
ATTACK
DEFENSE
by PentesterAcademy

Name	API Gateway Enumeration
URL	https://attackdefense.com/challengedetails?cid=2275
Type	AWS Cloud Security : API Gateway

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:

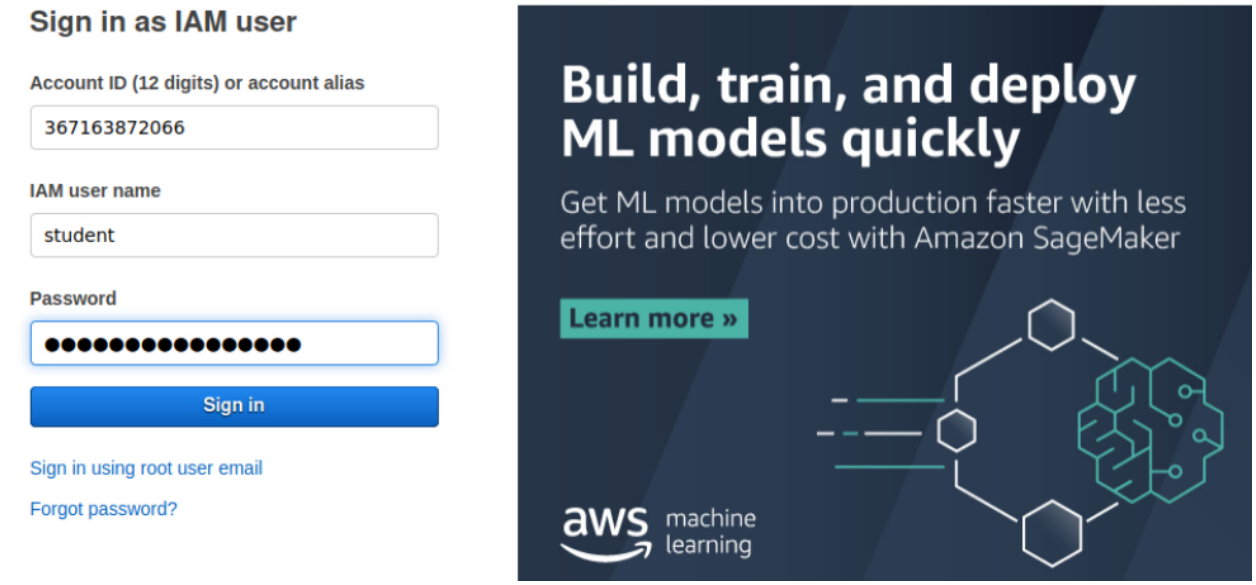
Console Based Enumeration

Step 1: Click on the lab link to get AWS access credentials.

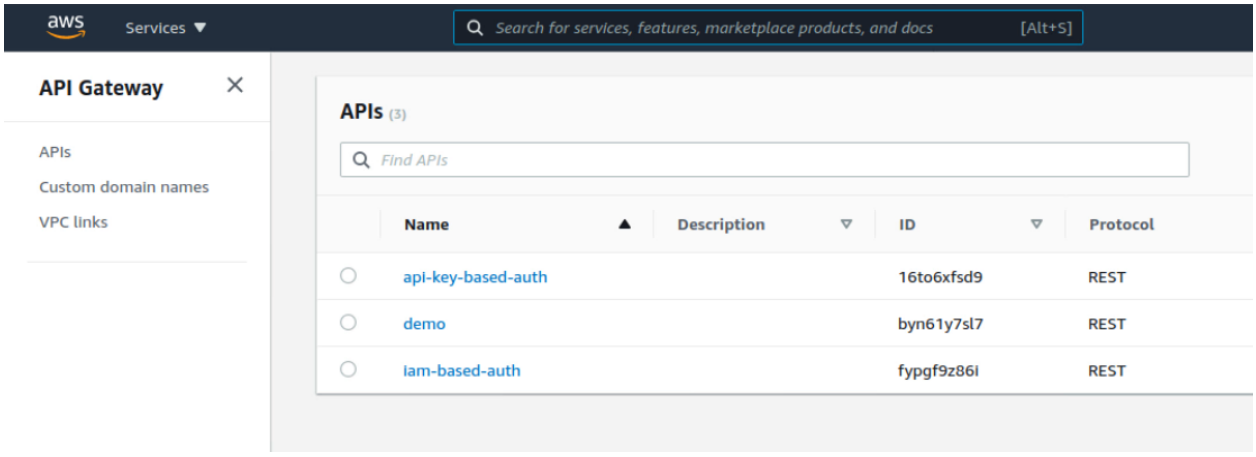
Access Credentials to your AWS lab Account

