**kube-hunter**, Kubernetes ortamlarında güvenlik açığı taraması yapmak için kullanılan açık kaynaklı bir araçtır. Aqua Security tarafından geliştirilmiştir. Kube-hunter, hem **pasif** hem de **aktif tarama** yaparak Kubernetes cluster’larında **yanlış yapılandırma**, **açık portlar**, **yetkisiz erişim**, **servis bilgi sızıntısı** gibi zafiyetleri tespit eder.

**Bu Aracın Özellikleri Nelerdir?**

* **Remote ve local (cluster içi) tarama modu**
* **Kubelet API, Dashboard, Etcd gibi servislerin test edilmesi**
* **JSON ve taban metin formatında çıktı**
* **CVE’lere dayalı açıklamalar**
* **Yanlış yapılandırma algılama (misconfiguration)**
* **Pod içinden avlanma (in-cluster hunting)**

**Kube-hunter Aracını Kali Linux’ta Kurma ve Kullanma Adımları**

**Adım 1: kube-hunter Kurulumu (pip ile)**

“sudo apt update

sudo apt install python3-pip -y

pip3 install kube-hunter”

Alternatif olarak GitHub’dan klonlayarak da kurulabilir:

“git clone https://github.com/aquasecurity/kube-hunter.git

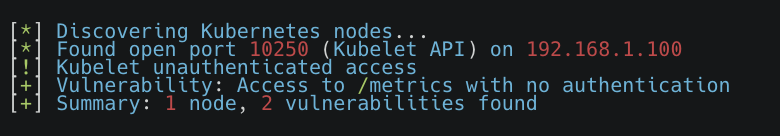
cd kube-hunter

pip3 install -r requirements.txt”

**Adım 2: Uzak Bir Kubernetes Hedefini Taramak (Passive Mode)**

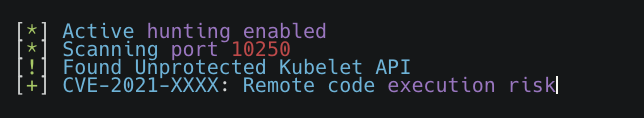
Örnek hedef IP: 192.168.1.100

**“kube-hunter --remote 192.168.1.100”**



**Adım 3: Aktif Tarama Modunu Başlat**

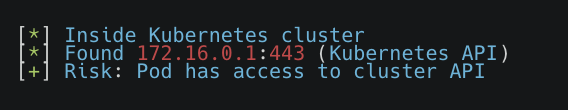
“kube-hunter --remote 192.168.1.100 –active”



**Adım 4: Pod İçinden (In-Cluster) Tarama**

Eğer bu komut bir pod içinde çalıştırılırsa otomatik olarak iç cluster’ı tarar:

**“kube-hunter”**



**Adım 5: JSON Formatında Rapor Almak**

“kube-hunter --remote 192.168.1.100 --report json > report.json”

“cat report.json”

