BoB12th Digital Forensics

AWS Team Assign

CICD Scenario

Team Name:

디포기강잡조

Team Members:

김대호, 이은빈, 최서우, 최이슬, 홍지원

1. **CI/CD Scenario**
    - 3 IAM Users
    - 1 EC2 Instance in a single VPC
    - 1 API Gateway
    - 1 Lambda Function
    - 1 ECR Image
    - 2 CodeBuild Projects
2. **Scenario Initiation**
    - Initial provision of IAM users with Access Key IDs and Secret Access Keys.
3. **Scenario Story**
    - FooCorp is a company that offers public APIs. FooCorp's customers submit sensitive data to the API endpoint every minute.

```
POST {apiUrl}/prod/hello
Host: {apiHost}
Content-Type: text/html

superSecretData=...
```

- API: Implemented through a Lambda function exposed via an API Gateway.
- FooCorp, being a DevOps adopter, establishes a continuous deployment pipeline, which enables them to automatically deploy new versions of the Lambda function from source code to production within minutes.

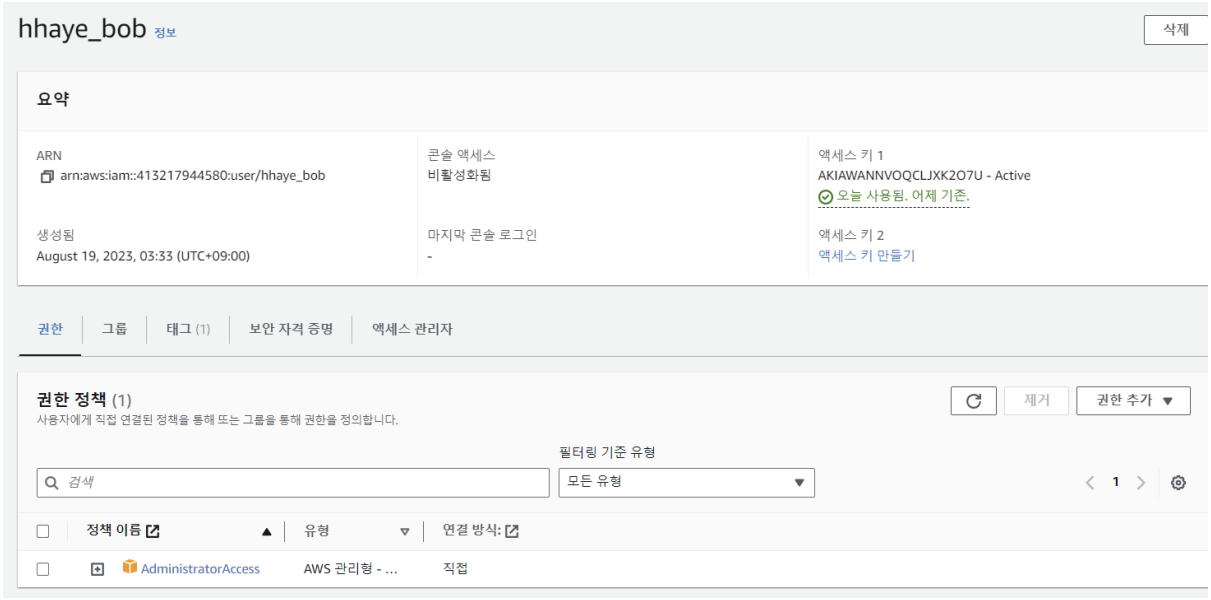
4. **Scenario Objectives**

- Search for customer-submitted sensitive data. Simulated user activities occur within the account. Executed every minute, the simulation of customer requests to the API is accomplished through the CodeBuild project.

