ID Account ID from Public S3 Bucket

Analyze the challenge

The challenge is to identify the AWS Account ID associated with a public S3 bucket named "mega-big-tech." We are given the IP address of a website, AWS credentials, and a tool called "s3-account-search" that can help us brute-force the account ID.

Plan of action

1. **Website and Source Code:** Briefly examine the website and its source code to understand how the S3 bucket is used.
2. **Install s3-account-search:** Use the provided instructions to install the "s3-account-search" tool.
3. **Configure AWS CLI:** Configure the AWS CLI with the provided credentials to be able to use the assumed role.
4. **Run s3-account-search:** Execute the "s3-account-search" tool with the provided role ARN and the target S3 bucket name to retrieve the account ID.
5. **Verify the Account ID (Optional):** Briefly explain how we can verify the account ID by searching for public EBS snapshots associated with it.

Perforrm the steps to identify the AWS Account ID associated with the public S3 bucket "mega-big-tech."

Website and Source Code

1. **Action:** Visit the website using the provided IP address (54.204.171.32) in a web browser.
2. **Action:** View the source code of the website (usually by right-clicking and selecting "View Page Source").
3. **Observation:** Observe that images on the website are being loaded from an Amazon S3 bucket named "mega-big-tech."

Install s3-account-search

1. **Action:** Open your terminal or command prompt.
2. **Action:** Run the following command to install the `s3-account-search` tool:

```
python3 -m pip install s3-account-search
```

3. **Action:** If necessary, add the tool's binary location to your PATH environment variable by running these commands:

```
echo 'export PATH=$PATH:~/.local/bin' >> ~/.zshrc
source ~/.zshrc
```

Configure AWS CLI

1. **Action:** In your terminal, run the following command to configure the AWS CLI:

```
aws configure
```

2. **Action:** Enter the Access key ID when prompted:

```
AWS Access Key ID [None]:
```

3. **Action:** Enter the Secret access key when prompted:

```
AWS Secret Access Key [None]:
```

4. **Action:** Set the region name when prompted:

```
Default region name [None]:
```

5. **Action:** Set the output format when prompted:

```
Default output format [None]:
```

Run s3-account-search

1. **Action:** In your terminal, run the following command to execute the `s3-account-search` tool:

```
s3-account-search arn:aws:iam::xxxxxxxx2155:role/LeakyBucket mega-big-
tech
```

2. **Observation:** The tool will attempt to brute-force the AWS account ID.

3. **Observation:** The tool will output the found AWS account ID. The output should be:

```
xxxxxxxx3799
```

Verify the Account ID (Optional)

1. **Action:** Run the following command in your terminal to find the region of the S3 bucket:

```
curl -I https://mega-big-tech.s3.amazonaws.com
```

2. **Observation:** Look for the `x-amz-bucket-region` header in the response. It should be set to `us-east-1`.
3. **Action:** Log in to the AWS Management Console using your own AWS account.
4. **Action:** Make sure the `us-east-1` region is selected.
5. **Action:** Search for and navigate to the EC2 service.
6. **Action:** In the left-hand menu, under "Elastic Block Store," click on "Snapshots."
7. **Action:** In the dropdown list, select "Public snapshots."
8. **Action:** Paste the discovered AWS account ID (xxxxxxxx3799) into the search field and press Enter.
9. **Observation:** If any public snapshots are found, it indicates that the account ID is likely correct.