Login URL	https://367163872066.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad63Q9Q0vNQUEGui
Access Key ID	AKIAVK7FMCNBB2Z4VRPY
Secret Access Key	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

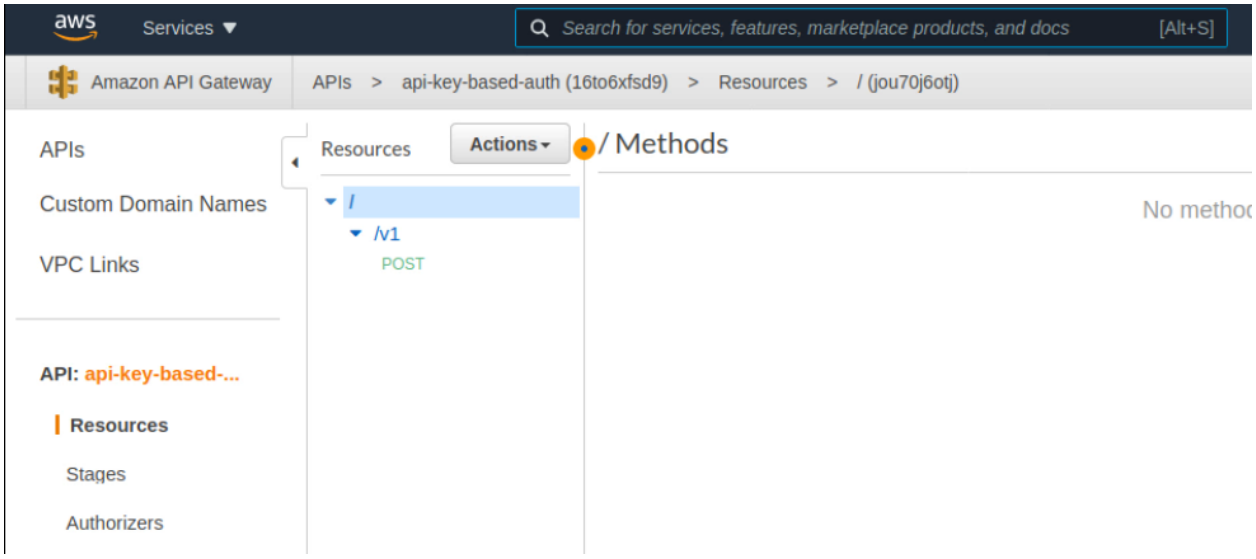
Step 2: Sign in to AWS console.



