SecOps CTF Lab Documentation

Palo Alto Networks

Aug 03, 2020

Contents:

CHAPTER 1

Introduction

Overview

CHAPTER 2

QUICKSTART

Do these steps to get your local machine ready.

2.1 Prepare your local environment.

- Add your public key half to /gcp/config/authorized_keys file
- For example:

```
cat ~/.ssh/.id_rsa.pub >> {PATH_TO_REPO_CLONE}/gcp/config/authorized_keys
```

- Create a file called /aws/terraform.tfvars
- For example:

```
project_id  = ""                    # Put your GCP Project ID.
bucket_name = "my-bucket-48693"     # Put the desired GCS Bucket name.
```

- Run the "config" script in this repo.
- Correct the errors until you get output as below.

2.2 Log in via gcloud

- Be sure to use your gmail or personal account
- Do not use your palo alto email to sign in.

```
gcloud auth login
gcloud projects list
gcloud projects create secops-iac-ctf-000378
gcloud config set project secops-iac-ctf-000378
```

- Use the cloud console to create a service account
- Save the file and then do like so:

```
export GOOGLE_APPLICATION_CREDENTIALS="/Users/fdiaz/.config/gcloud/secops-iac-ctf-
↪000378-ca7e78916a38.json"
```

- create a bucket to store your tfstate file

2.3 Terraform Time

```
cd gcp/deployment
terraform init
terraform plan -out franklin.out
terraform apply "franklin.out"
```

CHAPTER 3

Images

We have two buckets. One is permanent, called "ctf-backup". The other is setup and torn down by Terraform. We keep the images in this permanent bucket so they can be copied into the lab network on the fly as it is stood up and torn down.

3.1 Upload Images to Bucket

- Create .ova/ovf images as desired.
- Upload these images into the permanent "ctf-backup" bucket.
- The images should appear as below when finished.

```
fdiaz at REMMAC11ELVDT ~   gsutil ls gs://ctf-backup/
↪             deployment
gs://ctf-backup/Ubuntu-1.ova
gs://ctf-backup/W7P_x64.ova
```

You might like to transfer images from Google Drive to GCP Storage Bucket using colab: https://colab.research.google.com/drive/1ZZuWEBOrD8Twb78kpY18Cf9g27MfdD-M

3.2 Stand up Instances with GCP

Once the OVA/OVF images have been uploaded to a GCP Storage bucket, we need to create Compute Instances from them. We can use these directions

The command to create the Compute Instance should look like so:

```
gcloud compute instances import ubuntu1-secops-ctf-000378 --source-uri=gs://ctf-
↪backup/Ubuntu-1.ova --os=ubuntu-1804
```

You can verify that it worked properly like so:

```
 gcloud compute instances list
NAME                          ZONE        MACHINE_TYPE   PREEMPTIBLE  INTERNAL_IP ␣
↪EXTERNAL_IP     STATUS
ubuntu1-secops-ctf-000378  us-west1-a  n1-standard-1               10.138.0.6   35.
↪203.185.100  RUNNING
```

CHAPTER 4

Visual Studio Code Setup

From Command Palette:

Terraform: Enable Install/Update Language Server

CHAPTER 5

Packer

```
gcloud compute images list --project debian-cloud-testing --no-standard-images
```