**Sprint 3 Plan: Tool Deployment, Kubernetes Security Testing Understanding, and Test Case Collection**

Goal: Complete the development of the vulnerability scanning tool, deploy it within the Kubernetes cluster, deepen understanding of Kubernetes security testing, and assemble a diverse collection of test cases.

Objective 1: Tool Completion

- Focus on finalizing the vulnerability scanning tool during the initial four days.

- Refine the tool based on feedback and preliminary testing.

- Ensure the tool is capable of accurately detecting various vulnerabilities within Kubernetes clusters.

Objective 2: Deployment within Kubernetes Cluster

- Allocate the next two days to deploy the vulnerability scanning tool into the target Kubernetes cluster.

- Configure the tool to effectively interact with the cluster's resources.

- Verify that the tool functions as expected within the live environment.

Objective 3: Deeper Understanding of Kubernetes Security Testing

- Spend the first four days exploring advanced Kubernetes security testing concepts.

- Study runtime monitoring, container escape techniques, supply chain security vulnerabilities, and advanced exploitation scenarios.

Objective 4: Gathering Comprehensive Test Cases

- Dedicate the last two days to collecting an extensive set of test cases for Kubernetes security evaluation.

- Curate diverse scenarios encompassing misconfigurations, privilege escalations, network vulnerabilities, and other critical areas.

Through this sprint, the vulnerability scanning tool will be fully developed, deployed within the Kubernetes cluster, and extensively tested using a variety of curated test cases. Additionally, by deepening your understanding of advanced Kubernetes security testing techniques and assembling a comprehensive collection of test scenarios, and be well-equipped to assess and enhance the security posture of Kubernetes deployments. This sprint ensures a holistic approach to Kubernetes security and contributes to the robustness of your system.