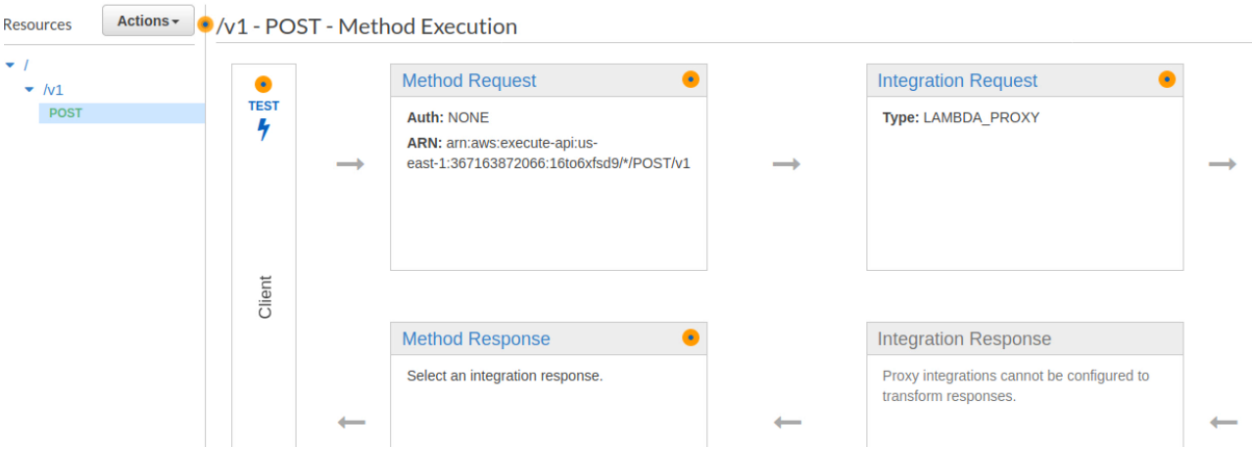
Step 3: Navigate to the API gateway dashboard.



Step 4: Click on API name to open API details.



Step 5: Click on Resources and enumerate Method Request, Integration request and proxy.



← Method Execution /v1 - POST - Method Request

Provide information about this method's authorization settings and the parameters it can receive.

