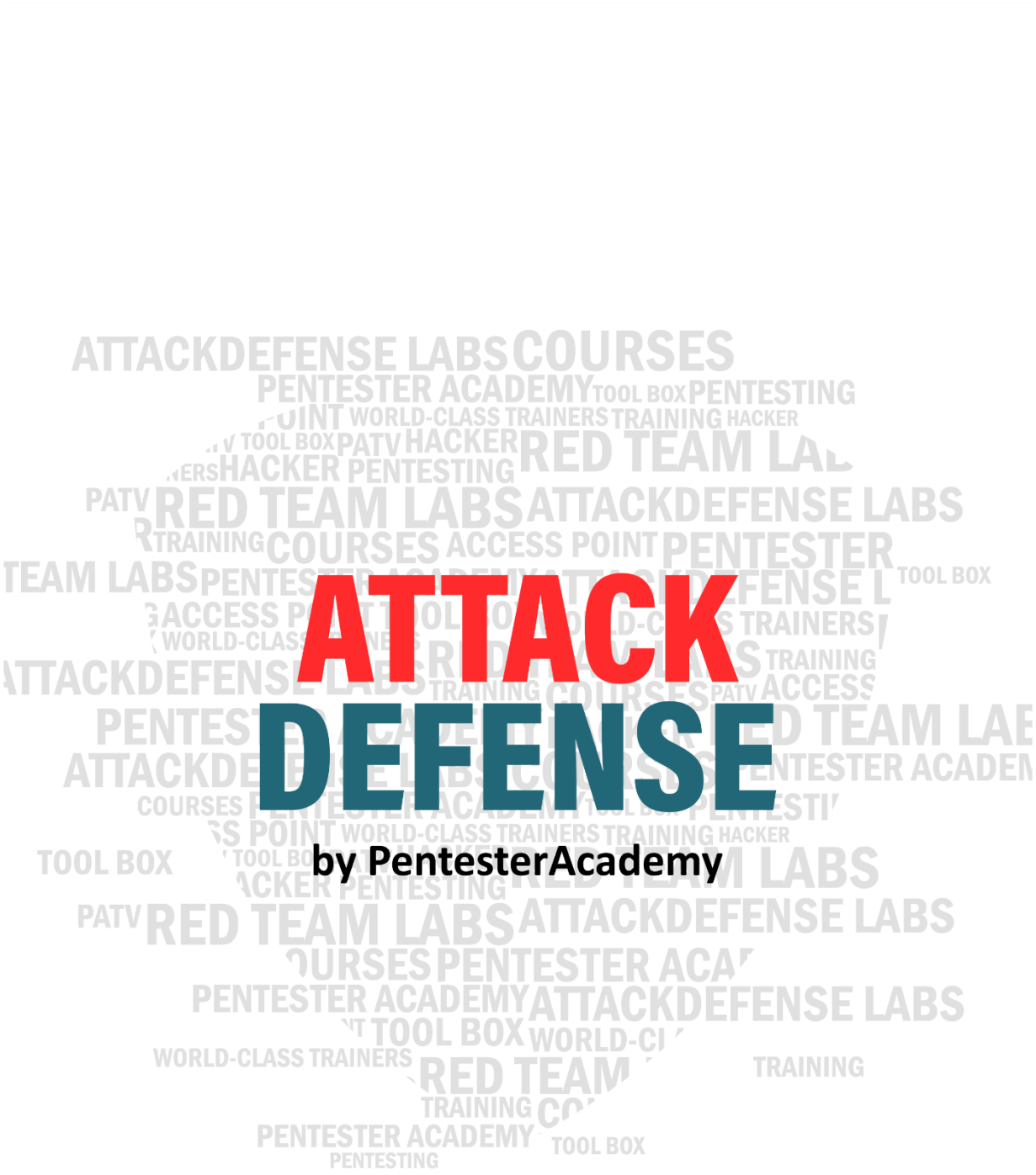

ATTACK
DEFENSE
by PentesterAcademy

Name	Special Request
URL	https://attackdefense.com/challengedetails?cid=2302
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

