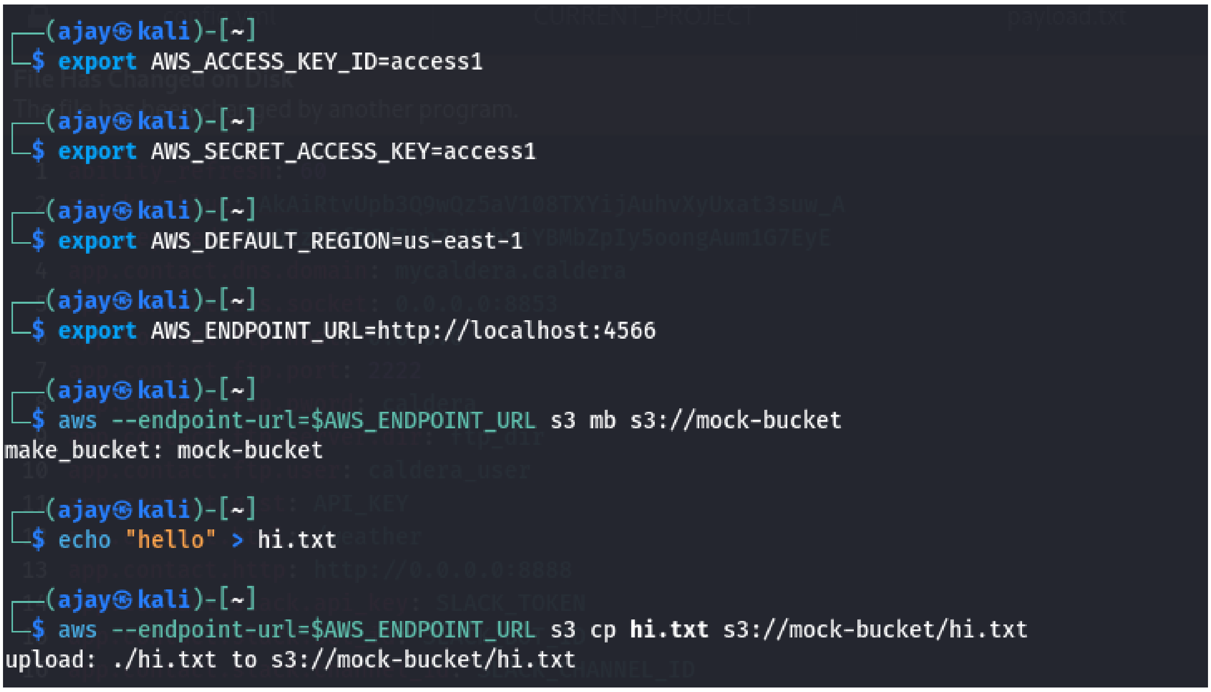
Capstone Report

Executive Summary

This capstone project demonstrates a full adversary simulation using LocalStack as a mockAWS environment and Pacu as the red team tool. The goal was to simulate various attacktechniques such as reconnaissance, exploitation, privilege escalation, persistence, andexfiltration in a controlled environment. This report includes all the commands executedduring the setup, resource creation, and exploitation phases, along with recommendations forblue team defenses.