Settings

Authorization NONE

Request Validator NONE

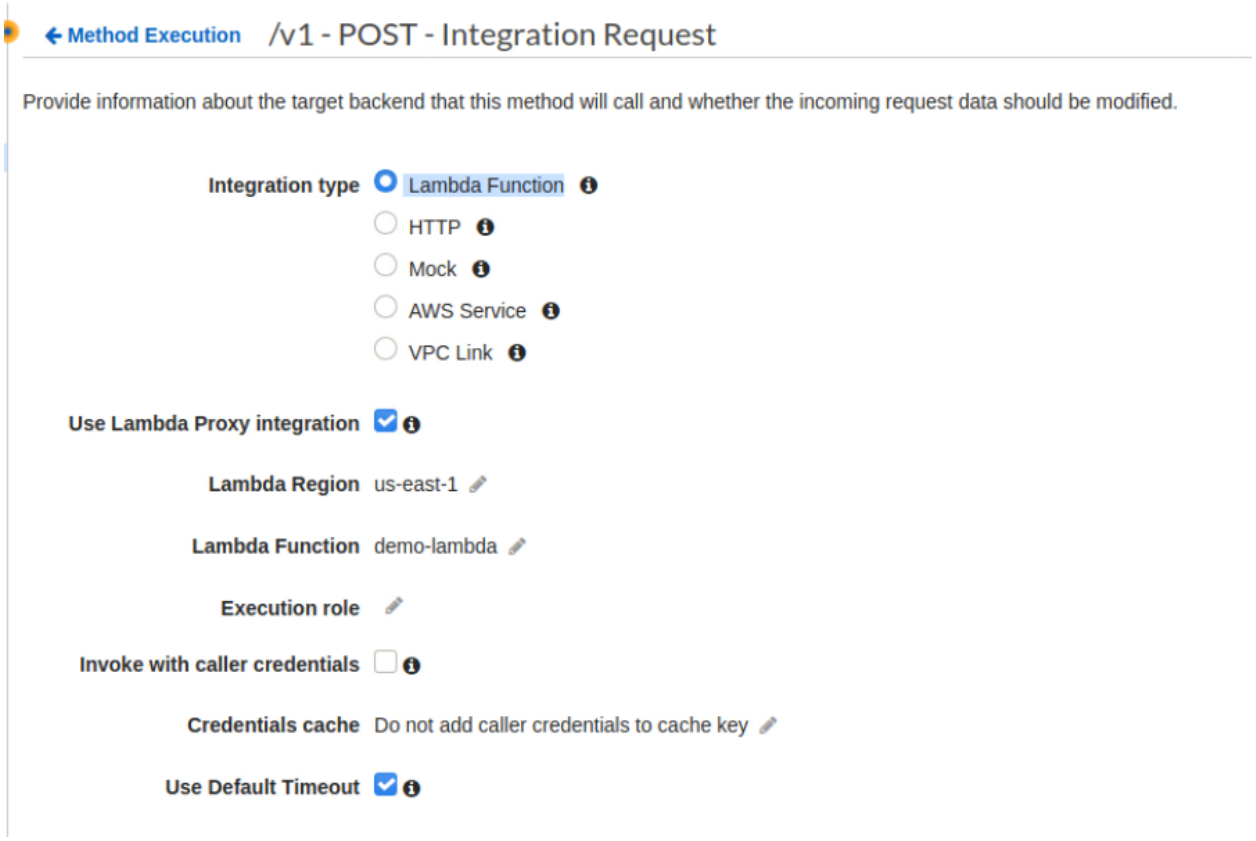
API Key Required true

URL Query String Parameters

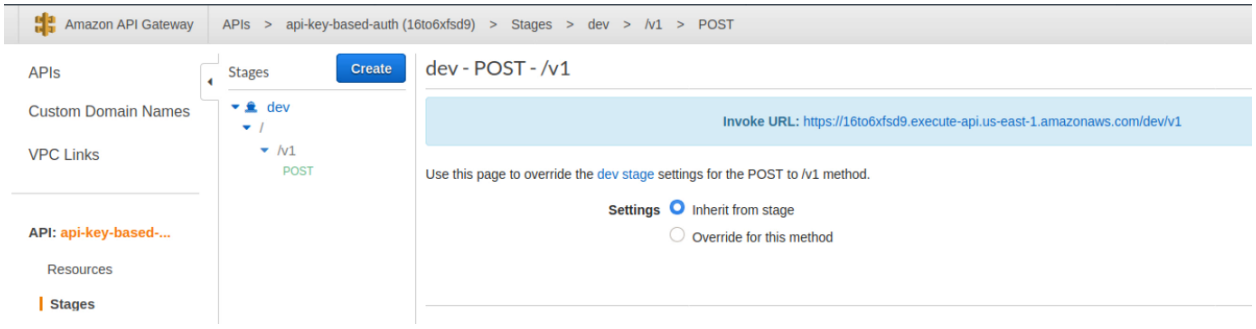
