# CloudGoat_rec_web_app


| Mentor | Niko |
|---|---|
| Trak | Digital Forensics |
| Name | Hunseok Song |
| Submit date | 24.08.13 |

# 내용

# 1. Installation process

Install the AWS CLI, create an account named BoB13CloudAdmin, and generate an IAM key.

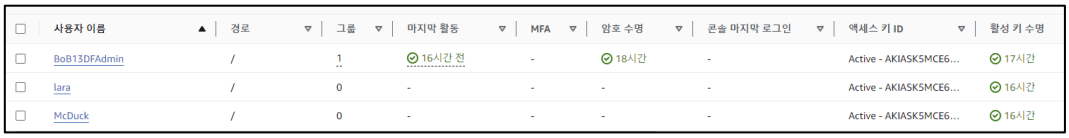

[Figure 1] IAM account created

Install CloudGoat – scenario: rce_web_app.

```
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat$ ./cloudgoat.py create rce_web_app
Using default profile "BoB13DFAdmin" from config.yml...
Loading whitelist.txt...
A whitelist.txt file was found that contains at least one valid IP address or range.

Now running rce_web_app's start.sh...
Initializing the backend...
Initializing provider plugins...
- Finding hashicorp/aws versions matching "~> 4.16"...
- Installing hashicorp/aws v4.67.0...
- Installed hashicorp/aws v4.67.0 (signed by HashiCorp)
Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.
```

[Figure 2] scenario: rce_web_app




[Figure 3] What AWS looks like after installation

# 2. Scenario

### 2.1 Summary

This scenario covers an attacker starting as the IAM user Lara, exploring the load balancer and S3 buckets, exploiting the web application's RCE vulnerability to expose confidential files, and finally accessing the RDS database. Another path would be to start as the IAM user McDuck, enumerating the S3 buckets and obtaining an SSH key, which would allow direct access to the EC2 server and database.

### 2.2 IAM User “Lara”

While exploring the AWS environment as IAM user Lara, the attacker discovers a web application and a secret admin page, and gains shell access to the EC2 instance through an RCE vulnerability. The attacker then accesses the RDS database via two paths to obtain the secret text, which is the goal of the scenario. In the first path (Branch A), they discover the RDS login credentials in a private S3 bucket, and in the second path (Branch B), they obtain the credentials through the EC2 metadata service.

### 2.3 IAM User “McDuck”

The attacker discovers an SSH key pair by listing S3 buckets with the provided key and uses it to log in to the EC2 instance. With the privileges of the EC2 instance, they browse the private S3 bucket to obtain the credentials of the RDS database, which they use to access the RDS database and obtain their goal: the ciphertext.

# 3. Solve problems

lara and mcduck's key

```
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb$ cat start.txt
cloudgoat_output_aws_account_id = 160885254045
cloudgoat_output_lara_access_key_id = AKIASK5MCE6O6D2UIH4X
cloudgoat_output_lara_secret_key = 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
cloudgoat_output_mcduck_access_key_id = AKIASK5MCE6O2EGN4ASY
cloudgoat_output_mcduck_secret_key = 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
```

[Figure 4] keys

```
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb$ aws configure --profile Lara
AWS Access Key ID [None]: AKIASK5MCE6O6D2UIH4X
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-2
```

[Figure 5] configure Lara

The current user does not have permission to view policies and role.

```
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb
$ aws iam list-user-policies --user-name lara --profile Lara

An error occurred (AccessDenied) when calling the ListUserPolicies operation: User: arn:aws:
iam::160885254045:user/lara is not authorized to perform: iam:ListUserPolicies on resource:
user lara because no identity-based policy allows the iam:ListUserPolicies action
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb
$ aws iam list-attached-user-policies --user-name lara --profile Lara

An error occurred (AccessDenied) when calling the ListAttachedUserPolicies operation: User:
arn:aws:iam::160885254045:user/lara is not authorized to perform: iam:ListAttachedUserPolici
es on resource: user lara because no identity-based policy allows the iam:ListAttachedUserPo
licies action
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb
$ aws iam list-roles --profile Lara

An error occurred (AccessDenied) when calling the ListRoles operation: User: arn:aws:iam::16
0885254045:user/lara is not authorized to perform: iam:ListRoles on resource: arn:aws:iam::1
60885254045:role/ because no identity-based policy allows the iam:ListRoles action
```

[Figure 6] permission deny

I looked up the Lara s3 bucket.

```
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7f
$ aws s3 ls --profile Lara
2024-08-12 23:32:08 cg-cardholder-data-bucket-cloud-breach-s3-cgidfekdpuipxr
2024-08-13 00:47:47 cg-keystore-s3-bucket-rce-web-app-cgid8wm0ntk7fb
2024-08-13 00:47:50 cg-logs-s3-bucket-rce-web-app-cgid8wm0ntk7fb
2024-08-13 00:47:47 cg-secret-s3-bucket-rce-web-app-cgid8wm0ntk7fb
```

[Figure 7] Lara bucket

The actual bucket that you can access and print when you output the contents of the bucket one by one is "cg-logs-s3-bucket-rce-web-app-cgid8wm0ntk7fb".

```
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb
$ aws s3 ls cg-cardholder-data-bucket-cloud-breach-s3-cgidfekdpuipxr --profile Lara

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb
$ aws s3 ls cg-keystore-s3-bucket-rce-web-app-cgid8wm0ntk7fb --profile Lara

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb
$ aws s3 ls cg-logs-s3-bucket-rce-web-app-cgid8wm0ntk7fb --profile Lara
                           PRE cg-lb-logs/
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb
$ aws s3 ls cg-secret-s3-bucket-rce-web-app-cgid8wm0ntk7fb --profile Lara

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb
```

[Figure 8] Accessible buckets

I checked the bucket and found the log file.

```
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb
$ aws s3 ls s3://cg-logs-s3-bucket-rce-web-app-cgid8wm0ntk7fb --recursive --profile Lara
2024-08-13 00:51:01        107 cg-lb-logs/AWSLogs/160885254045/ELBAccessLogTestFile
2024-08-13 00:51:39      19199 cg-lb-logs/AWSLogs/160885254045/elasticloadbalancing/us-east-
1/2019/06/19/555555555555_elasticloadbalancing_us-east-1_app.cg-lb-cgidp347lhz47g.d36d4f13b7
3c2fe7_20190618T2140Z_10.10.10.100_5m9btchz.log
```

[Figure 9] log file

I tried to extract and analyze the corresponding log file, but was unable to do so due to an error.

```
(.venv) song@song-VMware-Virtual-Platform:~/Desktop/git/cloudgoat/rce_web_app_cgid8wm0ntk7fb
$ aws s3 cp s3://cg-lb-logs/AWSLogs/160885254045/elasticloadbalancing/us-east-1/2019/06/19/5
55555555555_elasticloadbalancing_us-east-1_app.cg-lb-cgidp347lhz47g.d36d4f13b73c2fe7_2019061
8T2140Z_10.10.10.100_5m9btchz.log ./ --profile Lara
fatal error: An error occurred (403) when calling the HeadObject operation: Forbidden
```

[Figure 10] extract error