3 Project Plan

3.1 Task Decomposition

Our tasks are listed below underneath each milestone in descending order. Tasks at the top need to be completed first before the next task within the milestone can be completed. See section 3.4 for our timeline of milestones which lays out how the tasks will be completed in relation to each other. These task only encompass the design phase and milestones at this time. The design aspects will decide what our tools and resources our implementation will use. Thus, we will define our semester 2 tasks as the semester goes, with the goal of having them documented for the final design document.

Initial Set of Exploits Defined

- **Complete flAWS Level 1-2**
- Complete flAWS Level 3-4
- Complete flAWS Level 5-6
  - These are a blogger's educational exercises on AWS exploits
- Define an exploit that could be used in an attack path and where it could be used
  - This will be completed for unique exploits for each student

Attack Path 1 Designed

- Recon Defined - Attack Path 1
  - Define exposed ports/services
- Initial Exploitation Defined - Attack Path 1
  - Define entry point through exposed ports/services
- Persistence and Privilege Escalation Defined - Attack Path 1
  - Define the initial foothold on the network/resources
- Lateral Movement Defined - Attack Path 1
  - Define what will be exposed from potential footholds
- Looting (Exfiltration) defined - Attack Path 1
  - Define critical information that will be present in the resources along the attack path
- Define a use case for each AWS service/resource - Attack Path 1
  - Review the resources used in the attack path and define how they are used in relation to the exploits and what intended use cases would be for a business

Remediation of Attack Path 1 Defined

- Vulnerability/misconfiguration remediation defined - Attack Path 1
  - Define how the exploits of attack path 1 occurred, how to fix them, how to avoid them
- Events and Actions defined - Attack Path 1

    - The key information gained and actions taken by the attacker are defined

Attack Path 2 Designed

- Recon Defined - Attack Path 2
    - Define exposed ports/services
- Initial Exploitation Defined - Attack Path 2
    - Define entry point through exposed ports/services
- Persistence and Privilege Escalation Defined - Attack Path 2
    - Define the initial foothold on the network/resources
- Lateral Movement Defined - Attack Path 2
    - Define what will be exposed from potential footholds
- Looting (Exfiltration) defined - Attack Path 2
    - Define critical information that will be present in the resources along the attack path
- Define a use case for each AWS service/resource - Attack Path 2
    - Review the resources used in the attack path and define how they are used in relation to the exploits and what intended use cases would be for a business

Remediation of Attack Path 2 Defined

- Vulnerability/misconfiguration remediation defined - Attack Path 2
    - Define how the exploits of attack path 1 occurred, how to fix them, how to avoid them
- Events and Actions defined - Attack Path 2
    - The key information gained and actions taken by the attacker are defined

Review/Refinement

- Cross Review - Attack Path 1
    - Attack path has been completed by all members of the team to give meaningful feedback for refinement
- Cross Review - Attack Path 2
    - Attack path has been completed by all members of the team to give meaningful feedback for refinement
- Refinement - Attack Path 1
    - Feedback from refinement has been implemented
- Refinement - Attack Path 2
    - Feedback from refinement has been implemented

Logging Strategy Defined

For each of these, define relative use cases for the project and their pro’s and con’s relative to our requirements

- Research CloudWatch
- Research EventBridge
- Identify Alternative Logging Resources

Narrative Defined

- Line of Business Defined - Attack Path 1
- Line of Business Defined - Attack Path 2
- Use Case for Services Defined for Narrative - Attack Path 1
- Use Case for Services Defined for Narrative - Attack Path 2
- User Roles Defined - Attack Path 1
- User Roles Defined - Attack Path 2

3.2 Project Management/Tracking Procedures

We will use the Agile project management style. We have various phases that the project will be broken up into. Each of our milestones will be the various sprints that our project is split into.

We will use GitLab for project management. The milestones will be Milestones in Gitlab. Under each Milestone, major tasks will be their own issue. When applicable, new branches will be made from the issues. Each major task will be split into smaller Tasks listed within the issue. There are two types of tasks, design and implementation, which will be determined by the label on the issue. We will follow the Agile style using the Issue boards. There are five boards: Open, In Progress, Stuck, Review, and Closed. The Open board will be the backlog and Closed will be the completed spot.

