Exploiting S3 unauthenticated

@mmar

FLAWS.CLOUD –CHALLENGE-1

Amazon S3 bucket is a user-friendly object repository, that is used for storing and recovering various data from anywhere on the web. Misconfigurations in S3 result in exposing private data or even complete compromise of websites in some cases

Flaws.cloud Challenge1

✓ **Bucket's listing has it's listing permission set to "Everyone"**

ATTACK Scenarios

- ✓ A public Bucket that is used to host files for websites may have been misconfigured to allow write/ delete access instead of read-only access
- ✓ A private bucket that should have been configured to allow only authenticated access may have been misconfigured to allow public unauthenticated access

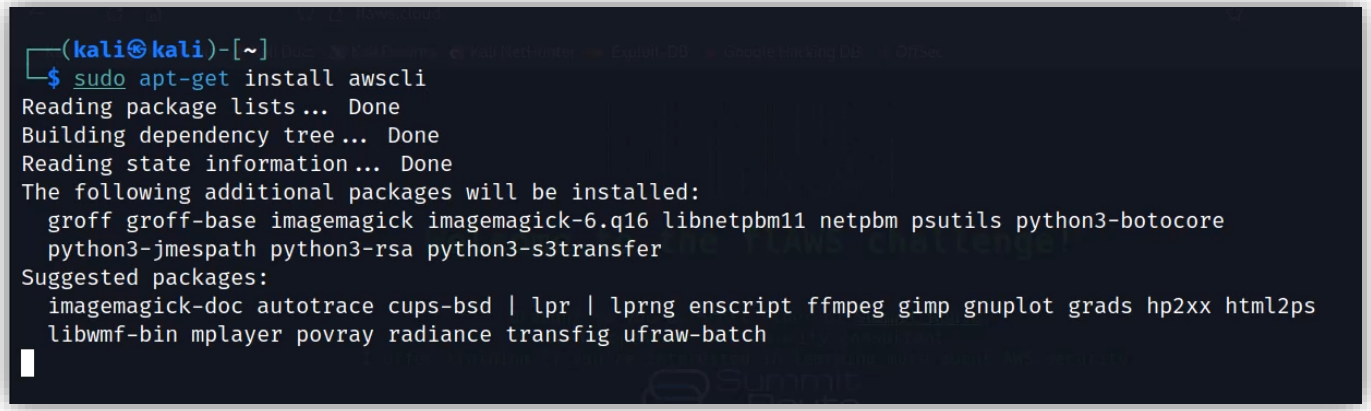
We will use a free cloud exploitation environment for our demo
Http://flaws.cloud

INSTALLING AWS CLI

Install AWS CLI

- Update your Kali Repositories and then download aws cli

- Sudo apt install update
- Sudo ap-get install awscli



Cloud_enum

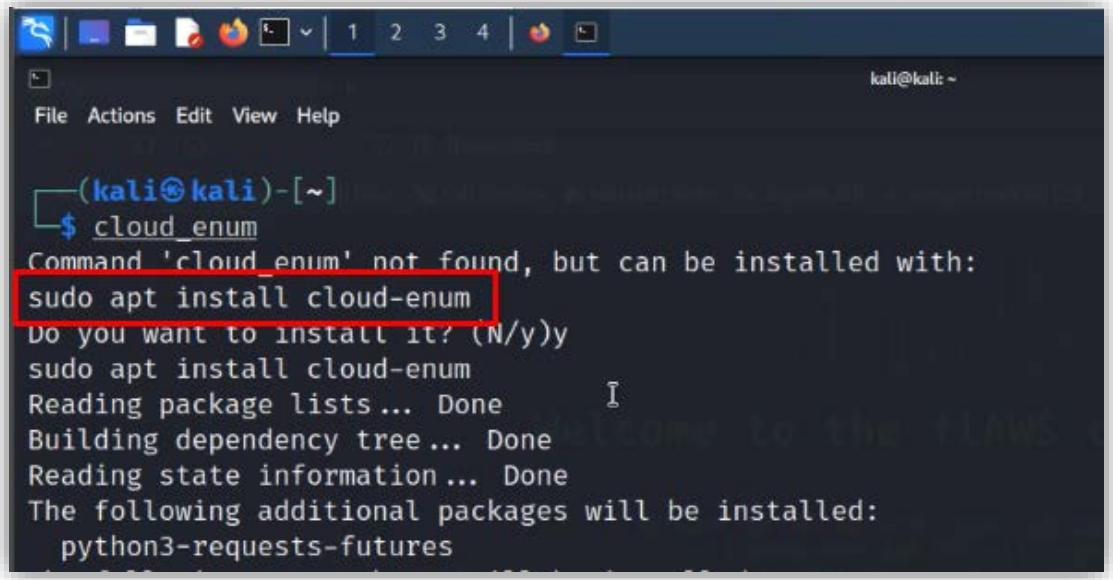
(Python Script – prebuilt in kali)