Setup and Resource Creation in LocalStack

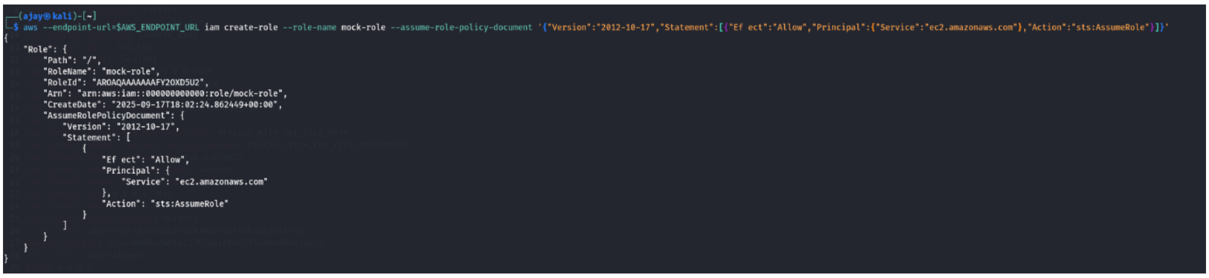
export AWS_ACCESS_KEY_ID=access1
export AWS_SECRET_ACCESS_KEY=access1
export AWS_DEFAULT_REGION=us-east-1
export AWS_ENDPOINT_URL=http://localhost:4566



```
┌──(ajay㉿kali)-[~]
└─$ export AWS_ACCESS_KEY_ID=access1

┌──(ajay㉿kali)-[~]
└─$ export AWS_SECRET_ACCESS_KEY=access1

┌──(ajay㉿kali)-[~]
└─$ export AWS_DEFAULT_REGION=us-east-1

┌──(ajay㉿kali)-[~]
└─$ export AWS_ENDPOINT_URL=http://localhost:4566

┌──(ajay㉿kali)-[~]
└─$ aws --endpoint-url=$AWS_ENDPOINT_URL s3 mb s3://mock-bucket
make_bucket: mock-bucket

┌──(ajay㉿kali)-[~]
└─$ echo "hello" > hi.txt

┌──(ajay㉿kali)-[~]
└─$ aws --endpoint-url=$AWS_ENDPOINT_URL s3 cp hi.txt s3://mock-bucket/hi.txt
upload: ./hi.txt to s3://mock-bucket/hi.txt
```

