CPE-321 Introduction of Computer Security

Lab: Access Control in Amazon Web Services (AWS)

DeBruhl/Hartman – 10/15/2022

Objectives

The objectives for this lab assignment are as follows:

- To explore advanced access control using AWS cloud services
- Analyze the strengths and weakness of AWS access control

Background

In this lab, you will explore a real-world identity and access management solution, namely AWS IAM. AWS includes a wide spectrum of built-in security mechanisms, including granular permissions, secure access to AWS resources for applications that run on Amazon EC2, multi-factor authentication (MFA), and identity federation. For this lab, we will concentrate on secure access to AWS resources, especially S3 storage buckets.

The AWS Academy Cloud Security Foundations course provides a general introduction to the identity and access management features of AWS. The lab focuses only on Lab 3.1 in Module 3, but feel free to look at the other material and labs in the course if you're interested:

- Module 1: Overview -- Short videos on objectives
- Module 2: Intro to Security on AWS – Videos on overview and design principles – overlaps many of our previous lectures.

- Module 3: Securing Access to Cloud Resources: There are several short videos of content covered in our IAM lectures that are worth watching. Lab 3.1 is our focus for this exercise.
- Module 4: Securing your infrastructure – Discusses AWS network security, which we have not yet covered.
- Module 5: Encrypting data / key management – overlaps with our previous discussions on encryption.
- Module 6: Logging and Monitoring – not covered.
- Module 7: Responding to and Managing an Incident – not covered.
- Module 8: Bridging to Certification – not covered.
- End of Course Assessment: not used.

A great advantage of using the lab through this course is that it takes care of provisioning and configuring your management console, EC2 instances, and S3 buckets. All you need to do is follow the instructions to run the lab.

To begin the lab, please be sure you have accepted the invite to join the AWS Academy and have registered in the AWS Canvas course. Note that the AWS Canvas course is a separate version of Canvas from our CSC-321 Canvas.

In the AWS Academy Cloud Security Foundations canvas course, navigate to Module 3 Securing Access to Cloud Resources. After watching the videos in this module, please carefully follow instructions to run Lab 3.1: Using Resource-Based Policies to Secure an S3 Bucket. Do the entire Lab 3.1, including the challenge task, and hit "submit" as directed at the end of the lab instructions so AWS

Academy Canvas will record your successful completion. **Every person in your group must individually complete the lab for credit in this module.**

While you do the hands-on lab, the group should answer the following questions about the lab and submit it in the 321 Canvas course. Provide one submission that answers the questions for everyone in your group.

Questions:

Task 1: Accessing the console as an IAM user

Do you think the kind of authentication you used to login was a good choice? Why or why not? Does AWS provide alternative authentication mechanisms?

Task 2: Attempting read-level access to AWS services

What is EC2, and why are there so many API errors displayed? What is S3, and what is contained in the buckets?

Task 3: Analyzing the identity-based policy applied to the IAM user

Why can't you see the security recommendations and IAM resources? What does the JSON in DeveloperGroupPolicy describe? Why do you think you were permitted to copy the JSON?

Task 4: Attempting write-level access to AWS services

What policy permitted you to create a bucket? Why did the upload fail, and what permission do you need so it will succeed? What were your impressions on the listing of Actions Defined by Amazon S3, and how easy was it for you to understand them?

Task 5: Assuming an IAM role and reviewing a resource-based policy

Why could you switch roles? Where in the U.S. is the photo in Image2.jpg taken from? How can assuming roles encourage least privilege?

Task 6: Understanding resource-based policies

Explain how the role-based and resource-based policies interact to permit access to different buckets for BucketsAccessRole.

Challenge task

How did you upload Image2.jpg to bucket3? Can you access other buckets? Why or why not?

Capital One Breach

Based your experience with AWS IAM during this lab, what is your hypothesis on how errors in S3 security policies affected the Capital One breach that was discussed in lecture? What advice would you give Capital One to fix their policies and avoid another breach? What advice would you give AWS to improve their IAM so their customers would not make mistakes like this again?

Submission: Include answers to all questions. Please include any explanations of the surprising or interesting observations you made.

Write at a level that demonstrates your technical understanding, and do not shorthand ideas under the assumption that the reader already "knows what you

mean”. Think of writing as if the audience was a smart colleague who may not have taken this class.

Submit your completed write up to Canvas in PDF format.