**Lab 8 Write Up: Submitted by Md Foyzer Rahman Mondal, SID: N01728463**

1. Check the profile using the command **aws --profile cloudfoxable sts get-caller-identity**

2. Check the managed policies attached to the user using the command **aws iam list-attached-user-policies --user-name ctf-starting-user --profile cloudfoxable**

1. Check the AWS Security Audit policy using the command **aws iam get-policy --policy-arn arn:aws:iam::aws:policy/SecurityAudit --profile cloudfoxable**

1. Find the exact policy granted using the command **aws iam get-policy-version --policy-arn arn:aws:iam::aws:policy/SecurityAudit --version-id v49 --profile cloudfoxable**

1. Get the secret policy using the command **aws iam get-policy --policy-arn arn:aws:iam::982081074901:policy/its-a-secret-policy --profile cloudfoxable**
2. From the description of the above we can see that “policy that only allows access to the its-a-secret flag”. Using this command **aws iam get-policy-version --policy-arn arn:aws:iam::982081074901:policy/its-a-secret-policy --version-id v1 --profile cloudfoxable**

We can get the ssm:GetParameter that allows us to store configuration data and secrets.

1. Retrieve information using the command **aws ssm get-parameter --name /cloudfoxable/flag/its-a-secret --profile cloudfoxable**

It shows the value of the SecureString in encrypted format

1. Decrypt the value of the SecureString using the command **aws ssm get-parameter --name /cloudfoxable/flag/its-a-secret --with-decryption --profile cloudfoxable** . The value of the SecureString is the flag of this challenge.

**FLAG{ItsASecret::IsASecretASecretIfTooManyPeopleHaveAccessToIt?}**