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**

**텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명**

**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

텍스트, 소프트웨어, 폰트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

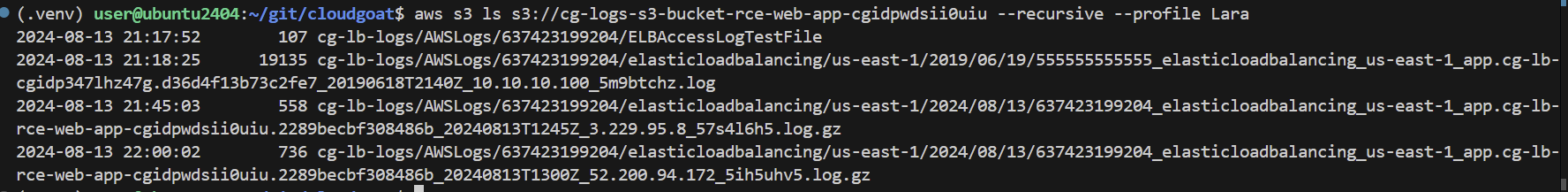
텍스트, 스크린샷, 소프트웨어, 컴퓨터 아이콘이(가) 표시된 사진

자동 생성된 설명

텍스트, 폰트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

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



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.

텍스트, 스크린샷, 소프트웨어, 컴퓨터 아이콘이(가) 표시된 사진

자동 생성된 설명

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.