Subdomain Discovery

Goals:

- Create and deploy a SAM app that will attempt to discover valid subdomains

Dependencies:

- Cloud9 IDE was created previously, see previous lab entitled: "Cloud9 & SAM 101"

- Understanding the content within the lab: "HTTP GET Parameters"

- Understanding the content within the lab: "Local Debug & Testing"

Code & Files:

- https://github.com/Stage2Sec/CaptureTheCloud/tree/master/train_aws_sam

Login to the Student AWS Red Team Account

AWS Login: **https://console.aws.amazon.com/ (https://console.aws.amazon.com/)**

IAM Username: <red_team_###>

IAM Password: <password>

Cloud9 IDE Environment

Region: US East (N. Virginia) us-east-1

Service: Cloud9

Locate the "HelloWorld101" Cloud9 environment

Click the "Open IDE" button

In the terminal, run the following command(s) to build a sample using **python 3.6**:

```
cd /home/ubuntu/environment

sam init

1

1

11

subdomain-app-001

1
```

We should see output similar to the following:

```
red_team_040:~/environment $ cd /home/ubuntu/environment


red_team_040:~/environment $ sam init


Which template source would you like to use?
1 - AWS Quick Start Templates
2 - Custom Template Location
Choice: 1


What package type would you like to use?
1 - Zip (artifact is a zip uploaded to S3)
2 - Image (artifact is an image uploaded to an ECR image repository)
Package type: 1



Which runtime would you like to use?
1 - nodejs14.x
2 - python3.9
3 - ruby2.7
4 - go1.x
5 - java11
6 - dotnetcore3.1
```

```
7 - nodejs12.x
8 - nodejs10.x
9 - python3.8
10 - python3.7
11 - python3.6
12 - python2.7
13 - ruby2.5
14 - java8.al2
15 - java8
16 - dotnetcore2.1


Runtime: 11

Project name [sam-app]: subdomain-app-001

Cloning from https://github.com/aws/aws-sam-cli-app-templates

AWS quick start application templates:
1 - Hello World Example
2 - EventBridge Hello World
3 - EventBridge App from scratch (100+ Event Schemas)
4 - Step Functions Sample App (Stock Trader)
Template selection: 1

-----------------------
Generating application:
-----------------------
Name: subdomain-app-001
Runtime: python3.6
Dependency Manager: pip
Application Template: hello-world
Output Directory: .

Next steps can be found in the README file at ./subdomain-app-001/README.md

red_team_040:~/environment $
```

Code the App

Inspect the source code of the following files:

- template.yaml -> /home/ubuntu/environment/subdomain-app-001/template.yaml

-- SAM Template that defines your application's AWS resources

Change the "Path" to be the URI "subdomain" in the "template.yaml" file:

```
...

Globals:

Function:

Timeout: 900

...

Properties:

CodeUri: subdomain/

Handler: app.lambda_handler

Runtime: python3.6

Timeout: 900

MemorySize: 512

Events:

HelloWorld:

Type: Api

Properties:

Path: /subdomain

Method: get

...
```

Click "File" -> "Save" or Ctrl+S on Windows, to save the "template.yaml" file

Next, move the "hello_world" directory to be called "subdomain":

```
pwd
```

```
cd /home/ubuntu/environment/subdomain-app-001/

ls -alF

mv hello_world/ subdomain/

ls -alF
```

