

- Filename: intro-to-aws-pentesting-3-2-1-flaws-level-2.md
- Show Name: Intro to AWS Pentesting
- Topic Name: Flaws
- Episode Name: Flaws: Level 2

Flaws: Level 2

Objectives:

- Utilize cloud pentesting techniques specific to AWS environments to complete the Flaws Level 2 challenge
- Utilize the awscli to enumerate sensitive information from an open S3 bucket

-
- Let's see if we can figure out what we're working with

- `nslookup level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud`
- `nslookup 52.92.210.163`

- Looks like another s3 bucket

- Let's see if we can list bucket contents

- `aws s3 ls level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud`

- Access Denied!

- Try the `--no-sign-request` option

- Still denied

- Are we done? NOPE!

- s3 permissions can get a bit tricky

- IAM policy attached to IAM users
- IAM policy attached to the bucket
- S3 ACLs

- Bucket ACLs
- Object ACLs

- <https://docs.aws.amazon.com/AmazonS3/latest/userguide/acl-overview.html#acl-access-policy-permission-mapping>
- Can set ACLs on specific accounts or predefined groups

- All Users
- Authenticated Users

- Guess what "Authenticated Users" means in this context ;)

- Mistakes are likely

- So how do we access the objects in this bucket?

- We need a user with S3 permissions

- Create a user with "AmazonS3FullAccess" permissions

- Add S3user keys profile to awscli

- `aws configure --profile S3user`

- Now to view bucket objects

- `aws --profile S3user s3 ls s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud`

- or

- `aws --profile S3user s3api list-objects-v2 --bucket level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud`

- The item **secret-e4443fc.html** looks interesting

- View in the browser

- View with `awscli`

- `aws --profile S3user s3 cp s3://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud/secret-e4443fc.html .`

- `cat secret-e4443fc.html`

- Hey, Look! A link to the next level!