3.3 Project Proposed Milestones, Metrics, and Evaluation Criteria

Design Milestones (Semester 1)

- Initial Set of Exploits Defined
- Attack Path 1 Designed
- Remediation of Attack Path 1 Defined
- Attack Path 2 Designed
- Remediation of Attack Path 2 Defined
- Review/Refinement
- Logging Strategy Defined
- Narrative Defined

Implementation Milestones (Semester 2)

- User roles are created
- Implement Attack Path 1
- Remediation of Attack Path 1 Documentation Completed
- Implement Attack Path 2
- Remediation of Attack Path 2 Documentation Completed
- Logging setup
- Attack Paths Successfully Tested
- Remediation Documentations have been documented

(Quantitative) Metrics:

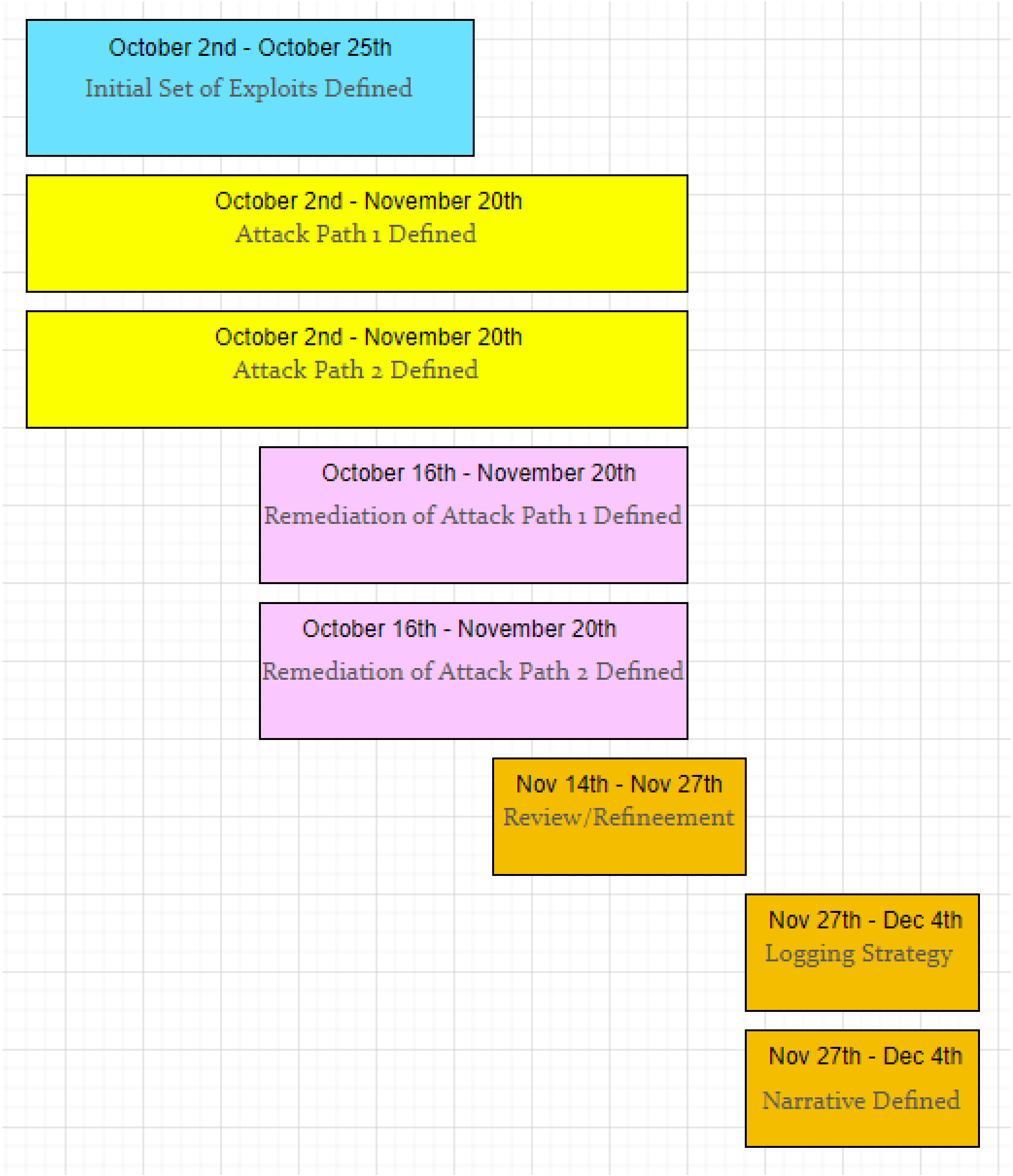
- Vulnerabilities per Component

- Misconfigurations per Component
- Infrastructure Vulnerabilities per Component
- Application Vulnerabilities per Component
- Estimated Monetary Resource Usage/hr
- Number of Resources Used
- Number of endpoints involved

(Qualitative) Evaluation Criteria:

- Setup complexity
    - How much of a burden does this place on the end user
- Professionalism/Realism
    - Used to for narrative items and related resources

3.4 Project Timeline/Schedule


October 2nd - October 25th
Initial Set of Exploits Defined
October 2nd - November 20th
Attack Path 1 Defined
October 2nd - November 20th
Attack Path 2 Defined
October 16th - November 20th
Remediation of Attack Path 1 Defined
October 16th - November 20th
Remediation of Attack Path 2 Defined
Nov 14th - Nov 27th
Review/Refineement
Nov 27th - Dec 4th
Logging Strategy
Nov 27th - Dec 4th
Narrative Defined

We have a total of 8 milestones. Some of the milestones have a similar timeline. In most of the milestones we have subtasks related to them. Below is a detailed breakdown of each milestone's subtasks.

