Documentation on the steps followed:

1. **S3 Setup:**
    - Create S3 buckets using the AWS S3 dashboard, ensuring that some of them don't have server-side encryption enabled.
2. **Lambda IAM Role:**
    - Create a new IAM role in the AWS IAM dashboard for Lambda.
    - Attach the **AmazonS3ReadOnlyAccess** policy to the role. This policy grants read-only access to S3 buckets.
3. **Lambda Function:**
    - Create a new Lambda function in the AWS Lambda dashboard.
    - Choose Python 3.x as the runtime.
    - Assign the IAM role created earlier to the Lambda function.
    - Use the provided Python script that uses Boto3 to:
        - Initialize a boto3 S3 client.
        - List all S3 buckets.
        - Detect buckets without server-side encryption.
        - Print the names of unencrypted buckets for logging purposes.
4. **Manual Invocation:**
    - Save the Lambda function.
    - Manually trigger the Lambda function.
    - Review the Lambda logs to identify the S3 buckets without server-side encryption. The logs will show the names of unencrypted buckets if any.