Fig 1.1

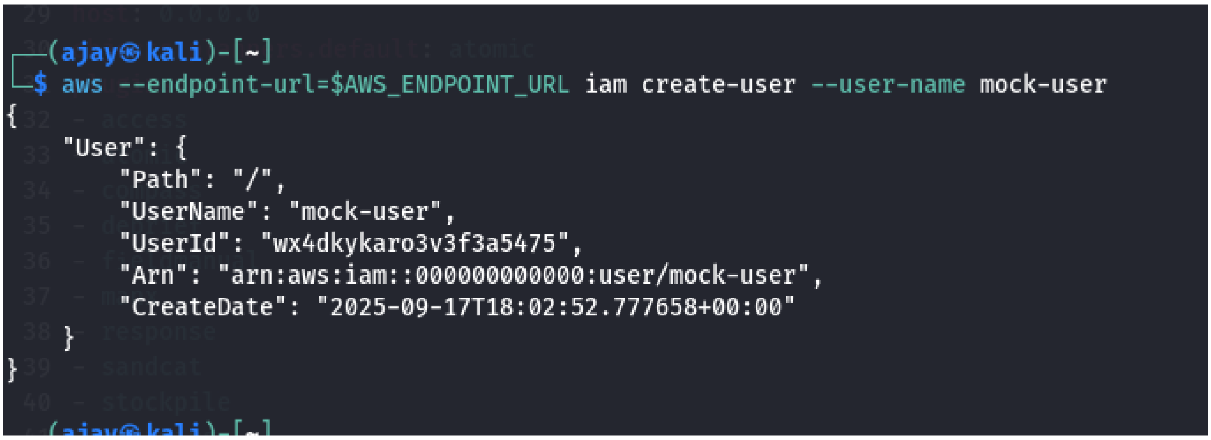
Create an S3 bucket and upload a dummy file



```
┌──(ajay㉿kali)-[~]
└─$ aws --endpoint-url=$AWS_ENDPOINT_URL iam create-role --role-name mock-role --assume-role-policy-document '{"Version":"2012-10-17","Statement":[{"Ef ect":"Allow","Principal":{"Service":"ec2.amazonaws.com"},"Action":"sts:AssumeRole"}]}'
{
    "Role": {
        "Path": "/",
        "RoleName": "mock-role",
        "RoleId": "AROAQAAAAAAAFY2OXD5U2",
        "Arn": "arn:aws:iam::000000000000:role/mock-role",
        "CreateDate": "2025-09-17T18:02:24.862449+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Ef ect": "Allow",
                    "Principal": {
                        "Service": "ec2.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Fig 1.2

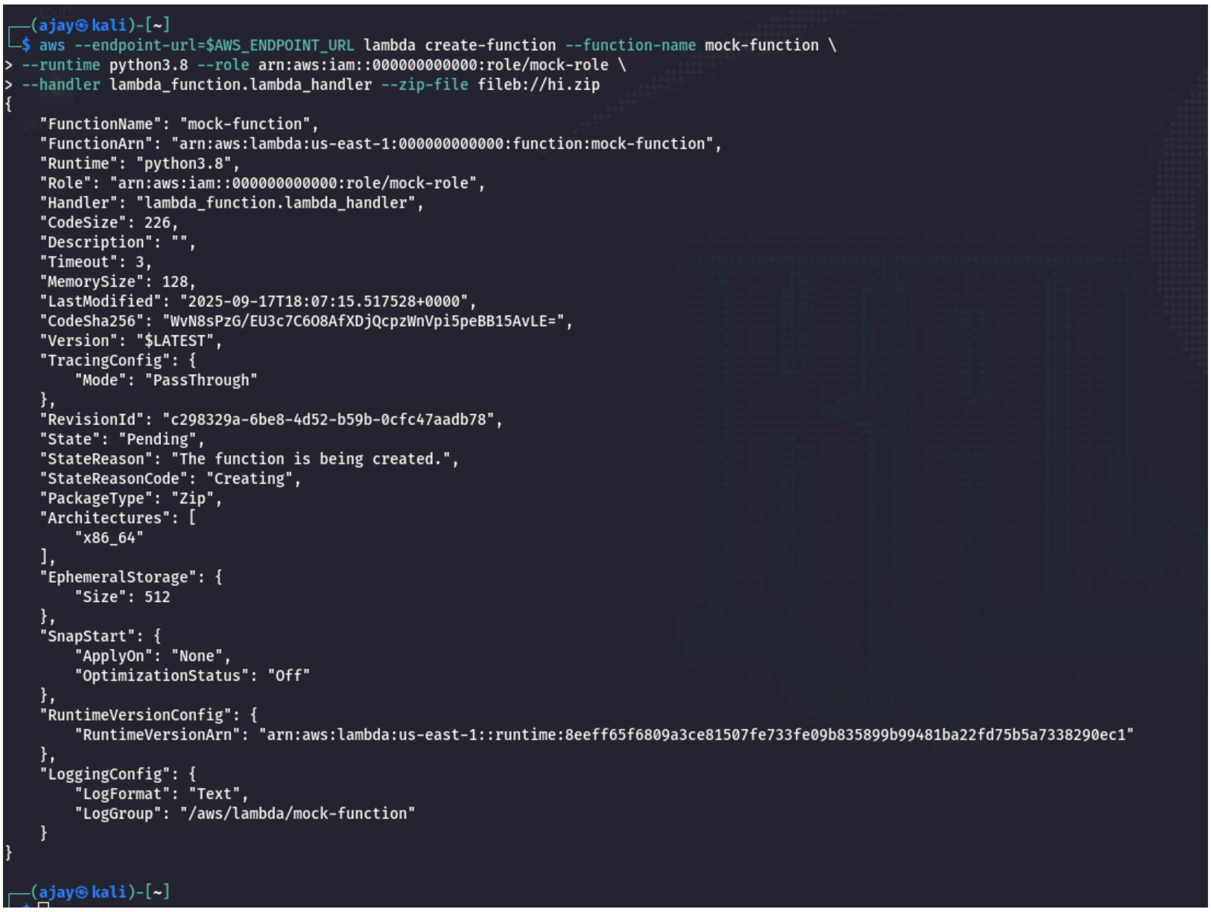
Create IAM role and user



