceship-storage-b38e8c6.s3-eu-west-1.amazonaws.com/external-spaceship-storage.txt
```

- Flag1 :- CTF{6c2c45330a85b126f551}

2> Checking your internal storage

You have managed to get the keys. See if you can get inside and check the internal spaceship storage.



Points :- [25 points]

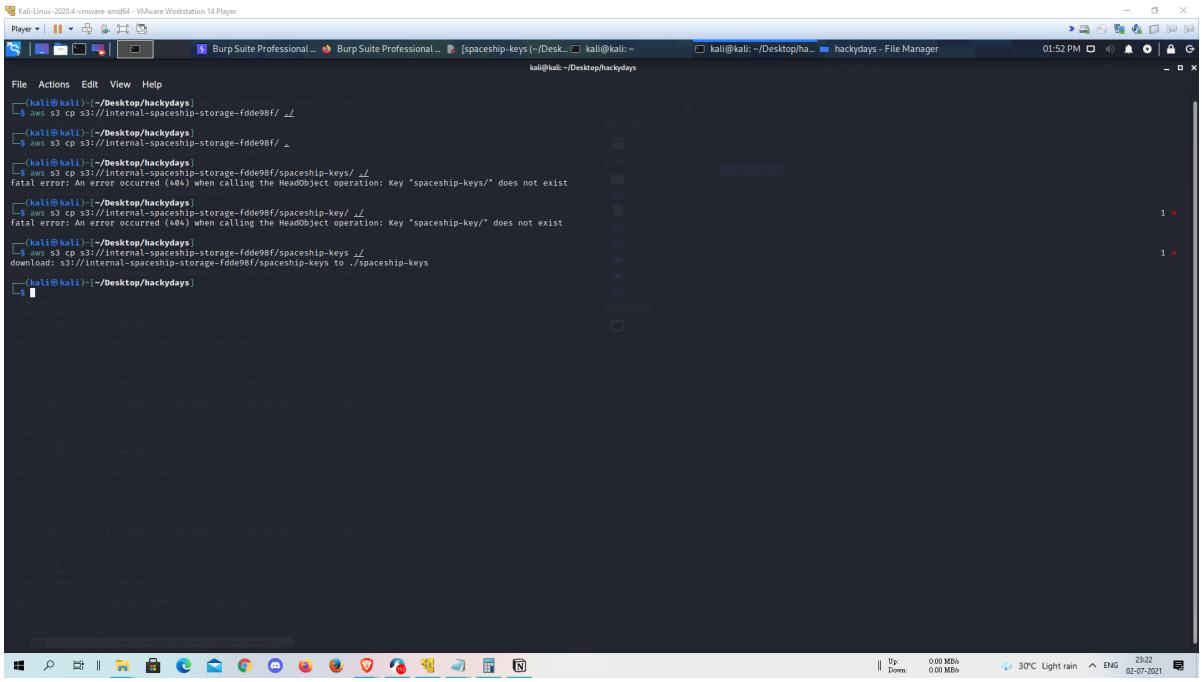
We have already retrieved some information from the earlier challenge we have to use this get access to internal spaceship storage

Access Key ID: AKIAQD6AU4VDTDJRGXRE
Secret Access Key: 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

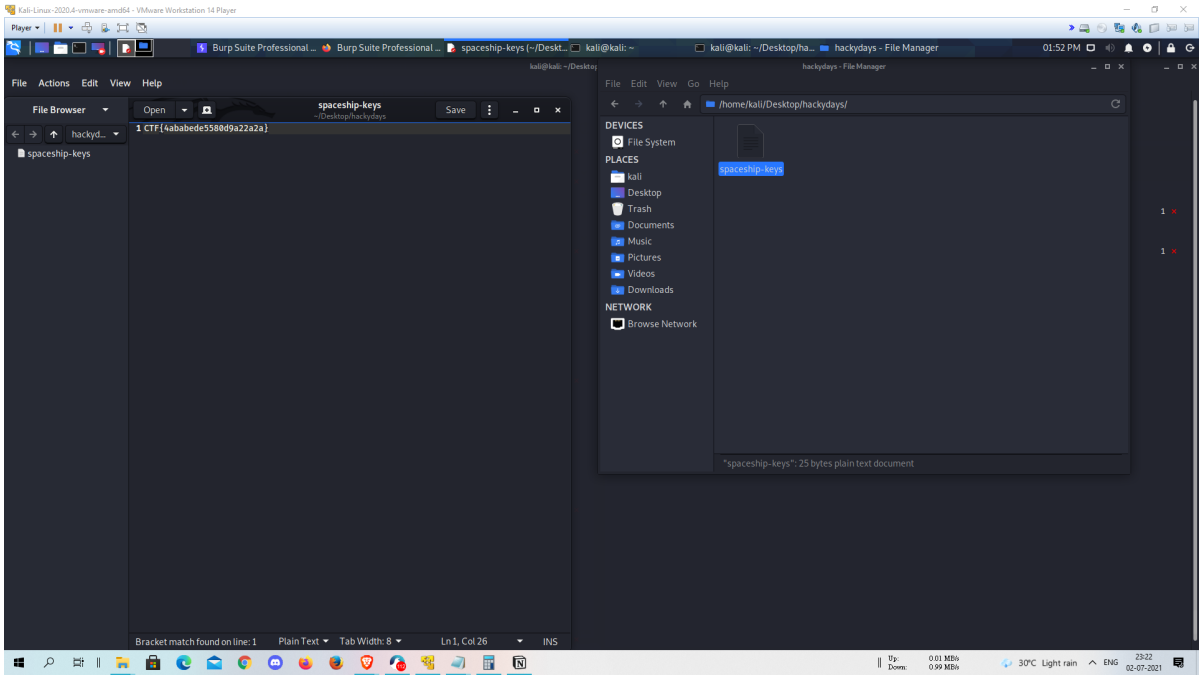
- So I searched how to use these access keys to get access to the bucket, the article below gave me information on configuring credentials in AWS cli and using them.

```
https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html
```

- I was able to guess that internal storage would also have a bucket name with internal-spaceship-storage and some bucket id which I didn't know and also bruteforcing it will take a lot of time and resources so I knew I had to find the bucket name first.
- Now I found out that since the access keys belong to an AWS instance when we enter aws s3 ls command it will list all the buckets in that instance and that's how I found out the internal-spaceship-storage-fdde98f bucket, then performed another ls on it and found out a folder named spaceship-keys copied it's content to my machine using the command aws s3 cp s3://internal-spaceship-storage-fdde98f/spaceship-keys.



- The file downloaded had the Key



Flag2 :- CTF{4ababede5580d9a22a2a}

- Reference links of all the AWS documentation used

- Aws cli command usage

```
https://docs.aws.amazon.com/cli/latest/userguide/cli-services-s3-commands.html
```

- Configuring AWS key to your cli

```
https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html
```

- Installation of AWS cli

```
https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2-linux.html
```