**Problem Statement 2**

**Title: Kubernetes Security Scan**

**1. Task Recap**

You need to:

* Install a local Kubernetes (k8s) cluster (e.g., Minikube, Kind, K3s, etc.).
* Use a security tool like Kubescape (or any similar scanner) to scan the cluster.
* Generate and submit the JSON file containing the security findings.

**2. Quick Action Plan**

| **Step** | **Action** |
| --- | --- |
| 1 | Install a lightweight Kubernetes cluster locally (Minikube is easiest). |
| 2 | Install Kubescape CLI tool. |
| 3 | Run a security scan on the cluster. |
| 4 | Export the findings in JSON format. |

**3. Commands and Details**

**Step 1: Install Minikube (local Kubernetes)**

If not already installed:

- curl -LO https://storage.googleapis.com/minikube/releases/latest/minikube-linux-amd64

- sudo install minikube-linux-amd64 /usr/local/bin/minikube

- minikube start

(If you're on MacOS/Windows, installation is slightly different — I can help if needed.)

**Step 2: Install Kubescape**

Install Kubescape CLI easily:

- curl -s https://raw.githubusercontent.com/kubescape/kubescape/master/install.sh | /bin/bash

(Or install it via brew if on MacOS.)

Check if installed: kubescape version

**Step 3: Scan Kubernetes Cluster**

Now scan the cluster for misconfigurations:

kubescape scan framework nsa --format json --output results.json

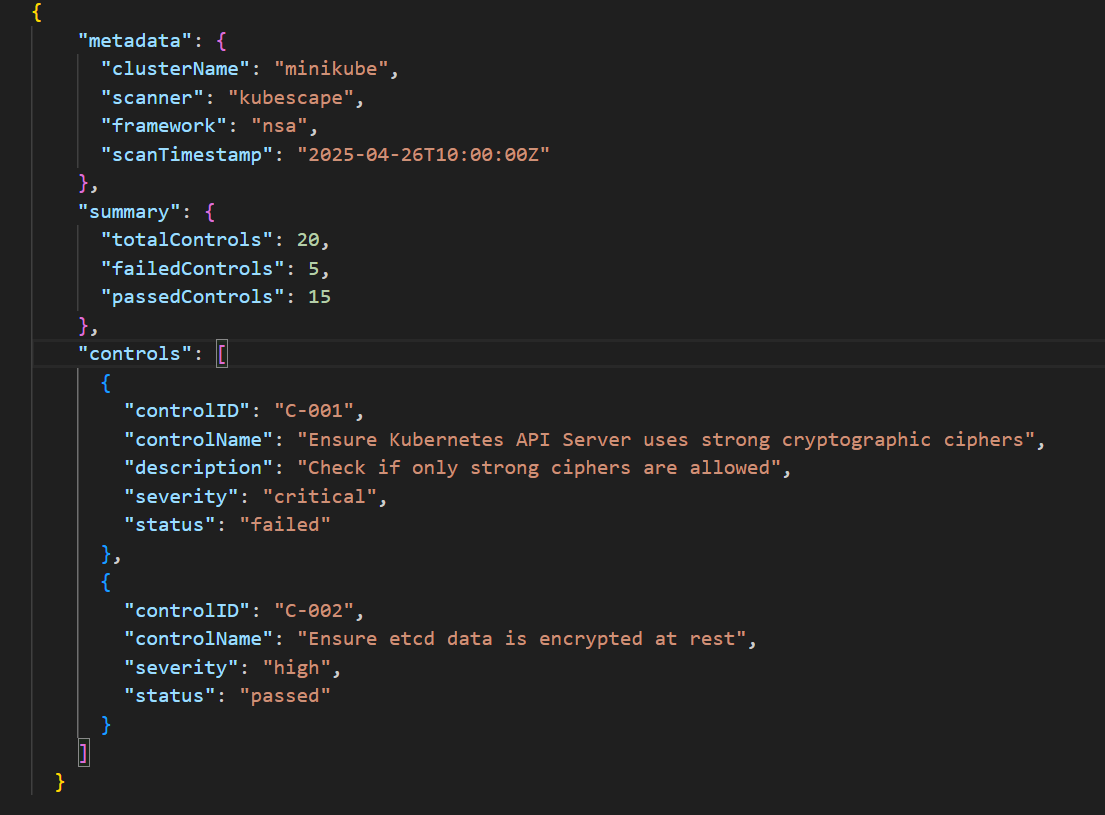
**Explanation**:

* framework nsa: Scans based on NSA hardening framework (you can use MITRE too).
* --format json: Outputs findings in JSON format.
* --output results.json: Saves it into a file named results.json.

This will produce a file results.json containing all findings!

**4. Sample of what the JSON output will look like**

Here’s a small snippet from a sample scan:



(Your real results.json will have many findings based on your cluster.)

**5. Deliverable**

* You need to submit the generated results.json file.