HTTP Request Headers

Request Body

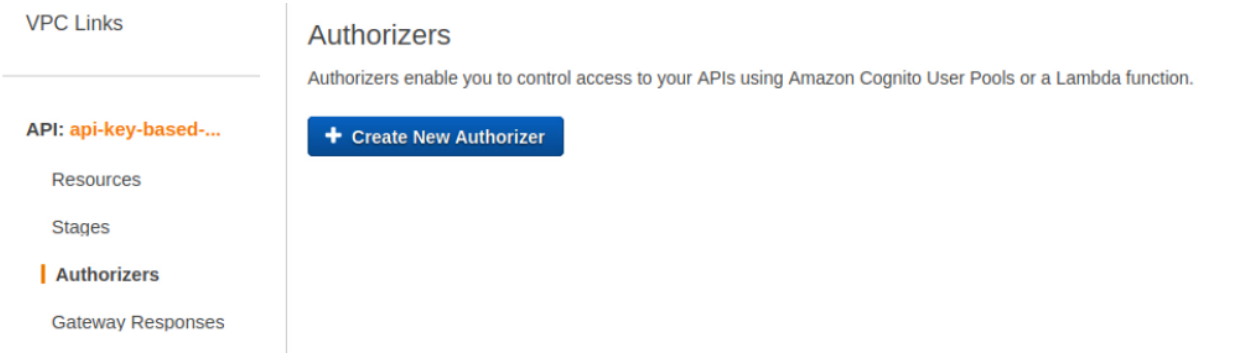
SDK Settings



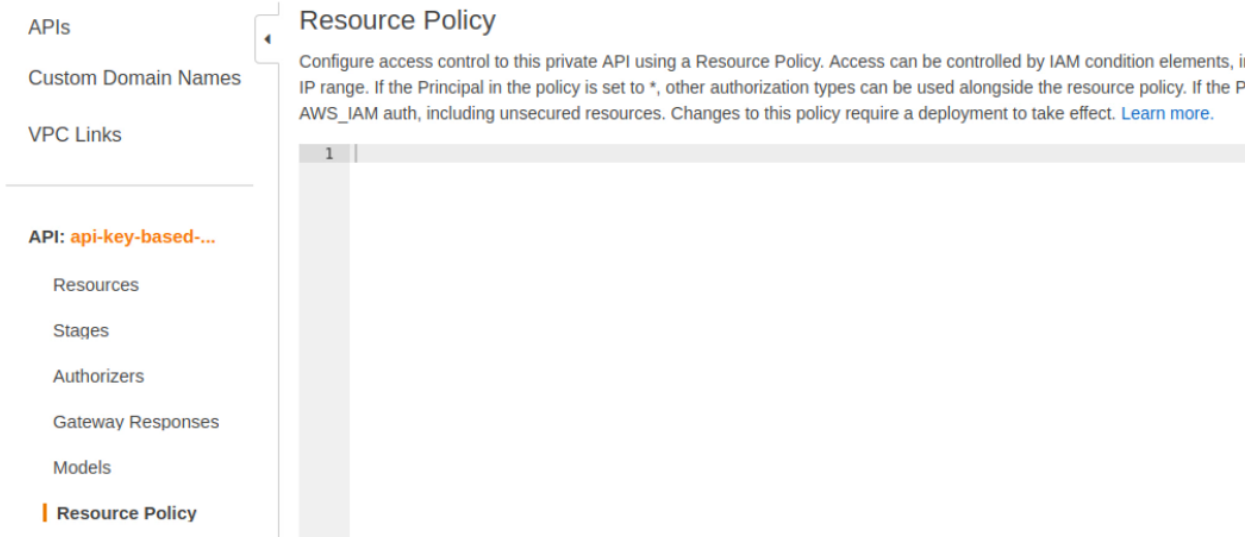
Step 6: Click on Stages on the left panel to enumerate stages for API.