We should see output similar to the following:

```
red_team_040:~/environment $ pwd
/home/ubuntu/environment


red_team_040:~/environment $ cd /home/ubuntu/environment/subdomain-app-001/


red_team_040:~/environment/subdomain-app-001 $ ls -alF
total 40
drwxrwxr-x 5 ubuntu ubuntu 4096 Sep 23 21:45 ./
drwxr-xr-x 6 ubuntu ubuntu 4096 Sep 23 21:45 ../
-rw-rw-r-- 1 ubuntu ubuntu 3730 Sep 23 21:45 .gitignore
-rw-rw-r-- 1 ubuntu ubuntu 8240 Sep 23 21:45 README.md
-rw-rw-r-- 1 ubuntu ubuntu 0 Sep 23 21:45 __init__.py
drwxrwxr-x 2 ubuntu ubuntu 4096 Sep 23 21:45 events/
drwxrwxr-x 2 ubuntu ubuntu 4096 Sep 23 21:45 hello_world/
-rw-rw-r-- 1 ubuntu ubuntu 1643 Sep 23 21:45 template.yaml
drwxrwxr-x 3 ubuntu ubuntu 4096 Sep 23 21:45 tests/


red_team_040:~/environment/subdomain-app-001 $ mv hello_world/ subdomain/


red_team_040:~/environment/subdomain-app-001 $ ls -alF
total 40
drwxrwxr-x 5 ubuntu ubuntu 4096 Sep 23 23:44 ./
drwxr-xr-x 9 ubuntu ubuntu 4096 Sep 23 23:43 ../
-rw-rw-r-- 1 ubuntu ubuntu 3730 Sep 23 23:43 .gitignore
-rw-rw-r-- 1 ubuntu ubuntu 8240 Sep 23 23:43 README.md
-rw-rw-r-- 1 ubuntu ubuntu 0 Sep 23 23:43 __init__.py
drwxrwxr-x 2 ubuntu ubuntu 4096 Sep 23 23:43 events/
drwxrwxr-x 2 ubuntu ubuntu 4096 Sep 23 23:43 port_check/
-rw-rw-r-- 1 ubuntu ubuntu 1643 Sep 23 23:43 template.yaml
drwxrwxr-x 3 ubuntu ubuntu 4096 Sep 23 23:43 tests/
```

```
red_team_040:~/environment/subdomain-app-001 $
```

Inspect the source code of the following files:

- app.py -> /home/ubuntu/environment/subdomain-app-001/subdomain/app.py

-- Contains the logic/code for your lambda application

Change the code so it looks like the following file: **https://github.com/Stage2Sec/CaptureTheCloud/blob/master/train_aws_sam/subdomain-app-001/subdomain/app.py** **(https://github.com/Stage2Sec/CaptureTheCloud/blob/master/train_aws_sam/subdomain-app-001/subdomain/app.py)**

Click "File" -> "Save" or Ctrl+S on Windows, to save the "app.py" file

Add the "namelist.txt" file into the same directory as the "app.py" file: **https://github.com/Stage2Sec/CaptureTheCloud/blob/master/train_aws_sam/subdomain-app-001/subdomain/namelist.txt** **(https://github.com/Stage2Sec/CaptureTheCloud/blob/master/train_aws_sam/subdomain-app-001/subdomain/namelist.txt)**

Build and Deploy

Build and Deploy the app:

```
cd /home/ubuntu/environment/subdomain-app-001

sam build

sam deploy --guided



subdomain-app-001

...
```

