Report: Cloud Privilege Abuse Simulation Lab

Lab Objective

Simulate privilege abuse in a cloud environment.
Privilege Abuse: Exploit a service principal or cross-tenant misconfiguration in AWS.

Tools

LocalStack, AWS CLI, Bash

Methodology

Start LocalStack and set up LocalStack

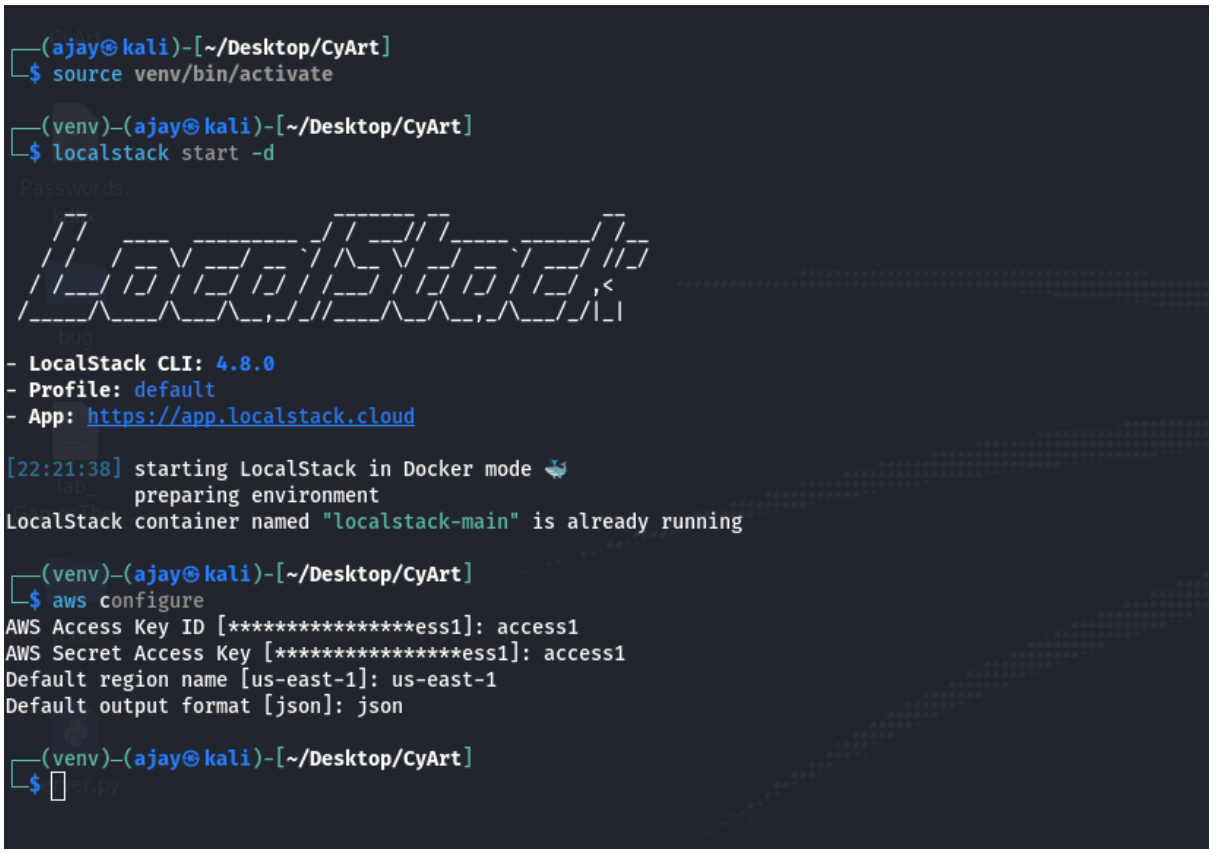

Fig 1.1 LocalStack being setup

Create an Overprivileged Role.

```
┌──(venv)─(ajay㉿kali)-[~/Desktop/CyArt]
└─$ aws iam create-role \
> --role-name OverprivilegedRole \
> --assume-role-policy-document '{
quote> "Version": "2012-10-17",
quote> "Statement": [
quote> {
quote> "Effect": "Allow",
quote> "Principal": {"Service": "ec2.amazonaws.com"},
quote> "Action": "sts:AssumeRole"
quote> }
quote> ]
quote> }' \
> --endpoint-url $AWS_ENDPOINT_URL
{
    "Role": {
        "Path": "/",
        "RoleName": "OverprivilegedRole",
        "RoleId": "AROAQAAAAAAAKUT4ZILFE",
        "Arn": "arn:aws:iam::000000000000:role/OverprivilegedRole",
        "CreateDate": "2025-09-17T16:56:14.490952+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ec2.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}

┌──(venv)─(ajay㉿kali)-[~/Desktop/CyArt]
└─$
```

Fig 1.2 Over-privileged role being created

Attach Admin Policy to it

```
┌──(venv)─(ajay㉿kali)-[~/Desktop/CyArt]
└─$ aws iam attach-role-policy \
--role-name OverprivilegedRole \
--policy-arn arn:aws:iam::aws:policy/AdministratorAccess \
--endpoint-url $AWS_ENDPOINT_URL

┌──(venv)─(ajay㉿kali)-[~/Desktop/CyArt]
└─$
```

