

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

Flaws: Level 3

Objectives:

- Utilize cloud pentesting techniques specific to AWS environments to complete the Flaws Level 3 challenge
- Utilize the awscli and git to enumerate sensitive information from an open S3 bucket

-
- Start with nslookup
 - Do `aws s3 ls s3://level3...flaw.cloud`
 - Access key id does not exist
 - Add `--no-sign-request`
 - Notice there is a `.git/` directory
 - Sync the bucket
 - `aws s3 sync s3://level3...flaws.cloud . --no-sign-request`
 - Let's do some `.git` enumeration
 - `git diff`
 - May reveal sensitive info
 - `git log`
 - Let's us look at previous versions
 - May reveal sensitive info
 - `tig`
 - `apt install tig (kali)`
 - Now that we have keys, what do we do with them?
 - Make a profile of course!
 - `aws configure --profile level3`
 - Now that we have a profile, what do we do with it?
 - Let's see if we can list ALL the s3 buckets
 - `aws --profile level3 s3 ls`
 - Yay! We found the bucket/subdomain for level4!