Allows to search for public S3 buckets and also list their contents

Cloud enum

- You can install the tool from Kali repositories with following command

Sudo apt install cloud-enum



Cloud enum

- Use the cloud_enum tool to find and list down the contents of the buckets

```
cloud_enum -k flaws.cloud --disable-azure --disable-gcp
```

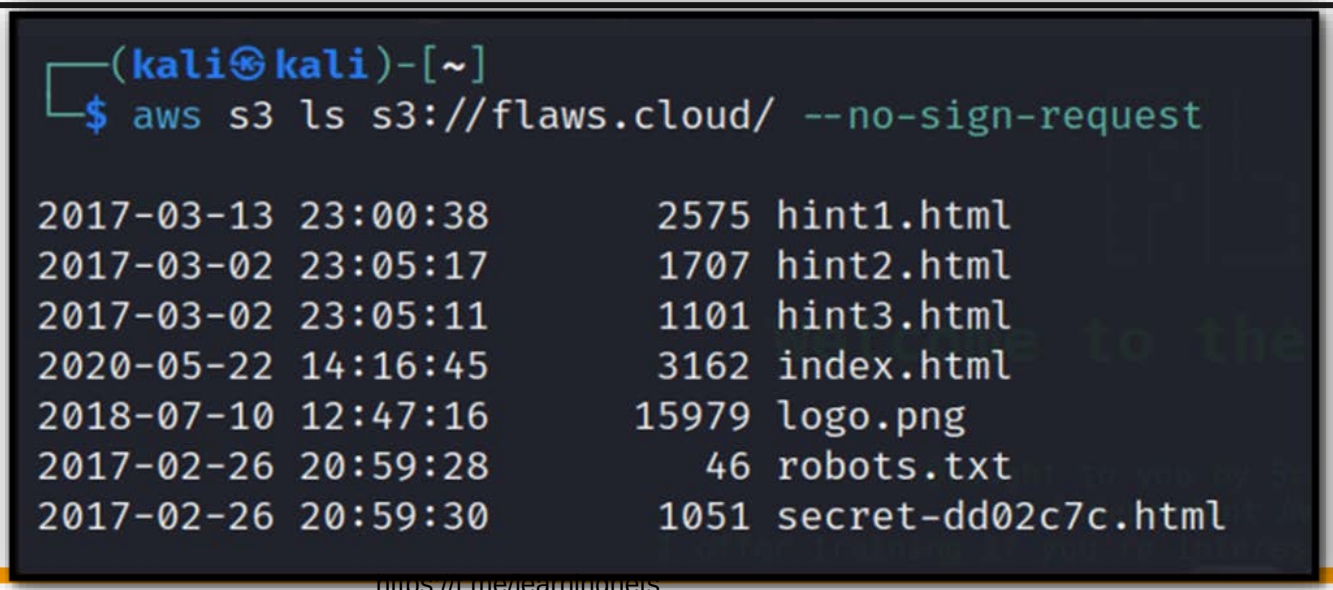
AWS CLI

Enumerating AWS S3 Buckets

Aws cli

- The contents of a bucket that allows unauthenticated access can be listed down with the following command

```
aws s3 ls s3://flaw.cloud/ --no-sign-request
```



Download contents

- We can use aws cli to download the contents of a bucket

```
aws s3 cp s3://flaws.cloud/secret-dd02c7c.html . --no-sign-request
```

Upload contents

- If the AWS bucket allows write access, we can upload a file to AWS and can also overwrite the existing files which may result in the defacement of a public website

```
aws s3 cp ./index.html s3://flaws.cloud --no-sign-request
```

DEMO

THANKS