Justin Slade

G00409678

CS 435

Fall 2024

Big Data & Cloud Security

AWS Lab Report 7.1

Date: 10/08/2024

Grambling State University

Big Data and Cloud Security

**Purpose or Objective:** Learn how to monitor EC2 Security groups, understand what ports should be available to certain groups, and learn how to remediate an incident should one happen.

**Procedure/s:**

* Updating IAM roles
* Securing groups
* Monitor ec2 groups with aws config
* Resolve incidents with lambda

**Task 1.**

I need to update the Current IAM roles available to make sure they are ready for future services that AWS offers.

A screenshot of a computer program

Description automatically generatedI check one group called AwsConfigLambdaSGRole to ensure that they have the necessary permissions provided to them. I repeat this process with every roll needed to be examined to make sure no role has been compromised.

A screenshot of a computer

Description automatically generated

The AWS config role didn’t have a role granted to them so I gave them the required role for this lab.

**Task 2.**

Now I need to set up AWS Config so I can monitor all activity happening in my lab environment.

A screenshot of a computer

Description automatically generatedThis is me setting up the presets for the AWS Config.

A screenshot of a computer

Description automatically generated

Then I set up the resources that I’m able to track utilizing AWS config.

**Task 3.**

Now I’m purposefully creating a group to simulate in incident via the VPC services aws provides.

A screenshot of a computer

Description automatically generatedThis is the lab thay I will be influencing for this exercise.

A screenshot of a computer

Description automatically generatedcurrently creating all the inbound ports for this exercise.

**Task 4.**

In this task I will be using AWS config to evoke lambda functions to ensure my ec2 groups are secure.

A screenshot of a computer program

Description automatically generatedThis is me creating a rule for my EC2 group so I can monitor and restrict access to specified ports.

A screenshot of a computer

Description automatically generatedEvery thing is working properly due to the rules being compliant since I changed the permissions to allow them to work.

**Task 5.**

Lastly I need to Check my config to see if the changes I proposed are seeable and fixable.

A screenshot of a computer

Description automatically generatedThere is a slight issue in that they only accept HTTP and HTTPS but the not the other two ports I allowed.

Task 6. Check the cloud watch to see what actually happend

A screenshot of a computer

Description automatically generated

In these log files in cloud watch If I did expand these files I can see that these logs would have expressly stated that the other two ports allowed open is being shut down because of some lambda script I open in the previous task.

**Conclusions:**

This lab was actually very involved with a lot of moving parts that did admittedly felt a bit too automated for my liking. This is because I felt I didn’t actually feel like I contributed to the lab despite getting full marks because I was able to observed everything that happened. Overall it was nice to see that there are just a bunch of systems in place that even though I actively sabotaged the lab Lambda and AWS config was able to quickly remedy it and log it all on AWS Cloud watch.

**Knowledge Check (7) Screenshot:**

A screenshot of a test results

Description automatically generated