Kubernetes Security Scan Report

1. Introduction :

This report documents the process of scanning a local Kubernetes (K8s) cluster for security vulnerabilities using Kubescape. The generated results.json file contains the findings of the scan, including identified security risks and their severity levels.

2. Tools Used :

- Minikube – To create a local Kubernetes cluster.
- Kubescape – A Kubernetes security scanner to detect vulnerabilities.
- Command Prompt (cmd) – To execute commands and generate the report.

3. Steps Followed :

1. Set Up a Local Kubernetes Cluster.
2. Installed Kubescape for Security Scanning
3. Scanned the Kubernetes Cluster
4. Verified the Scan Results : json file

4. Findings

The detailed report includes a list of security issues, affected components, and recommendations.

5. Conclusion

The Kubernetes security scan successfully identified potential vulnerabilities in the cluster. The results.json file provides detailed insights into these issues, helping improve container security. Further steps could include remediation of critical vulnerabilities and integrating security checks into CI/CD pipelines.