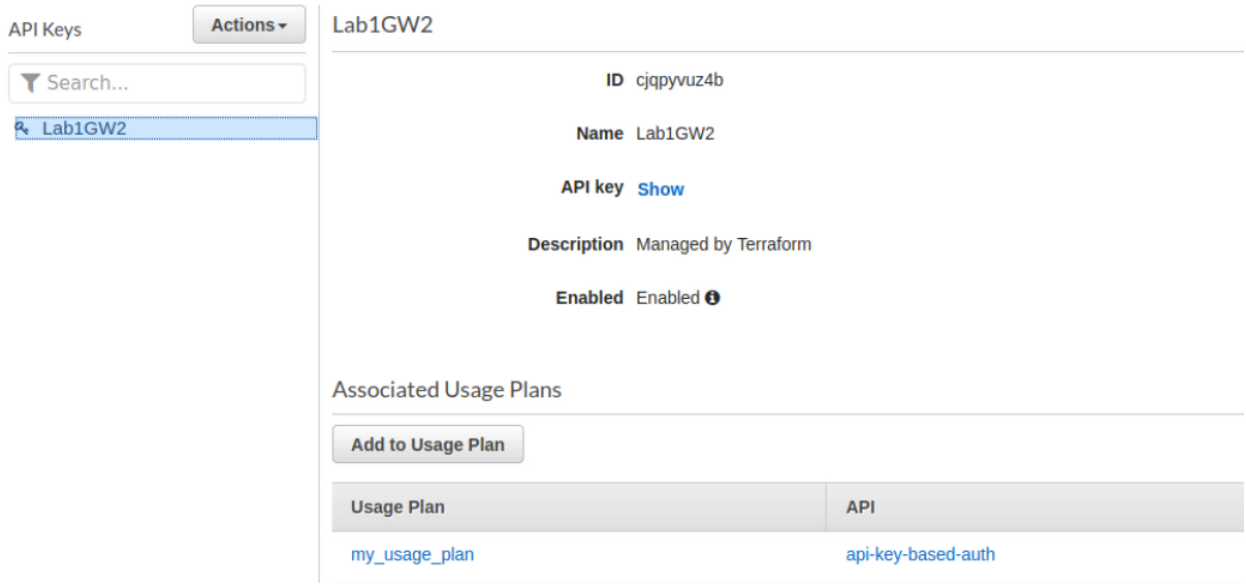
Step 7: Click on authorizers to check authorizers for the API.

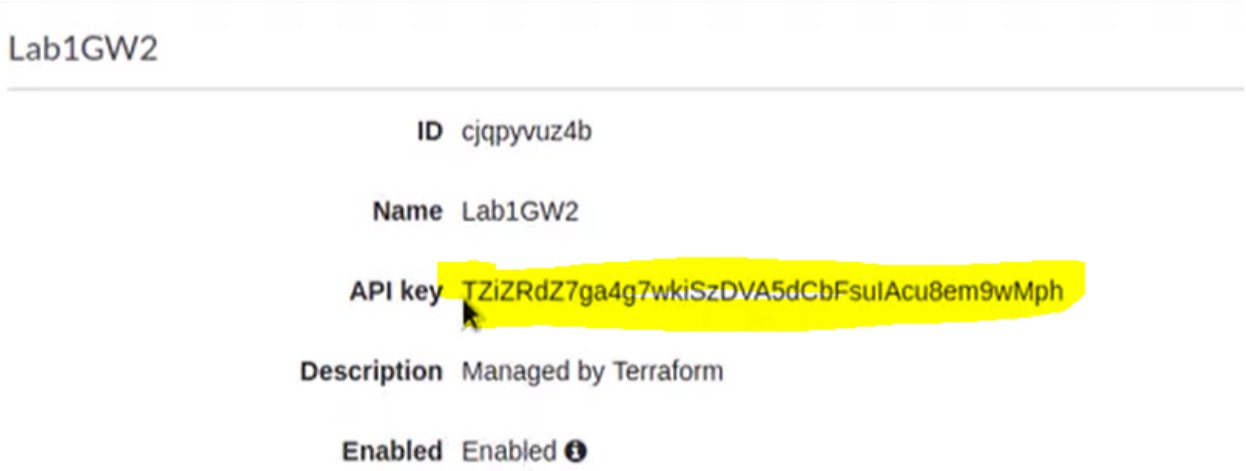


Step 8: Click on Resources on the left panel to enumerate resources for API.



Step 9: Check API's usage plans and check API keys. Go to the API Keys section in the left panel. Click on the API Key name listed.





Step 10: Similarly enumerate other apis on the AWS account.

CLI Based Enumeration

Step 1: Click on the lab link to get AWS access credentials.

Access Credentials to your AWS lab Account

Login URL	https://367163872066.signin.aws.amazon.com/console
Region	**US East (N. Virginia) us-east-1**
Username	**student**
Password	**Ad63Q9Q0vNQUEGui**
Access Key ID	**AKIAVK7FMCNBB2Z4VRPY**
Secret Access Key	**oPUtAdyGufy1ZCWtFZ39ViO1xpup/OlzD9AG5Pl8**

Step 2: Configure AWS CLI with AWS access keys.