We should see output similar to the following...

```
red_team_040:~/environment/subdomain-app-001 $ pwd
/home/ubuntu/environment/subdomain-app-001
red_team_040:~/environment/subdomain-app-001 $ sam build
Building codeuri: /home/ubuntu/environment/subdomain-app-001/subdomain runtime: python3.6
metadata: {} functions: ['HelloWorldFunction']
Running PythonPipBuilder:ResolveDependencies
Running PythonPipBuilder:CopySource

Build Succeeded

Built Artifacts : .aws-sam/build
Built Template : .aws-sam/build/template.yaml

Commands you can use next
=========================
[*] Invoke Function: sam local invoke
[*] Deploy: sam deploy --guided


red_team_040:~/environment/subdomain-app-001 $ sam deploy --guided

Configuring SAM deploy
======================

Looking for config file [samconfig.toml] : Not found

Setting default arguments for 'sam deploy'
=========================================
Stack Name [sam-app]: subdomain-app-001
AWS Region [us-east-1]:
#Shows you resources changes to be deployed and require a 'Y' to initiate deploy
Confirm changes before deploy [y/N]: y
#SAM needs permission to be able to create roles to connect to the resources in your template
Allow SAM CLI IAM role creation [Y/n]: y
HelloWorldFunction may not have authorization defined, Is this okay? [y/N]: y
Save arguments to configuration file [Y/n]: y
SAM configuration file [samconfig.toml]:
SAM configuration environment [default]:

Looking for resources needed for deployment:
Managed S3 bucket: aws-sam-cli-managed-default-samclisourcebucket-1sivrgk5lqe6g
A different default S3 bucket can be set in samconfig.toml

Saved arguments to config file
Running 'sam deploy' for future deployments will use the parameters saved above.
```

```
The above parameters can be changed by modifying samconfig.toml
Learn more about samconfig.toml syntax at
https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-sam-cli-config.html

Uploading to subdomain-app-001/08f8169c02c7610bf1c165b282cbc5dc 445795 / 445795 (100.00%)

Deploying with following values
================================
Stack name : subdomain-app-001
Region : us-east-1
Confirm changeset : True
Deployment s3 bucket : aws-sam-cli-managed-default-samclisourcebucket-1sivrgk5lqe6g
Capabilities : ["CAPABILITY_IAM"]
Parameter overrides : {}
Signing Profiles : {}

Initiating deployment
=====================
Uploading to subdomain-app-001/ef7b8ea5786e9dc5d3147bd6f54e931e.template 1252 / 1252 (100.00%)

Waiting for changeset to be created..

CloudFormation stack changeset
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
Operation LogicalResourceId ResourceType Replacement
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
+ Add HelloWorldFunctionHelloWorldPermissionProd AWS::Lambda::Permission N/A
+ Add HelloWorldFunctionRole AWS::IAM::Role N/A
+ Add HelloWorldFunction AWS::Lambda::Function N/A
+ Add ServerlessRestApiDeployment3caa84f1bd AWS::ApiGateway::Deployment N/A
+ Add ServerlessRestApiProdStage AWS::ApiGateway::Stage N/A
+ Add ServerlessRestApi AWS::ApiGateway::RestApi N/A
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Changeset created successfully. arn:aws:cloudformation:us-east-1:580299357056:changeSet/samcli-deploy1632447663/a431542c-58e6-4cda-8332-1448d05801fa


Previewing CloudFormation changeset before deployment
```

```
============================================================
Deploy this changeset? [y/N]: y

2021-09-24 01:41:16 - Waiting for stack create/update to complete

CloudFormation events from changeset
------------------------------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------
ResourceStatus ResourceType LogicalResourceId ResourceStatusReason
------------------------------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------
CREATE_IN_PROGRESS AWS::IAM::Role HelloWorldFunctionRole -
CREATE_IN_PROGRESS AWS::IAM::Role HelloWorldFunctionRole Resource creation Initiated
CREATE_COMPLETE AWS::IAM::Role HelloWorldFunctionRole -
CREATE_IN_PROGRESS AWS::Lambda::Function HelloWorldFunction -
CREATE_IN_PROGRESS AWS::Lambda::Function HelloWorldFunction Resource creation Initiated
CREATE_COMPLETE AWS::Lambda::Function HelloWorldFunction -
CREATE_IN_PROGRESS AWS::ApiGateway::RestApi ServerlessRestApi -
CREATE_IN_PROGRESS AWS::ApiGateway::RestApi ServerlessRestApi Resource creation Initiated
CREATE_COMPLETE AWS::ApiGateway::RestApi ServerlessRestApi -
CREATE_IN_PROGRESS AWS::ApiGateway::Deployment ServerlessRestApiDeployment3caa84f1bd -
CREATE_IN_PROGRESS AWS::ApiGateway::Deployment ServerlessRestApiDeployment3caa84f1bd
Resource creation Initiated
CREATE_IN_PROGRESS AWS::Lambda::Permission HelloWorldFunctionHelloWorldPermissionProd -
CREATE_COMPLETE AWS::ApiGateway::Deployment ServerlessRestApiDeployment3caa84f1bd -
CREATE_IN_PROGRESS AWS::Lambda::Permission HelloWorldFunctionHelloWorldPermissionProd
Resource creation Initiated
CREATE_IN_PROGRESS AWS::ApiGateway::Stage ServerlessRestApiProdStage -
CREATE_IN_PROGRESS AWS::ApiGateway::Stage ServerlessRestApiProdStage Resource creation
Initiated
CREATE_COMPLETE AWS::ApiGateway::Stage ServerlessRestApiProdStage -
CREATE_COMPLETE AWS::Lambda::Permission HelloWorldFunctionHelloWorldPermissionProd -
CREATE_COMPLETE AWS::CloudFormation::Stack subdomain-app-001 -
------------------------------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------

CloudFormation outputs from deployed stack
------------------------------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------
Outputs
------------------------------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------
Key HelloWorldFunctionIamRole
```

```
Description Implicit IAM Role created for Hello World function
Value arn:aws:iam::580299357056:role/subdomain-app-001-HelloWorldFunctionRole-SRLDVXIW66SN

Key HelloWorldApi
Description API Gateway endpoint URL for Prod stage for Hello World function
Value https://ty6pqvk7lb.execute-api.us-east-1.amazonaws.com/Prod/hello/

Key HelloWorldFunction
Description Hello World Lambda Function ARN
Value arn:aws:lambda:us-east-1:580299357056:function:subdomain-app-001-HelloWorldFunction-yiJRGcQrASwa
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Successfully created/updated stack - subdomain-app-001 in us-east-1

red_team_040:~/environment/subdomain-app-001 $
```

