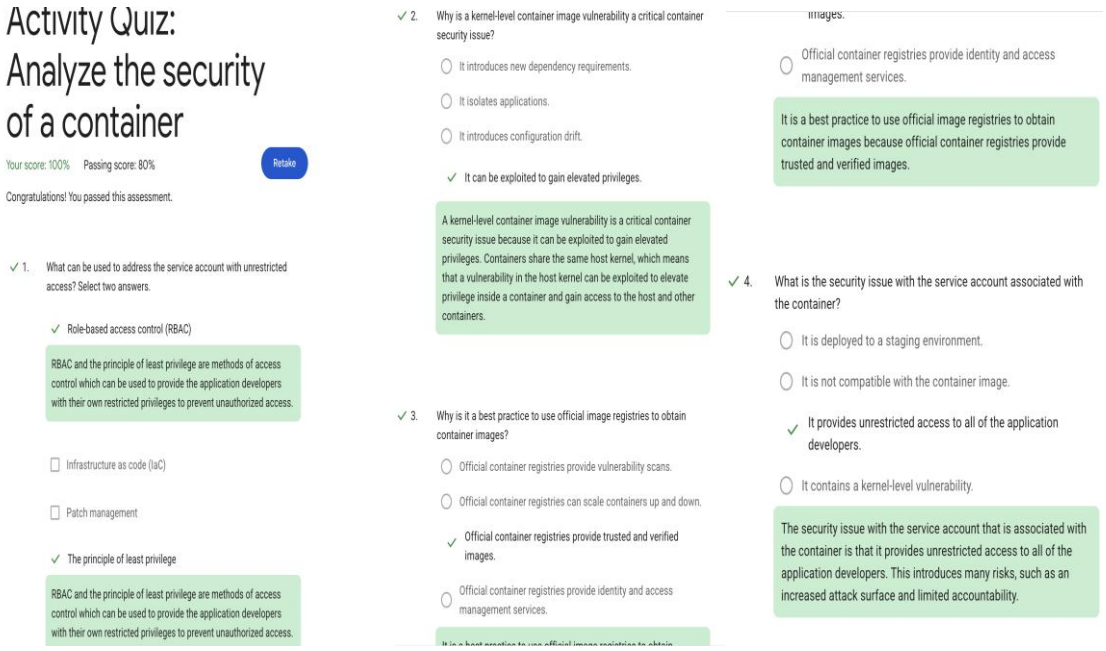
# Container security checklist (Bri's Answers)

Container security best practice: Scan the container image for vulnerabilities
**Explanation**: Scanning the image for vulnerabilities before implementation is a step that will keep the environment secure. Using images that have been flagged with vulnerabilities could mean that the organization's system is now susceptible to various attacks.

Container security best practice: Implement access based controls on the Kubernetes service account. Individuals should not have unrestricted access.
**Explanation**: Determining who or what has access to organizational resources are important. You wouldn't want someone from marketing having access or the ability to change technical infrastructure as an example. Setting up role-based access allows security professionals to know who has been granted not only access but permissions to resources and data.

Container security best practice: Verify that the image is from a trusted source
**Explanation**: In the configuration image provided by Google it indicates the image is from the internet. Because the internet is vast and the majority of people have access, it is important to know and verify that an image is from a trusted source rather than a threat actor implementing a social engineering tactic to gain access to a system.

## Activity Quiz Answers (First Attempt Score): Analyze the security of a Container:




**My Assessment:** Based on the Google answers in comparison to my answers listed above, I did not include which security measures were implemented (checkboxes) and I did not include Patch any vulnerabilities apart of the checklist. Patching vulnerabilities, especially when the security team is aware they exist, is a necessary step in securing the system, and in this scenario, the container. Containers are vital in the cloud as it contains the application and its dependencies, they also communicate with other containers and if one container has been corrupted there is a chance it can corrupt other containers, especially if it shares resources.

**Google Answer:**

## Container security checklist

Ensure that the container image is pulled from a trusted and verified source.
**Explanation**: Containers use container images. The developers obtained a container image from an official image registry service.
Scan the container image.
**Explanation**: Vulnerabilities can exist in container images. Images should be regularly scanned and updated to identify vulnerabilities. The developers performed a vulnerability scan on the container image.
Patch any vulnerabilities.
**Explanation**: The vulnerability scan reported a kernel-level vulnerability. It should be immediately patched.
Implement role-based access control (RBAC) and the principle of least privilege.
**Explanation**: All of the developers are using a single Kubernetes service account with unrestricted access. The developers must consider creating roles for users with restricted privileges in order to prevent unauthorized access.

**Google Instructions & Container Configuration Details:**

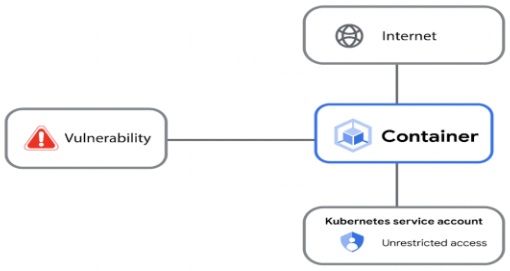
Step 1: Access the supporting materials.
Step 2: Analyze the container configuration.
Step 3: Provide suggestions for container security.
Step 4: Access the quiz and answer questions about container security.

What to Include in Your Response
Be sure to address the following criteria in your completed activity:
● 3–4 checklist items with 1–2 sentences describing a container security best practice
● 1–2 sentences providing an explanation for each security best practice
● A check next to each security best practice that has been implemented

**Container configuration details**

The diagram provides an overview of the container configuration details. To summarize:

- The application developers used an official image registry service to obtain the container image.
- A vulnerability scan for the container reports a kernel-level vulnerability.
- There is one Kubernetes service account with unrestricted access that all application developers have been using.




[ALT Text: A flowchart diagram shows the details of a container configuration that includes a kernel-level vulnerability and a Kubernetes service account with admin level privilege]