

- Filename: intro-to-aws-pentesting-3-5-1-flaws-level-5.md
- Show Name: Intro to AWS Pentesting
- Topic Name: Flaws
- Episode Name: Flaws: Level 5

Flaws: Level 5

Objectives:

- Utilize cloud pentesting techniques specific to AWS environments to complete the Flaws Level 5 challenge
 - Utilize the awscli and a web browser to discover and exploit in the EC2 Instance Metadata Service which allows for an SSRF attack
-
- Here we have another EC2 instance, but we are told and can see by the URLs that there is an HTTP proxy. What does this tell us about the target?
 - Could be vulnerable to SSRF
 - SSRF to access the Instance Metadata Service
 - What is the IMDS?
 - <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>
 - Basically, it's info about the instance
 - Host Names
 - Security Groups
 - User data
 - It's only accessible from within the instance itself
 - Can we access this metadata?
 - Yes, with SSRF
 - This brings us back to our proxy.
 - We see the use of a proxy or a file query and we might be able to do SSRF
 - <http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/flaws.cloud/>
 - You may see this like this as well
 - <http://4d0cf...6f3b.flaws.cloud/?proxy=somesite.com>
 - Look for anything that might be a File Inclusion
 - So, how do we access the instance metadata using the proxy?
 - You just need to know the metadata service structure
 - <http://169.254.169.254/latest/>
 - We plug that in as our request through the proxy
 - <http://4d0cf...6f3b.flaws.cloud/proxy/169.254.169.254/latest>
 - The sky is the limit from here
 - So what should we do with this access?
 - Let's see if we can find any keys
 - <http://4d0cf...6f3b.flaws.cloud/proxy/169.254.169.254/latest/meta-data/iam/security-credentials>
 - Drill down further to the *flaws* user
 - Jackpot!
 - Now that we have keys for this user, what do we do?
 - We're told there is an s3 bucket we need to kick

- <http://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud>
 - And then it has a hidden directory in it
- So we should enumerate the s3 bucket with the same tactics as before?
 - Couldn't hurt :)
 - Make a profile with the level5 creds
 - `aws configure --profile flaws-l5`
 - Now go after that s3 bucket
 - `aws --profile flaws-l5 s3 ls s3://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud`
 - Browse to the hidden directory.
 - <http://level6-cc4c404a8a8b876167f5e70a7d8c9880.flaws.cloud/ddcc78ff>
 - And there's the link to Level 6