```
┌──(ajay㉿kali)-[~]
└─$ aws --endpoint-url=$AWS_ENDPOINT_URL iam create-user --user-name mock-user
{
    "User": {
        "Path": "/",
        "UserName": "mock-user",
        "UserId": "wx4dkykaro3v3f3a5475",
        "Arn": "arn:aws:iam::000000000000:user/mock-user",
        "CreateDate": "2025-09-17T18:02:52.777658+00:00"
    }
}
┌──(ajay㉿kali)-[~]
```

Fig 1.3 IAM role and user

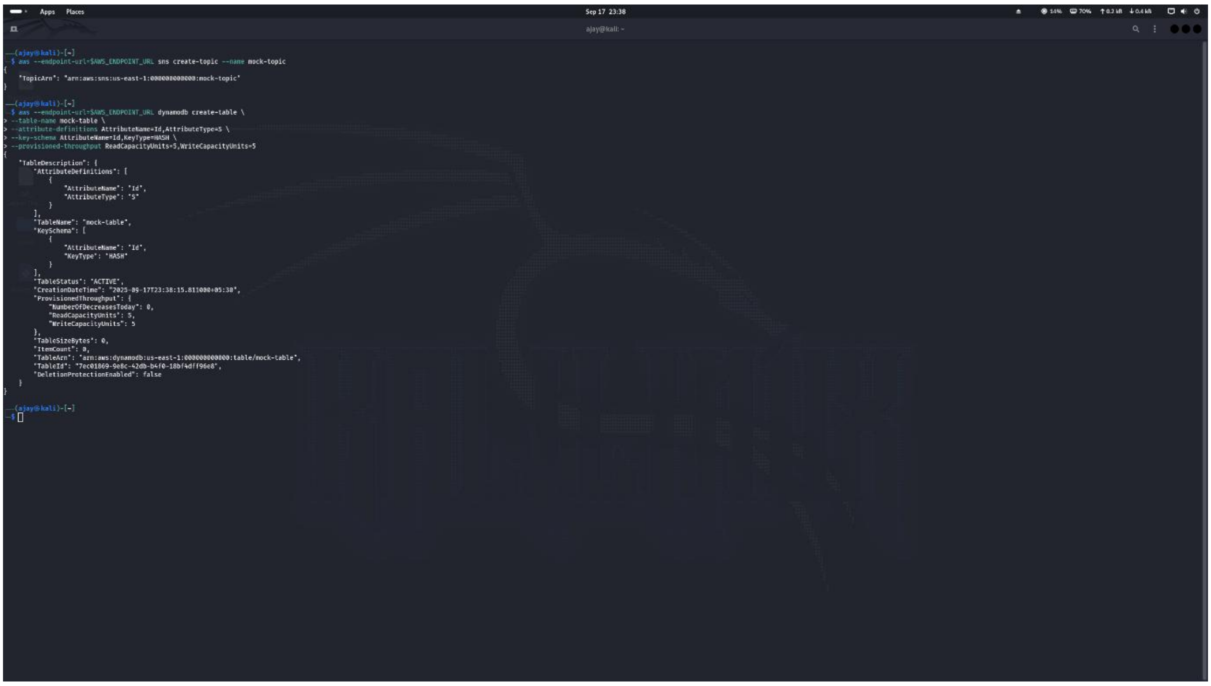
Create Lambda function



```
┌──(ajay㉿kali)-[~]
└─$ aws --endpoint-url=$AWS_ENDPOINT_URL lambda create-function --function-name mock-function \
> --runtime python3.8 --role arn:aws:iam::000000000000:role/mock-role \
> --handler lambda_function.lambda_handler --zip-file fileb://hi.zip
{
    "FunctionName": "mock-function",
    "FunctionArn": "arn:aws:lambda:us-east-1:000000000000:function:mock-function",
    "Runtime": "python3.8",
    "Role": "arn:aws:iam::000000000000:role/mock-role",
    "Handler": "lambda_function.lambda_handler",
    "CodeSize": 226,
    "Description": "",
    "Timeout": 3,
    "MemorySize": 128,
    "LastModified": "2025-09-17T18:07:15.517528+0000",
    "CodeSha256": "WvN8sPzG/EU3c7C6O8AfXDjQcpzWnVpi5peBB15AvLE=",
    "Version": "$LATEST",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "RevisionId": "c298329a-6be8-4d52-b59b-0cfc47aadb78",
    "State": "Pending",
    "StateReason": "The function is being created.",
    "StateReasonCode": "Creating",
    "PackageType": "Zip",
    "Architectures": [
        "x86_64"
    ],
    "EphemeralStorage": {
        "Size": 512
    },
    "SnapStart": {
        "ApplyOn": "None",
        "OptimizationStatus": "Off"
    },
    "RuntimeVersionConfig": {
        "RuntimeVersionArn": "arn:aws:lambda:us-east-1::runtime:8eeff65f6809a3ce81507fe733fe09b835899b99481ba22fd75b5a7338290ec1"
    },
    "LoggingConfig": {
        "LogFormat": "Text",
        "LogGroup": "/aws/lambda/mock-function"
    }
}

