**Instaruction**

Kube-Hunter can deploy in a local machine or server (ex. Google Cloud Platform) or containerized version on aquatic/Kube-Hunter. Kube Hunter can deploy locally on windows, mac, linux or cloud such as Google Cloud Platform and AWS. The following step is required for deploying Kube-Hunter on GKE (Google Kubernetes Engin) are:

* Python 3.7.1 installation
* Kube-Hunter pip installation: pip3 install Kube-Hunter

* Clone the repository: https://github.com/aquasecurity/Kube-Hunter.git
* Dependency Installation: docker run -it --rm --network host

aquasec/kube-hunter

**Installl**

pip install kube-hunter

#### **Scanning**

In this stage, Scanning is a critical part of finding the vulnerability or misconfiguration on our Kubernetes cluster infrastructure.

* Remote Scanning
* Interface Scanning
* Network Scanning

#### **Testing**

Testing our infrastructure from external and internal attacks is crucial for many enterprises to keep their data safe from any breaches and attacks. Kube-Hunter offers the two different testing such as Active Hunting and Passive Hunting to ensure the infrastructure is in healthy state. Most of the penetration testing is performed on the kubernetes interface.

##### **Active Hunting**

The active state enables additional testing for retrieve log and executing nameinside the random containers, finding versions, and building date when the proxy is exposed. It can set the operational parameter to enable additional testing. In this stage, scanning exploits the vulnerability it finds in Kubernetes clusters, and it could change the cluster, which is harmful.

The table below Table 2.1 is an example of an active Hunting Scan to find Critical vulnerabilities on the Kubernetes cluster.

|  |  |
| --- | --- |
| Arp Spoof Hunter | Scan for the ARP spoof attack within a pod. |
| DNS Spoof scan | Scanning malicious pods that compromised DNS requests. |
| Kubelet Run scan | Check the uname inside the containers. |
| Kubelet Container Logs | Scanning logs from various containers |
| Build Date Scan | Checks build date when the cluster is exposed. |
| API server Scan | Scan any attack on the API server. |

***Active Hunting Scanning***

##### **Passive Hunting**

The passive hunting can perform on the Kubernetes cluster interface to find any open ports within the cluster, which can cause attackers to gain access to the operating system and the possibility of data breaches. In addition, Passive Hunt checks Kubernetes SSL certificates and open dashboards behind proxies to mitigate any attack explosion

The table below Table 2.2 is an example of a passive Hunting Scan to find Critical vulnerabilities on the Kubernetes cluster.

|  |  |
| --- | --- |
| Port Scan | Scans and discovery knew ports and open endpoints. |
| K8s Dashboard Discovery | Known Dashboard will check. |
| API Service Discovery | Known K8s API will check. |
| Proxy Discovery | Open Proxy service will check. |
| Access Secrets scan | Accessing the secrets accessible to the pod. |
| API Version scan | Obtain the API Server's version from the endpoint. |
| Certificate Email scan | Kubernetes SSL certificates check for the email addresses. |

***Passive Hunting Scanning Vulnerability***