EE/CprE/SE 492 WEEKLY REPORT 3
2/10/2024 - 2/24/2024

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 - Assistant to the Identity & Access Management Intern Manager
Ayo Ogunsola - Identity & Access Management Lead
Ethan Douglass - Testing Lead

o Weekly Summary

This week, we continued to work on the individual units of the attack paths. A majority of the units are completed, our next step is to test the connection between units next as well as adding fake data to simulate a real environment. Our client recommended starting on the templates sooner rather than later so part of the work we are doing is converting parts that are done to Cloudformation Templates.

o Past Week(s) Accomplishments

- Garrett Arp - Created Roles/policies for attack path 2, utilized the newly created user to test functionality of new roles/policies. Able to create new ec2.
- Ashler Benda - Added security groups to VPC, successfully deployed template as a stack to account. Begin work on the database, AHEAD OF SCHEDULE 🙂 Created db template and parameters
- Karthik Kasarabada - Working on API Gateway/Lambda/S3 Stack in Cloud Formation, Expected to be done by 25th-26th.
- Andrew Bowen - Finished the persistence user Cloudformation template and validated it created the resources correctly. Started on the template design for the final privilege escalation.
- Ahmed Nasereddin - Created Roles/policies for second part of attack path 2, utilized the newly created user to test functionality of new roles/policies. Last thing needed implementing/testing is the passrole function. Everything that was added/done has been documented.
- Ayo Ogunsola - Helped get access and policy permission for attack path 2. Did documentation on attack path 2 steps and helped test user access/current implementation across the attack path.
- Ethan Douglass - Researched and implemented attack path 2 needed security policies. Created user and attached permissions for second half team. Consulted with client to rework permissions given to the engineer permissions boundary. Tested new user

policies by running through back half of attack path 2.

o Individual Accomplishments

Name	**Hours this week**	**Hours cumulative**
Garrett Arp	7	14
Ashler Benda	10	18
Karthik Kasarabada	4	14
Andrew Bowen	7	16
Ahmed Nasereddin	6	14
Ayo Ogunsola	9	16
Ethan Douglass	23	30

o Plans for the upcoming week

- Garrett Arp - Finish up the second part of attack path 2, add some “confidential information” to the last s3 bucket in order to simulate a real world breach scenario. Need to keep up with documentation.
- Ashler Benda - Finish the database and begin testing access with an EC2
- Karthik Kasarabada - Complete Cloud Formation stack, design PII documentation and create Developer Credentials for narrative
- Andrew Bowen - Finish privilege escalation 4 template, resolve errors in the template
- Ahmed Nasereddin - Finish up the second part of attack path 2, add some “confidential information” to the last s3 bucket in order to simulate a real world breach scenario.
- Ayo Ogunsola - Continue to go through the first part of attack path 2 and work on documentation to ensure it's up to date. Additionally, begin cloudformation work.
- Ethan Douglass - Finish and test first half of attack path 2. Start documentation and could formation templates. Test full attack path for completion.

o Broader Context

Our original context for Public Health, Safety and Welfare still applies. The original was well planned out with our client to ensure the information was correctly used. We will illustrate the protection portion of the context by documenting how to fix the issues in the remediation reports. Additionally, the project will only train employees focused on legal hacking. There is a risk of someone using the information to hack websites illegally, but since it is meant for internal company use only, we can’t do anything to reduce the risk. We also highlighted how our project will contribute to a culture of secure designs.

o Weekly Advisor/Client Meeting

Attendance: Jon Schnell, Julie Rursch, Ashler Benda, Ahmed Nasereddin, Garrett Arp, Ethan Douglass, Andrew Bowen, Karthik Kasarabada, Ayo Ogunsola
Meeting Date: 2/12/2024

Agenda:

- Updates
    - No CI/CD pipeline
    - Attack Path 2 going well
        - Initial entry framework is set
        - Starting on Privilege Escalation 1
        - Working in the Console first before creating CloudFormation Templates
            - Jon suggests beginning to work on a base template
- Json vs YML
    - Jon suggests JSON
    - Use tabs instead of spaces