┌──(ajay㉿kali)-[~]
```

Fig 1.4

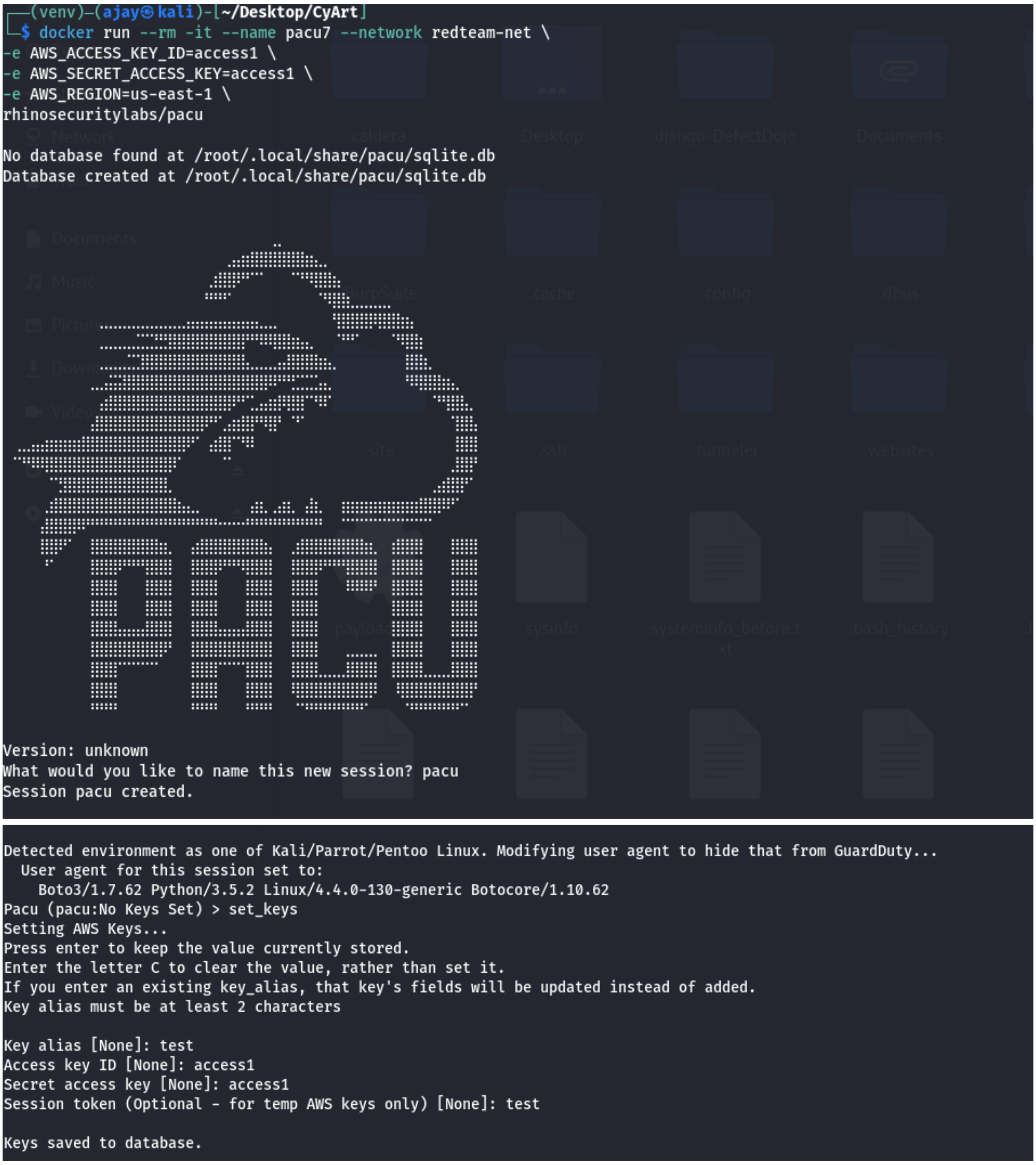
Create SNS topic



```
┌──(ajay㉿kali)-[~]
└─$ aws --endpoint-url=$AWS_ENDPOINT_URL sns create-topic --name mock-topic
{
    "TopicArn": "arn:aws:sns:us-east-1:000000000000:mock-topic"
}