Initial Set of Exploits Defined Issues: (3 Weeks):

- [Template] Exploit Defined by {Student Name}

- Complete flAWS Level 1-2

- Complete flAWS Level 3-4

- Complete flAWS Level 5-6

Attack Path 1 Defined and Attack Path 2 DesignedIssues (7 Weeks):

- Define a use case for each AWS service/resource - Attack Path 1/2
- Looting (Exfiltration) defined - Attack Path 1/2
- Lateral Movement Defined - Attack Path 1/2
- Persistence and Privilege Escalation Defined
- Attack Path 1/2 , Initial Exploitation Defined
- Attack Path 1/2 , Recon Defined - Attack Path 1/2.

Remediation of Attack Path 1 and Attack Path 2 Defined Issues (5 Weeks):

- Vulnerability/misconfiguration remediation defined - Attack Path 1/2
- Events and Actions defined - Attack Path 1/2

Review/Refinement Issues (2 Weeks):

- Cross Review - Attack Path 1
- Cross Review - Attack Path 2
- Refinement - Attack Path 1
- Refinement - Attack Path 2

Logging Strategy Defined Issues (1 Week):

- Research CloudWatch
- Research EventBridge
- Identify Logging Resources

Narrative Defined Issues (1 Week):

- Line of Business Defined - Attack Path 1
- Line of Business Defined - Attack Path 2
- Use Case for Services Defined for Narrative - Attack Path 1
- Use Case for Services Defined for Narrative - Attack Path 2
- User Roles Defined - Attack Path 1
- User Roles Defined - Attack Path 2

3.5 Risks And Risk Management/Mitigation

This section is intended to outline anticipated pitfalls or challenges we would face during the project, and to develop a plan to mitigate said risks should they arise. The risk level serves as an indicator of how likely each risk is to arise.

Tools not fitting in the scope of user security testing as defined in the AWS Shared Responsibility Model [Risk: 0.7]

- The AWS Shared Responsibility model broadly defines the use cases, and the Customer Service Policy for Penetration Testing more clearly defines the services that are permitted for customer Penetration Testing. These resources are broad in variety, so the primary concern here is scope creep into prohibited services to accompany allowed ones. This risk should be reduced through an understanding of these limitations by the team, and by reviewing these limitations during testing and review periods.

Resource cost is not reasonable for an individual to use [Risk: 0.5]

- This project will use a wide variety of resources, most of which have free tiers. Should the expected resource usage exceed these limitations, the availability of this project could be greatly reduced. We plan to reduce this risk by compartmentalizing parts of the project into distinct attack paths that will ensure that only the resources that are being used at the given time are being run. We can also help educate our users on how to cap resource usage if needed.

AWS lacks depth in opportunities for misconfiguration/vulnerabilities [Risk: 0.2]

- With over 200 services offered, and a large number of combinations of services working together it is unlikely that we will run out of misconfigurations. This would most likely be seen due to a lack of AWS specific items, but would be remediated by implementing more common vulnerabilities in an AWS environment.

3.6 Personnel Effort Requirements

Milestone	Est. Man Hrs
Initial Set of Exploits Defined	90
Remediation of Attack Path 2 Defined	80
Attack Path 2 Defined	112
Remediation of Attack Path 1 Defined	80
Attack Path 1 Defined	112
Review/Refinement	40
Logging Strategy Defined	20
Narrative Defined	20

Each task above in the list has multiple subtasks which vary in time needed to complete. This table provides a rough estimate of the expected number of hours each task will take to complete. The number of hours is not a per-person measurement, rather it is an estimated full team number of hours.

3.7 Other Resource Requirements

Identify the other resources aside from financial (such as parts and materials) required to complete the project.

- Since our implementation is designed & implemented on another company's hardware (amazon), we are reliant on their service availability. If AWS services were to go down or data became unrecoverable, the entire project resources would be effectively lost. These resource requirements and risks can be mitigated by taking backups, gathering detailed documentation, and the general reliability of AWS services.
- Due to the nature of making exploitable environments, certain vulnerabilities may be reliant upon outsourced methodology. In these cases, exploiting a certain vulnerability or utilizing an attack path is dependent on existing architecture as it relates to software environments.
- The project requires internet connection.
- Personal/RSM AWS account
- AWS Services
    - S3 Bucket
    - Lambda
    - API Gateway
    - dEC2
    - Eventbridge
    - CloudFormation Templates