

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.

hhye_bob 정보

삭제

요약

ARN arn:aws:iam::413217944580:user/hhye_bob	콘솔 액세스 비활성화됨	액세스 키 1 AKIAWANNVOQCLJXK2O7U - Active 오늘 사용됨. 어제 기준.
생성됨 August 19, 2023, 03:33 (UTC+09:00)	마지막 콘솔 로그인 -	액세스 키 2 액세스 키 만들기

권한 그룹 태그 (1) 보안 자격 증명 액세스 관리자

권한 정책 (1)
사용자에게 직접 연결된 정책을 통해 또는 그룹을 통해 권한을 정의합니다.

필터링 기준 유형
모든 유형

검색

정책 이름 유형 연결 방식

AdministratorAccess AWS 관리형 - ... 직접

- Creating an IAM User with Administrator privileges

ap-northeast-2.console.aws.amazon.com/ec2/home?region=ap-northeast-2#InstanceDetails:instanceId=i-00a08183910abb0a9

aws 서비스 검색 [일트+S]

New EC2 Experience Tell us what you think

EC2 대시보드 EC2 글로벌 보기 이벤트

EC2 > 인스턴스 > i-00a08183910abb0a9

i-00a08183910abb0a9 (cicd)에 대한 인스턴스 요약 정보
less than a minute 전에 업데이트됨

연결 인스턴스 상태 작업

인스턴스 ID i-00a08183910abb0a9 (cicd)	퍼블릭 IPv4 주소 15.164.162.71 개방 주소법	프라이빗 IPv4 주소 172.31.36.79
---------------------------------------	---------------------------------------	------------------------------

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

```
hhye@hhye-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 'hhye_bob'

```
hhaye@hhaye-ubuntu:~$ aws ec2 describe-instances --region ap-northeast-2 --profile cicd
{
  "Reservations": [
    {
      "Groups": [],
      "Instances": [
        {
          "AmiLaunchIndex": 0,
          "ImageId": "ami-0c9c942bd7bf113a2",
          "InstanceId": "i-04bec6c97abb2dd22",
          "InstanceType": "t2.micro",
          "KeyName": "Public_web",
          "LaunchTime": "2023-08-11T02:04:03+00:00",
          "Monitoring": {
            "State": "disabled"
          },
          "Placement": {
            "AvailabilityZone": "ap-northeast-2a",
            "GroupName": "",
            "Tenancy": "default"
          },
          "PrivateDnsName": "ip-10-0-9-24.ap-northeast-2.compute.internal",
          "PrivateIpAddress": "10.0.9.24",
          "ProductCodes": [],
          "PublicDnsName": "ec2-13-209-84-161.ap-northeast-2.compute.amazonaws.com",
          "PublicIpAddress": "13.209.84.161",
          "State": {
            "Code": 16,
            "Name": "running"
          },
          "StateTransitionReason": "",
          "SubnetId": "subnet-003a13314fb646e91",
          "VpcId": "vpc-036f230416ef585b6",
          "Architecture": "x86_64",
          "BlockDeviceMappings": [
            {
              "DeviceName": "/dev/sda1",
              "Ebs": {

```

- Checking profile cicd

```
hhaye@hhaye-ubuntu:~$ aws ec2 create-tags --resources i-00a08183910abb0a9 --tags Key=Environment,Value=sandbox
An error occurred (InvalidInstanceID.NotFound) when calling the CreateTags operation: The instance ID 'i-00a08183910abb0a9' does not exist
```

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

```
Can't private_by_attachment
hhaye@hhaye-ubuntu:~$ ./cloudgoat.py create cicd
/usr/lib/python3/dist-packages/requests/__init__.py:87: RequestsDependencyWarning: urllib3 (2.0.4) or chardet (4.0.0) doesn't match a supported version!
  warnings.warn("urllib3 ({}), or chardet ({}), doesn't match a supported version".format(urllib3.__version__, chardet.__version__))
Using default profile "cicd" from config.yml...
```

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

```
Error: Listing CodeBuild Projects: AccessDeniedException: User: arn:aws:iam::413217944580:user/hhaye_bob is not authorized to perform: codebuild:BatchGetProjects on resource: arn:aws:codebuild:us-east-1:749904558024:project/build-docker-image because no resource-based policy allows the codebuild:BatchGetProjects action
status code: 400, request id: 6db0255b-a7a4-46d2-bda8-30e21ad77f1b

with aws_codebuild_project.build-docker-image,
on codepipeline.tf line 1, in resource "aws_codebuild_project" "build-docker-image":
1: resource "aws_codebuild_project" "build-docker-image" {}

Error: reading Amazon S3 (Simple Storage) Bucket (codepipeline-bucket-cicd-cgldxbun2ayro): Forbidden: Forbidden
status code: 403, request id: DK054QCAQZAT757J, host id: lMnIQwXGe0K8jC8+NAB9jPctazj5xw004sh/y1FD2VA3gdAp4DefIHRxxIf+z/8CMAaYfW/H0Ipu+LKQNLDDMyL7DPTPpC5518RG6f60uI=

with aws_s3_bucket.codepipeline_bucket,
on codepipeline.tf line 8, in resource "aws_s3_bucket" "codepipeline_bucket":
8: resource "aws_s3_bucket" "codepipeline_bucket" {}
```

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

```
hhaye@hhaye-ubuntu:~/cloudgoat$ ls
cicd_cgidx0bum2ayro  config.yml  Dockerfile      LICENSE      requirements.txt  whitelist.txt
cloudgoat.py         core       docker_stack.yml  README.md    scenarios
hhaye@hhaye-ubuntu:~/cloudgoat$ cicd_cgidx0bum2ayro
cicd_cgidx0bum2ayro: command not found
hhaye@hhaye-ubuntu:~/cloudgoat$ cd cicd_cgidx0bum2ayro
hhaye@hhaye-ubuntu:~/cloudgoat/cicd_cgidx0bum2ayro$ ls
assets  cheat_sheet.md  manifest.yml  README.md  start.sh  terraform
hhaye@hhaye-ubuntu:~/cloudgoat/cicd_cgidx0bum2ayro$ cat start.sh
#!/bin/bash
```

- 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.