┌──(ajay㉿kali)-[~]
└─$ aws --endpoint-url=$AWS_ENDPOINT_URL dynamodb create-table \
> --table-name mock-table \
> --attribute-definitions AttributeName=Id,AttributeType=S \
> --key-schema AttributeName=Id,KeyType=HASH \
> --provisioned-throughput ReadCapacityUnits=5,WriteCapacityUnits=5
{
    "TableDescription": {
        "AttributeDefinitions": [
            {
                "AttributeName": "Id",
                "AttributeType": "S"
            }
        ],
        "TableName": "mock-table",
        "KeySchema": [
            {
                "AttributeName": "Id",
                "KeyType": "HASH"
            }
        ],
        "TableStatus": "ACTIVE",
        "CreationDateTime": "2025-09-17T23:38:15.811000+05:30",
        "ProvisionedThroughput": {
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 5,
            "WriteCapacityUnits": 5
        },
        "TableSizeBytes": 0,
        "ItemCount": 0,
        "TableArn": "arn:aws:dynamodb:us-east-1:000000000000:table/mock-table",
        "TableId": "7ec01869-9e8c-42db-b4f0-18bf4dff96e8",
        "DeletionProtectionEnabled": false
    }
}

┌──(ajay㉿kali)-[~]
└─$ 
```

Fig 1.5

Pacu Commands Executed



```
┌──(venv)─(ajay㉿kali)-[~/Desktop/CyArt]
└─$ docker run --rm -it --name pacu7 --network redteam-net \
-e AWS_ACCESS_KEY_ID=access1 \
-e AWS_SECRET_ACCESS_KEY=access1 \
-e AWS_REGION=us-east-1 \
rhinosecuritylabs/pacu

No database found at /root/.local/share/pacu/sqlite.db
Database created at /root/.local/share/pacu/sqlite.db

Version: unknown
What would you like to name this new session? pacu
Session pacu created.
```

```
Detected environment as one of Kali/Parrot/Pentoo Linux. Modifying user agent to hide that from GuardDuty...
  User agent for this session set to:
    Boto3/1.7.62 Python/3.5.2 Linux/4.4.0-130-generic Botocore/1.10.62
Pacu (pacu:No Keys Set) > set_keys
Setting AWS Keys...
Press enter to keep the value currently stored.
Enter the letter C to clear the value, rather than set it.
If you enter an existing key_alias, that key's fields will be updated instead of added.
Key alias must be at least 2 characters

Key alias [None]: test
Access key ID [None]: access1
Secret access key [None]: access1
Session token (Optional - for temp AWS keys only) [None]: test

Keys saved to database.
```

Fig 1.6 Pacu setup

For controlled security assessments that aim to test security postures, mimic actual attacks, and find flaws in IAM configurations, Pacu is perfect. Nonetheless, the AWS CLI or SDKs are advised for accurate resource management and endpoint-specific operations.

Log table

Timestamp	Command	Action
2025-09-17 22:20	aws --endpoint-url=http://localhost:4566 s3 mb s3://mock-bucket	Created S3 bucket mock-bucket
2025-09-17 22:21	echo "This is a test file for exfiltration." > hi.txt	Created dummy exfiltration file
2025-09-17 22:21:30	aws --endpoint-url=http://localhost:4566 s3 cp hi.txt s3://mock-bucket/hi.txt	Uploaded dummy file to S3 bucket
2025-09-17 22:23	aws --endpoint-url=http://localhost:4566 iam create role --role-name mock-role	Created IAM role mock-role
2025-09-17 22:24	aws --endpoint-url=http://localhost:4566 iam create- user --user-name mock-user	Created IAM user mock-user
2025-09-17 22:26	aws --endpoint-url=http://localhost:4566 ec2 create- volume --availability-zone us-east-1a -- size 1	Created 1GB EC2 volume
2025-09-17 22:30	aws --endpoint-url=http://localhost:4566 logs create log-group --log-group-name /mock/log/group	Created CloudWatch log group
2025-09-17 22:30	aws --endpoint-url=http://localhost:4566 lambda create function --function-name mock function	Created Lambda function

2025-09-17 22:31	aws --endpoint-url=http://localhost:4566 dynamodb create-table --table-name mock-table .	Created DynamoDB table mock-table
2025-09-17 22:31	aws --endpoint-url=http://localhost:4566 s3 ls	Enumerated available S3 buckets
2025-09-17 22:33	aws --endpoint-url=http://localhost:4566 iam list-users	Listed IAM users