**Detecció de vulnerabilitats amb kube-hunter**

**Objectiu**

*Analitzar l’estat de seguretat del clúster Kubernetes creat a la pràctica 1, simulant un reconeixement intern com el que podria fer un atacant que ha compromès un pod dins del clúster.*

*Utilitzarem l’eina kube-hunter per detectar* ***vulnerabilitats reals*** *en el desplegament actual (amb el servei web-nginx actiu) i entendre els riscos de configuracions per defecte.*

*kube-hunter és una eina de seguretat ofensiva per a Kubernetes desenvolupada per Aqua Security.*

*Està dissenyada per ajudar administradors i professionals de ciberseguretat a detectar vulnerabilitats i configuracions insegures en un clúster Kubernetes.*

*kube-hunter actua com ho faria un atacant real: explora i escaneja els serveis i components interns de Kubernetes, cercant possibles punts febles o mal configuracions que podrien ser explotades.*

*kube-hunter es pot executar en dos modes principals:*

* *Remote mode:
Escaneja des de fora del clúster, com si fos un atacant extern.
Especificant una IP o domini del clúster, analitza serveis accessibles públicament.*
* *Internal (pod) mode:
Es llança dins del clúster (com un pod) per simular el que podria fer un atacant que ja ha compromès un contenidor.
Aquest és el mode que farem servir a la pràctica, ja que proporciona una visió realista de les debilitats internes.*

*Alguns exemples de vulnerabilitats que kube-hunter pot identificar:*

* *Ports i serveis exposats sense autenticació.*
* *Accés al servidor d’API sense restriccions.*
* *Secrets accessibles sense protecció.*
* *Dashboards oberts al públic o sense control d’accés.*
* *Falta de polítiques de xarxa entre pods.*

*kube-hunter és útil per:*

* *Conèixer l’estat real de la seguretat d’un clúster.*
* *Detectar errors de configuració abans que ho faci un atacant.*
* *Simular escenaris de pentesting dins d’un entorn controlat.*

**Escenari**

Simularem que un atacant ha obtingut accés a un contenidor dins del clúster. Des d’allà, executarem kube-hunter per veure quines vulnerabilitats o serveis exposats pot detectar.

Comproveu que encara estan funcionant els serveis de la pràctica anterior amb:

kubectl get services

**Fase 1: Crear un pod per executar kube-hunter**

kubectl run kube-hunter --image=aquasec/kube-hunter --restart=Never -- --pod

Aquest pod arrencarà, executarà l’escaneig i es pararà automàticament.

Si en algun moment d’hem d’eliminar, podem fer:

kubectl delete pod kube-hunter

**Fase 2: Anàlisi dels resultats**

Un cop el pod hagi finalitzat (estat Completed), consulta els resultats amb:

kubectl logs kube-hunter

L’eina mostrarà les vulnerabilitats detectades dins del clúster.

****

**Fase 3: Reflexió i documentació**

1. Anota dues vulnerabilitats detectades i completa per cada una:
	* Quin component afecta?
	* Quin risc suposa?
	* Com es podria mitigar?

**Fase 4: Neteja del pod de kube-hunter**

kubectl delete pod kube-hunter

**Extensió opcional**

* Comparar els resultats de kube-hunter abans i després d’aplicar mesures de seguretat (ex: RBAC o polítiques de xarxa).
* Instal·lar kube-hunter en mode remote per simular un atac des de fora del clúster.