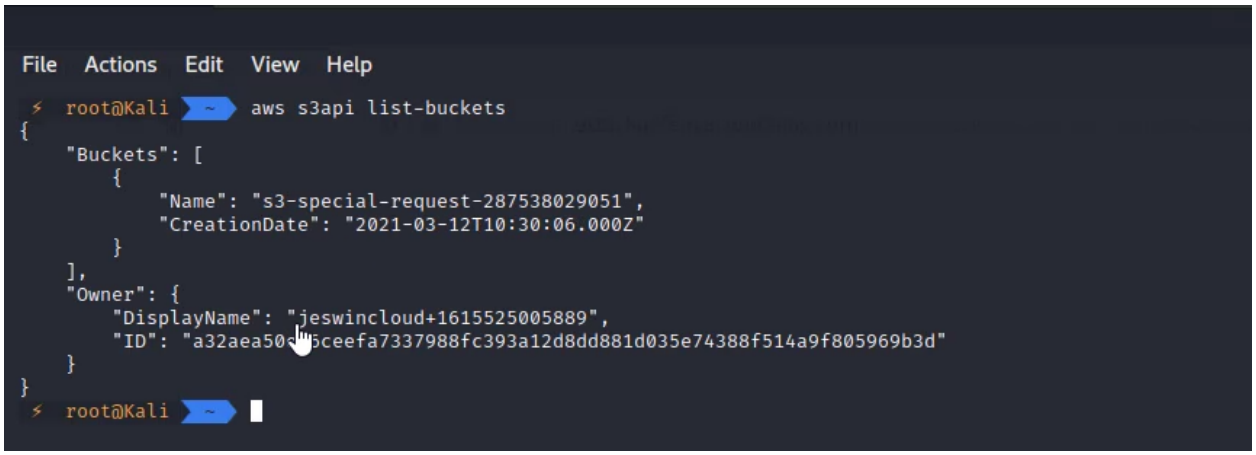
Login URL	https://287538029051.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad1sgZr48hOybr2T
Access Key ID	AKIAUF4U2EH5ZLON7EUH
Secret Access Key	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

Command: aws configure

```
File  Actions  Edit  View  Help
 ⚡ root@Kali ~ aws configure
AWS Access Key ID [****************7EUH]: AKIAUF4U2EH5ZLON7EUH
AWS Secret Access Key [****************QSmK]: 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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>

Flag present in s3 bucket.

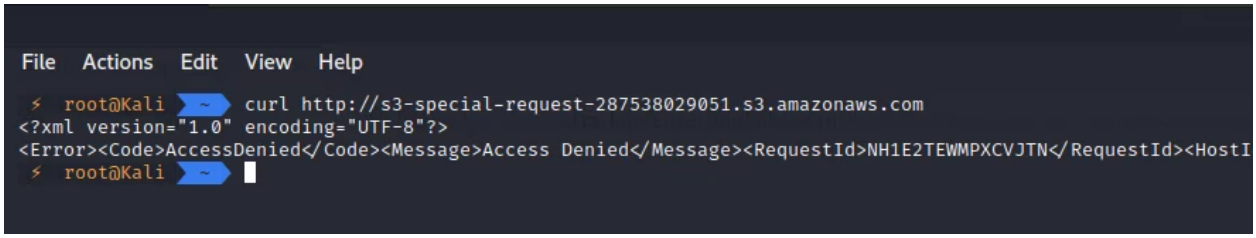
Step 4: Check bucket policy.

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

The bucket policy only allows access using a specified user agent.

Step 5: Send a simple curl request to access the bucket.

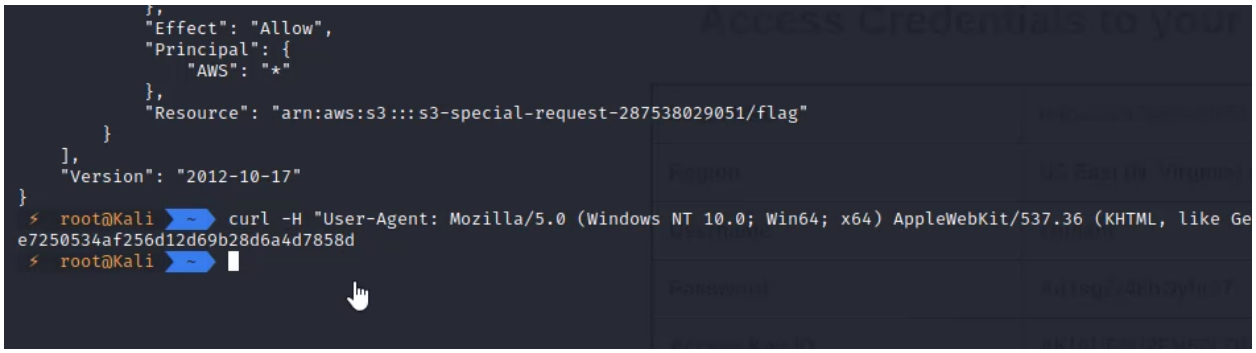
Command: curl http://<bucket-name>.s3.amazonaws.com



Access denied because curl's default user agent is not allowed to access the bucket.

Step 6: Use the user agent specified in the bucket policy to access the flag.

Command: curl -H "User-Agent: <user-agent in bucket policy>" http://<bucket-name>.s3.amazonaws.com/flag



FLAG: e7250534af256d12d69b28d6a4d7858d

Successfully retrieved flag.

References:

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