EE/CprE/SE 492 WEEKLY REPORT 4
2/24/2024 - 3/30/2024

Group number: sdmay24-11
Project title: Damn Vulnerable AWS API
Client: RSM - Jon Schnell
Advisor: Julie Rursch
Team Members/Role:
Garrett Arp - Team Website Lead
Ashler Benda - Client Interaction
Karthik Kasarabada - Client Interaction
Andrew Bowen - Scrum Master
Ahmed Nasereddin - Identity & Access Management
Ayo Ogunsola - Identity & Access Management
Ethan Douglass - Testing Lead

o Weekly Summary

During this period, we finished all of the individual components of the attack paths. With the completion of each part, we started to document the steps to complete each component. We also started working on merging the components into one template and standardizing formats. Some testing was completed as well along with reflection on what documentation we need after receiving feedback from another team.

o Past Week(s) Accomplishments

- Garrett Arp - Finished priv escalation 2, looting 2, and went through initial entry to document the steps needed.
- Ashler Benda - Created access key, iam user, policy for connection w Karthik's components. Updated database
- Karthik Kasarabada - Created and debugged all components to Inital Entry for AP1, Looting, and and Priv Esc 1(With Ashler) the template. API GET and POST pathway reworked. Integration testing between the part of attack path I am responsible for have also been completed.
- Andrew Bowen - I added an EC2 instance to my template so that it will be deleted with the rest of the resources when the user is done with the attack path. To do so, I had to work with VPC and Subnet resources as well. Additionally, I created outlines for the documentation we must have for client.
- Ahmed Nasereddin - Finished the implementation of privilege escalation 2 and looting 2, tested them individually, and they seem to be working.
- Ayo Ogunsola - Finished the implementation of privilege escalation 2 and looting 2, tested them individually, and they seem to be working.
- Ethan Douglass - Finished priv escalation 2 and looting 2

o Individual Accomplishments

Name	Hours this period	Hours cumulative
Garrett Arp	7	21
Ashler Benda	7	18
Karthik Kasarabada	15	29
Andrew Bowen	15	31
Ahmed Nasereddin	5	19
Ayo Ogunsola	7	23
Ethan Douglass	6	36

o Plans for the upcoming period

- Garrett Arp - Need to test priv esc 2 and looting 2 in one full go. Need to test the entire attack path. Need to find a for sure way to put starting data into S3 buckets. Need to go through documentation and make sure we are not missing anything.
- Ashler Benda - Create template to populate RDS database, work on testing between components, finalize documentation.
- Karthik Kasarabada - Main Focus is to begin integration testing for the combined template. Work on documentation for my part of the remediation and solution guides and explore public repository options to populate narrative data with Andrew.
- Andrew Bowen - My focus for the upcoming period will be writing documentation for the client. I will write an introduction to AWS for the users as well as my part of the remediation and solution guides.
- Ahmed Nasereddin - Populate s3 bucket in looting 2 phase with “sensitive info” that is tied to the scenario our attack path chooses. Along with aiding in the creation/formation of the cloud formation template for the attack path.
- Ayo Ogunsola - Continued testing and creation of cloudformation template for the first part of the attack path. Assisted in debugging the final parts of the latter half of the attack path, and began stack testing.
- Ethan Douglass - Create the template for attack path 2 and work on the introduction documentation required for the client.

o Issues

During our client meeting, we talked about progress and future plans. We realized we need to find a way to populate the narrative data necessary for the attack paths. This is not something we thought of during our planning phase.

o Midterm Review

Summary of Feedback

Most of the feedback about limitations and suggestions from the other team was related to the simplicity of the vulnerabilities and ways to find the vulnerabilities. Part of our plan that wasn't mentioned in the video was creating documentation for each step of the attack path. This is one of our last milestones after the attack paths are implemented. As for the limitation of the types of vulnerabilities, we were aware of this when creating the designs. We are limited by the amount of time we have for this. Additionally, we are limited by the legal policies of AWS. Significant vulnerabilities would potentially already be patched by AWS or be illegal by their policies to exploit.

The feedback was positive about the design and having two attack paths. We didn't provide a clear idea about the exact amount of progress and how to evaluate that in quantitative value. There were also concerns about the tool's safety and malicious use. We addressed those concerns because the Initial Entry methods are internal and can't be accessed from the Internet.

Insights

One of the questions was about using an existing stack to design these attack paths. While this would not work for us, this is a potential solution if RSM wants to create more complex attack paths in the future. Another great question was about the different levels of knowledge and how to cater to that. We planned to develop a step-by-step walkthrough, which would be great for the beginner level. We can look into creating a second document geared towards middle-level experience. Another part of the documentation will ensure we add a list of terms and definitions the user should know.

Next Steps

We decided to add another document focused on information about AWS, including the terms and definitions suggested by our review team. We will also add more information about how the project is secure as well as a disclaimer that we aren't responsible for any issues. We decided not to create a middle-level experience document at this time.

o Weekly Advisor/Client Meeting

Attendance: Jon Schnell, Julie Rursch, Ashler Benda, Nasereddin, Garrett Arp, Ethan Douglass, Andrew Bowen, Karthik Kasarabada, Ayo Ogunsola
Meeting Date: 2/26/2024

Agenda:

- S3 Bucket and Starting Data
    - Discuss how to populate data into databases
        - No tag in Templates
        - Best option would be to have RSM host a public repository to pull resources from
            - Github or S3 bucket with Lambda to clone
- Make sure to add a deletion policy to our templates

Attendance: Ashler Benda, Nasereddin, Garrett Arp, Ethan Douglass, Andrew Bowen, Karthik Kasarabada, Ayo Ogunsola
Meeting Date: 3/25/2024

Agenda:

- Start full system testing next week
    - Finish merging individual components to one template this week
    - Need to find ways to populate narrative
- Setup structure for documentation and started working on it
    - Eventually, transfer documentation to a Git Wiki
- Three - four weeks left
    - Need to do Final Report/Poster/Presentation end of April