Test Deployment

Let's test our deployment (change the URL to the URL created for your deployment):

```
curl https://ty6pqvk7lb.execute-api.us-east-1.amazonaws.com/Prod/subdomain/?RootDomainName=lizardblue.com
```

We should see output similar to the following:

```
red_team_040:~/environment/subdomain-app-001 $ curl https://ty6pqvk7lb.execute-api.us-east-1.amazonaws.com/Prod/subdomain/?RootDomainName=lizardblue.com


[+] START
[+] Subdomain discovered: cdn.lizardblue.com -> 52.217.194.113
[+] Subdomain discovered: cdn2.lizardblue.com -> 52.219.105.19
[+] Subdomain discovered: hash.lizardblue.com -> 52.85.61.12, 52.85.61.64, 52.85.61.65, 52.85.61.94
[+] Subdomain discovered: images.lizardblue.com -> 52.219.142.28
[+] Subdomain discovered: ixhash.lizardblue.com -> 3.226.63.115, 3.228.53.222, 3.230.230.89, 3.232.236.175, 34.193.24.255, 52.73.45.196, 54.172.93.56, 54.80.73.136
[+] END
```

Clean Up

SAM uses the AWS CloudFormation service to deploy resources, hence we can use the CloudFormation service to clean up the SAM application deployment. We will need to know the following information:

#1 - Stack Name: e.g. sam-app-001

#2 - AWS Region: e.g. us-east-1

In the terminal, run the following command(s):

```
aws cloudformation delete-stack --stack-name sam-app-001 --region us-east-1
```

We should see output similar to the following:

```
red_team_040:~/environment/sam-app-001 $ aws cloudformation delete-stack --stack-name sam-app-
001 --region us-east-1


red_team_040:~/environment/sam-app-001 $
```

Next we can check to ensure the delete was succuessful...

In the terminal, run the following command(s):

```
aws cloudformation list-stacks
```

We should see output similar to the following:

```
red_team_040:~/environment/sam-app-001 $ aws cloudformation list-stacks
{
"StackSummaries": [
{
"StackId": "arn:aws:cloudformation:us-east-1:580299357056:stack/sam-app-001/7704fd60-1b1d-11ec-
8228-0eea388cb225",
"StackName": "sam-app-001",
"TemplateDescription": "sam-app-001\nSample SAM Template for sam-app-001\n",
"CreationTime": "2021-09-21T20:49:50.792Z",
"LastUpdatedTime": "2021-09-21T20:52:28.346Z",
"DeletionTime": "2021-09-21T21:00:06.896Z",
"StackStatus": "DELETE_COMPLETE",
"DriftInformation": {
"StackDriftStatus": "NOT_CHECKED"
}
},

...
```

References

Tutorial: Deploying a Hello World application - **https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-getting-started-hello-world.html** **(https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/serverless-getting-started-hello-world.html)**