Cloud Security, Spring 2024, CS-GY 9223

Final Project
In-class Presentations: April 25, May 2
Final write ups due: May 12

The final project is designed for you to put together the knowledge you've gained throughout the course in a real-world AWS implementation. It is also an opportunity to work with and get to know your fellow students.

For the final project, you will build a solution in AWS to solve a particular cloud security problem you've identified. You are free to use any AWS tools at your disposal, though you will want to be mindful of costs. You will be assigned to a group of 3-4 people by the instructors.

Deliverables

You will give a presentation and demo of your work during class on April 25th or May 2nd. Presentations **must not** exceed 10 minutes in length. Please rehearse your presentation to ensure you're able to stay within these time limits, as we will have many presentations to get through. You will be assigned a presentation date at the time your groups are assigned. You will also submit a writeup in the form of a 1-2 page lab report due on May 12th.

Your presentation should address the following five main points and will be graded using these criteria:

1. Problem Statement - What is the problem you're trying to solve with your solution
    - Student clearly states the problem - 10 pts
    - Unclear problem statement - 5 pts
    - No problem statement - 0 pts

2. Initial proposal/design - What was your initial proposed solution to address the problem
    - Student provides a clear explanation or diagram of initial solution and scope is appropriate to the time allowed - 20 pts
    - Initial scope and proposal is unclear and does not address the problem - 10 pts
    - No initial design provided - 0 pts

3. Issues encountered - What were the problems you encountered (if any) along the way to doing the implementation
    - Student provided a clear description of issues encountered and workarounds - 20 pts
    - Issues encountered weren't clearly described or were ambiguous - 15 pts
    - No discussion of issues encountered provided - 0 pts

4. Final design - what adjustments to your initial proposal did you make to get to your implementation
    - Proposed scope was successfully delivered with any necessary adjustments - 30 pts
    - No changes made from initial design based on learnings and applying lessons learned - 25 pts
    - Delivered on less than 50% of the proposed scope - 20 pts
    - Delivered on less than 25% of the proposed scope - 10 pts
    - Did not deliver any implementation - 0 pts

5. Lessons learned/Future work - What would you have done differently, knowing what you know now? What additional features would you have implemented if you had more time?
    - Student provided at least two additional feature suggestions or areas of improvement - 20
    - Student provided at least one feature suggestion or area of improvement - 15 pts
    - Student did not provide any feature suggestions or ideas for improvement - 0 pts

For the lab write-up, students will need to submit a writeup in the form of a 1-2 page lab report. The lab write-up should follow the same format as the presentation, addressing the same five questions.

Example project ideas:

- Fraud detection: this is a form of security. You could use the CloudWatch logs and run it through Kafka into a Hadoop server and run Spark/MapReduce Analytics on it to detect fraud or anomalies

- Similarly, use CloudWatch to trigger lambdas to retrieve messages from the message queue, that identify potentially malicious behavior

- Connect CloudWatch data to a visualization tool for analysis

- Build a continuous monitoring system with AWS, similar to Splunk. Feel free to use canned data or logs available online.

- Take sample data, store it in S3 and use it for security analysis with other AWS tools

- Encryption/Decryption pipeline:
    - Have a controlled key management system for two users
    - Starting with unencrypted data, create a data pipeline to ingest and encrypt that existing data.
    - Read the encrypted data in S3 through another pipeline

- Build an implementation of an AWS Clean room using sample data

- If there is some known technology you already use or have experience with, integrate some AWS security features to it

- Setup a publicly shared CloudFormation template, run a security tool, such as ScoutSuite, Quiet Riot or Prowler, and report on the issues identified by the security tool

- Build an SLSA architecture in AWS: https://slsa.dev/get-started

- Build a CI/CD pipeline with security testing automated as part of the build pipeline

- Work thru an existing workshop and propose improvements and/or extensions to the workshops

Resources:
Public CloudTrail dataset:
https://summitroute.com/blog/2020/10/09/public_dataset_of_cloudtrail_logs_from_flaws_cloud/

Workshops:
https://github.com/aws-samples/aws-serverless-security-workshop
https://aws.amazon.com/blogs/security/2021-aws-security-focused-workshops/
https://aws.amazon.com/blogs/security/aws-cirt-announces-the-release-of-five-publicly-available-workshops/

Tools:
https://github.com/nccgroup/sadcloud

List of tool ideas:
https://summitroute.com/blog/2021/02/16/aws_security_project_ideas/