# Kubernetes Security Scan - Task Overview

Title: Kubernetes Security Scan

Background/Task:

This task involves setting up a local Kubernetes cluster using tools such as Minikube, K3s, or Kind, and performing a security scan using tools like Kubescape or any equivalent. The goal is to identify configuration risks, policy violations, and other potential security issues in the cluster.

Steps to Perform:

1. Install a local Kubernetes cluster (Minikube, K3s, Kind, etc).
2. Deploy a security scanning tool such as Kubescape.
3. Run a full scan on the cluster.
4. Collect and export the scan findings as a JSON file.

Deliverables:

- A JSON file containing the list of Kubernetes security findings detected by the scanning tool.

Purpose:

This task helps ensure the Kubernetes environment is aligned with security best practices and provides a report that can be used for remediation planning.

Expected Outcome:

- Comprehensive visibility into security issues within the Kubernetes setup.
- Actionable insights based on industry standards (e.g., NSA-CISA, MITRE ATT&CK for K8s).