EE/CprE/SE 492 WEEKLY REPORT 2
1/29/2024 - 2/10/2024

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

Individually, we started working on the separate parts of the attack paths. We are creating Cloudformation Templates for the individual components that will be connected together later in the process. Additionally, we will not use CI/CD with Gitlab. After research, we determined it is not as portable to GitLab as we had hoped. We were also unable to create the necessary credentials with given permissions. The CI/CD pipeline was a team decision for convenience, not required by the client so we are fine with not doing it.

o Past Week(s) Accomplishments

- Garrett Arp - Created and configured security group for attack path 2 initial entry ec2, team effort contribution to initial entry ec2
- Ashler Benda - Started VPC template in GitLab, tried to set up a CI/CD pipeline and determined it was not necessary
- Karthik Kasarabada - Got the API to actually return values from test Lambda when invoked, however, main lambda has some bugs
- Andrew Bowen - Created the Lab Workstation Developer role and user for attack path 1 persistence in AWS Console to figure out the policy settings. Started converting the determined policies into templates.
- Ahmed Nasereddin - Helped with initial entry set up with researching and understanding how to use django, configured security group/port numbers to allow certain traffic.
- Ayo Ogunsola - Helped get the initial entry logged in and set up. Installed initial django web app and initial code to get the website running on the ip properly.
- Ethan Douglass - Create ec2 for initial entry and then setup ssrf vulnerability with metadata service credential stealing and Set-Default-Policy permissions

o Individual Accomplishments

Name	Hours this week	Hours cumulative
Garrett Arp	3	7
Ashler Benda	4	8
Karthik Kasarabada	4	7
Andrew Bowen	4	9
Ahmed Nasereddin	4	8
Ayo Ogunsola	4	7
Ethan Douglass	4	7

o Plans for the upcoming week

- Garrett Arp -
- Ashler Benda - Finish VPC, start testing it
- Karthik Kasarabada - Finished API Gateway, investigating Lambda Bugs
- Andrew Bowen - Finish converting the EC2 User and Lab Workstation Developer role into cloud formation templates, then test deploying the templates.
- Ahmed Nasereddin - Finalize initial entry, split off into two smaller groups to build other components of attack path, like s3 buckets that rely on roles that contain previous versions with more permissions.
- Ayo Ogunsola - Finish off initial entry with the team then break out to build S3 buckets.
- Ethan Douglass - Finish initial entry and test. Break out to lateral movement and priv esc

o Weekly Advisor/Client Meeting

- **No meeting due to Advisor and Client not being available at regularly scheduled time**