**KubeBench Nedir?**

KubeBench, Kubernetes kümelerinin güvenlik uyumluluğunu test etmek için kullanılan açık kaynaklı bir araçtır. Özellikle CIS (Center for Internet Security) Kubernetes Benchmark’lerine göre sistemin güvenlik standartlarına uyup uymadığını kontrol eder.

**KubeBench Özellikleri**

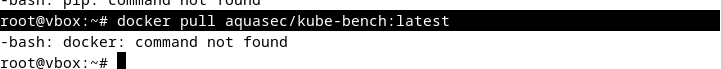
* **CIS Benchmark Uyumluluğu:** Kubernetes bileşenlerinin CIS Benchmark kurallarına göre değerlendirilmesini sağlar.
* **Otomatik Güvenlik Tarama:** Kubernetes yapılandırmalarını otomatik olarak tarar.
* **JSON ve HTML Raporlama:** Sonuçları JSON ve HTML formatlarında raporlar, kolay analiz imkanı sunar.
* **Platform Bağımsız:** Linux ve Windows ortamlarında çalışabilir.
* **Açık Kaynak:** GitHub üzerinden ücretsiz erişilebilir ve geliştirilebilir.

**KubeBench Kurulum Aşamaları**

**1. Gereksinimler**

* Kubernetes kümeniz çalışıyor olmalı.
* Linux (veya Windows) işletim sistemi.
* Docker veya başka container runtime (isteğe bağlı).

**2. Kurulum Yöntemleri**

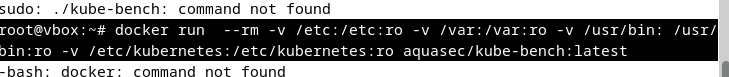
**a) Docker ile Kurulum: **

**b) Binary İndirerek Kurulum : **

**c) Kubernetes Üzerinde Pod olarak Çalıştırmak: **

**KubeBench Kullanımı:**

**-**Komut satırından doğrudan çalıştırarak kümenin kontrolünü yapabilirsiniz: 

-Docker kullanıyorsanız: 

-Kubernetes job ile kullanıyorsanız pod loglarını takip edin.

**Dikkat Edilmesi Gereken Noktalar**

* KubeBench'i çalıştırmak için genellikle root veya sudo yetkisi gerekir.
* CIS Benchmark sürümü, KubeBench sürümü ile uyumlu olmalıdır.
* Kubernetes versiyonuna göre farklı benchmark profilleri kullanılır (örn: 1.21, 1.22 vs).
* KubeBench sadece önerilen güvenlik ayarlarını kontrol eder, tüm güvenlik açığı tespitlerini yapmaz.
* Çalıştırma ortamında gerekli izinlerin ve dosya erişimlerinin olması gerekir.
* Test edilen küme canlıysa, çalıştırırken dikkatli olun; KubeBench sadece okuma işlemi yapar ama yine de izinler önemlidir.

**KubeBench Kullanım Alanları**

* Kubernetes kümelerinin güvenlik değerlendirmesi.
* Otomatik güvenlik raporlaması.
* DevOps pipeline’larında güvenlik testi aşaması olarak entegrasyon.
* Güvenlik uyumluluğunu sağlamak isteyen kurum ve şirketlerde risk azaltma aracı.
* Eğitim ve denetim amaçlı kullanım.