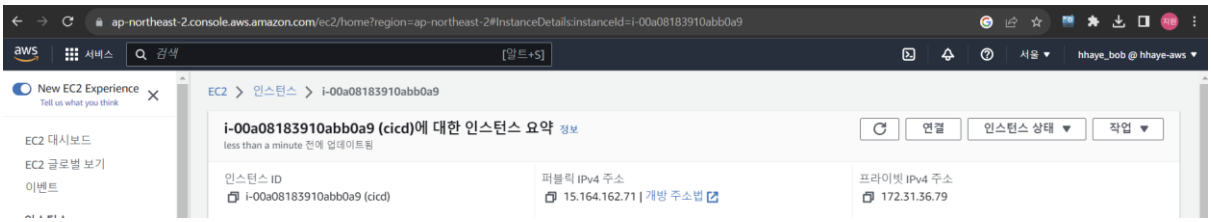
5. **Summary**

- Elevate permissions by overriding the tags on the EC2 instance used for attribute-based

access control. Steal SSH keys from the instance and use them to clone the CodeCommit repository. Examine commit history and identify new sets of AWS credentials. Utilize these to backdoor applications and exfiltrate critical data.



- Creating an IAM User with Administrator privileges

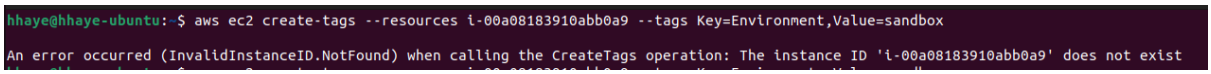


- Creating an EC2 for getting id (for cicd scenario) at perior IAM User account

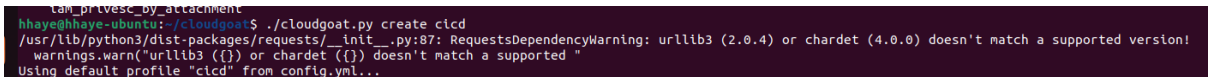
```
hhaye@hhaye-ubuntu:~$ aws configure --profile cicd
AWS Access Key ID [****************PM7N]: AKIAWANNVOQCLJXK2O7U
AWS Secret Access Key [****************dka5]: 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
Default region name [us-east-1]: ap-northeast-2
Default output format [json]: json
```

- Creating profile for cicd scenario and registering the access key and secret key of IAM user named 'hhaye_bob'

- Checking profile cicd

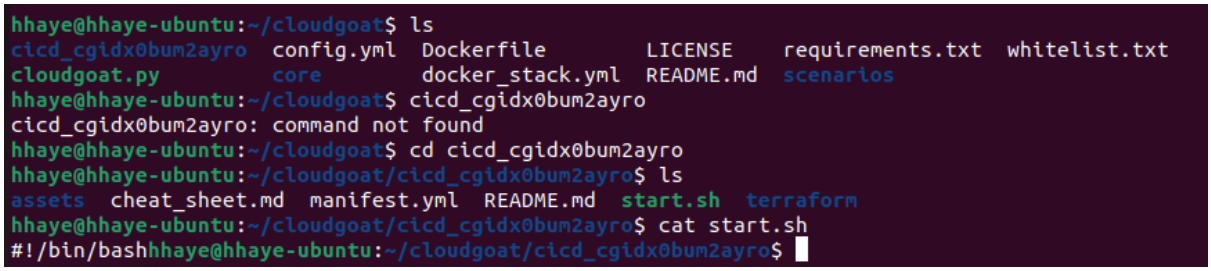


- But I faced repeatable connection error between cicd account and my ec2 although both are created in the same IAM account



- I double double double double checked '~create cicd' to get 'start.txt'

- But this is the big problem all the team members are continuing facing



- There is 'start.sh' instead of 'start.txt', so I used 'cat' command but that is just /bin/bash

Q1. Do we have to use our own aws access/secret key or cloudgoat aws access/secret key made for just scenario?

Q2. Is it ok to change scenario before 24 when the presentation is planned?

Thanks a lot and really sorry to make our assignment unfinished.