Fig 1.3 Admin policy added to overprivilege role

Now verify role

```
┌──(venv)─(ajay㉿kali)-[~/Desktop/CyArt]
└─$ aws iam list-roles --endpoint-url $AWS_ENDPOINT_URL
{
    "Roles": [
        {
            "Path": "/",
            "RoleName": "OverprivilegedRole",
            "RoleId": "AROAQAAAAAAAKUT4ZILFE",
            "Arn": "arn:aws:iam::000000000000:role/OverprivilegedRole",
            "CreateDate": "2025-09-17T16:56:14.490952+00:00",
            "AssumeRolePolicyDocument": {
                "Version": "2012-10-17",
                "Statement": [
                    {
                        "Effect": "Allow",
                        "Principal": {
                            "Service": "ec2.amazonaws.com"
                        },
                        "Action": "sts:AssumeRole"
                    }
                ]
            },
            "MaxSessionDuration": 3600
        }
    ]
}
```

Fig 1.4 role being verified

Assume Overprivileged Role

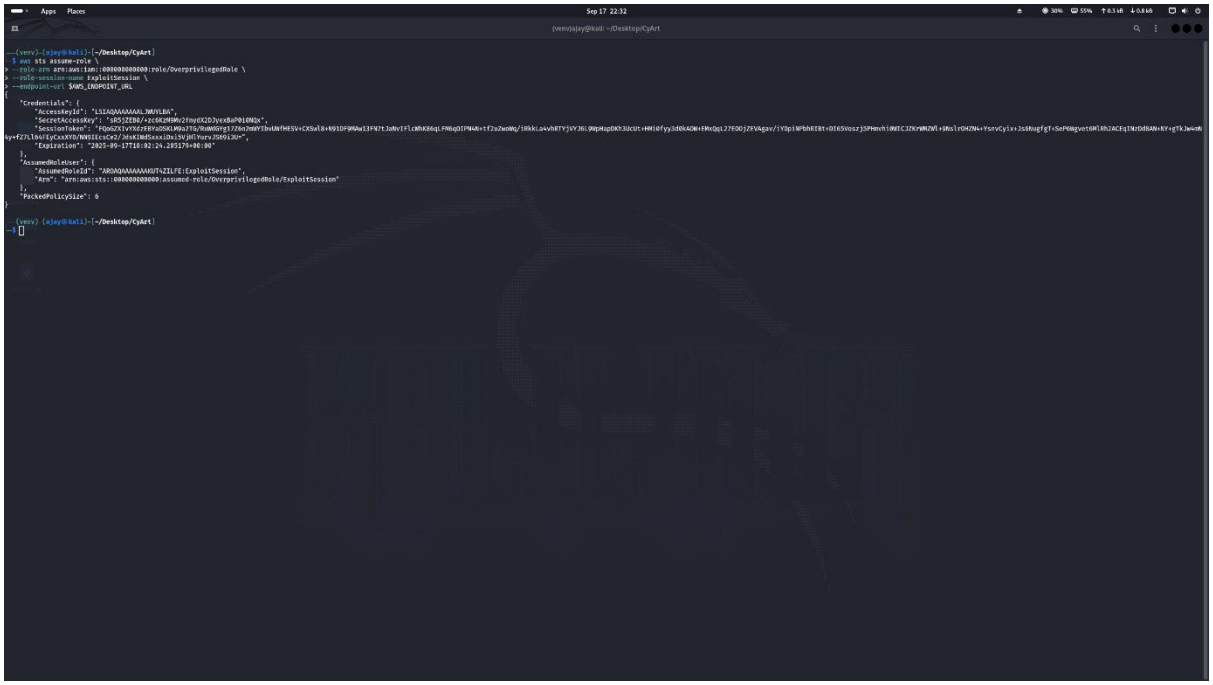

Fig 1.5 Credentials of over -privilege role

Now export the Temporary Credentials and test admin privileges.

```
┌──(venv)─(ajay㉿kali)-[~/Desktop/CyArt]
└─$ aws iam list-users --endpoint-url $AWS_ENDPOINT_URL
{
    "Users": []
}

┌──(venv)─(ajay㉿kali)-[~/Desktop/CyArt]
└─$ aws iam create-user --user-name TestUser --endpoint-url $AWS_ENDPOINT_URL
{
    "User": {
        "Path": "/",
        "UserName": "TestUser",
        "UserId": "v1gsf9favepvgbtptyd6",
        "Arn": "arn:aws:iam::000000000000:user/TestUser",
        "CreateDate": "2025-09-17T17:04:48.921580+00:00"
    }
}

┌──(venv)─(ajay㉿kali)-[~/Desktop/CyArt]
└─$
```

Fig 1.6 Test IAM role being created

Now attach policy to role

```
┌──(venv)─(ajay㉿kali)-[~/Desktop/CyArt]
└─$ aws iam attach-user-policy \
--user-name TestUser \
--policy-arn arn:aws:iam::aws:policy/AdministratorAccess \
--endpoint-url $AWS_ENDPOINT_URL
```

Fig 1.7 User Policy being attached

Now verify Policies and cleanup and after that detach polices,IAM users and roles.

Fig 1.8 Deleting users