Command: aws configure

```
root@Kali ~ aws configure
AWS Access Key ID [****************VTGY]: AKIA2DM3DTVBTTSD3IG4
AWS Secret Access Key [****************FAmU]: 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
Default region name [us-east-1]:
Default output format [None]:
root@Kali ~
```

Step 3: Check API settings for the account.

Command: aws apigateway get-account

```
root@Kali ~ aws apigateway get-account
{
    "throttleSettings": {
        "burstLimit": 5000,
        "rateLimit": 10000.0
    },
    "features": [
        "UsagePlans"
    ],
    "apiKeyVersion": "4"
}
root@Kali ~
```

Step 4: List API's on the AWS account.

Command: aws apigateway get-rest-apis

```
root@Kali ~ aws apigateway get-rest-apis
{
    "items": [
        {
            "id": "4xn6jt50a6",
            "name": "iam-based-auth",
            "createdDate": 1613658554,
            "apiKeySource": "HEADER",
            "endpointConfiguration": {
                "types": [
                    "EDGE"
                ]
            },
            "disableExecuteApiEndpoint": false
        },
        {
            "id": "57z6f0kgxi",
            "name": "demo",
            "createdDate": 1613658554,
            "apiKeySource": "HEADER",
            "endpointConfiguration": {
                "types": [
                    "EDGE"
                ]
            },
```

Step 5: Check API resources

Command: aws apigateway get-resources --rest-api-id 4xn6jt50a6

Step 6: Enumerate API resource HTTP methods.

Command: aws apigateway get-method --rest-api-id 4xn6jt50a6 --http-method GET --resource-id lmxnuv

Step 7: Check authorizers for API.

Command: aws apigateway get-authorizers --rest-api-id yz2duibd7a

```
root@Kali ~ aws apigateway get-authorizers --rest-api-id yz2duibd7a
{
    "items": []
}
root@Kali ~
```

Step 8: Check API keys for the AWS account.

Command: aws apigateway get-api-keys

```
root@Kali ~ aws apigateway get-api-keys
{
    "items": [
        {
            "id": "pex0pljl5h",
            "name": "Lab1GW2",
            "description": "Managed by Terraform",
            "enabled": true,
            "createdDate": 1613658554,
            "lastUpdatedDate": 1613658554,
            "stageKeys": []
        }
    ]
}
root@Kali ~
```

Step 9: Get API key details.

Command: aws apigateway get-api-key --api-key pex0pljl5h

```
root@Kali ~ aws apigateway get-api-key --api-key pex0pljl5h
{
    "id": "pex0pljl5h",
    "name": "Lab1GW2",
    "description": "Managed by Terraform",
    "enabled": true,
    "createdDate": 1613658554,
    "lastUpdatedDate": 1613658554,
    "stageKeys": [],
    "tags": {}
}
root@Kali ~
```

Step 10: Get API key values.

Command: aws apigateway get-api-key --api-key pex0pljl5h --include-value

```
root@Kali ~ aws apigateway get-api-key --api-key pex0pljl5h --include-value
{
    "id": "pex0pljl5h",
    "value": "2UkSM508yl8UoDOwUSZFR4n0oe5tdBU28Cxuj2f2",
    "name": "Lab1GW2",
    "description": "Managed by Terraform",
    "enabled": true,
    "createdDate": 1613658554,
    "lastUpdatedDate": 1613658554,
    "stageKeys": [],
    "tags": {}
}
root@Kali ~
```

Step 11: Enumerate API client certificates.

Command: aws apigateway get-client-certificates

```
File  Actions  Edit  View  Help
root@Kali ~ aws apigateway get-client-certificates
{
    "items": []
}
root@Kali ~
```

References:

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