Assignment 3 – S3

Make sure you follow the least privilege principle for the IAM policies for these 3 tasks and next classes.

1. Create a bucket for assets of the web app hosted on EC2. Put an image into the bucket.
    a. Create an inline IAM policy in the LabRole that allows the instance to get objects from the bucket.
    b. Download the image

aws s3 cp s3://<bucket>/< image_name> <image_name>

    c. Update the index.html and read the image from the /var/www/html folder
2. Send an email to yourself when the object is created in the bucket. You need to create an SNS topic. Modify the policy. Subsribe it.

```
{
 "Version": "2008-10-17",
 "Id": "__default_policy_ID",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "Service": "s3.amazonaws.com"
   },
   "Action": "SNS:Publish",
   "Resource": "arn:aws:sns:us-east-1:475249589989:MyS3Topic",
   "Condition": {
    "StringEquals": {
     "AWS:SourceAccount": "475249589989"
    },
    "ArnLike": {
     "AWS:SourceArn": "arn:aws:s3:::csnov516demo"
    }
   }
  }
 ]
}
```

3. Write a lambda that returns a Signed URL of the object. Make sure the LabRole has an inline policy that allows getting objects from the bucket.

```
const AWS = require("aws-sdk");

const s3 = new AWS.S3({apiVersion: '2006-03-01'});


exports.handler = async (event) => {
```

```
    const params = { Bucket: 'myfirstbucketcreatedwithcli2022cs516', Key: 'Capture.PNG' };

    return s3.getSignedUrl('getObject', params);

};
```

Refer: https://docs.aws.amazon.com/AWSJavaScriptSDK/latest/AWS/S3.html#getSignedUrl-property

Extra:

- Read a file from S3 in EC2 using S3 Gateway Endpoint. After a successful connection, write S3 resource-based policy that allows read access only from the VPC endpoint in the bucket policy. Refer: https://www.youtube.com/watch?v=TqApkvJx5hw