DevSecOps Tools

Recopilación de herramientas complementarias para auditoría de Docker, K8, AWS, etc.

Estas herramientas me han sido útiles en pentesting (tanto caja negra como blanca) y en la revisión de la seguridad de diferentes entornos y diferentes tecnologías.

Índice

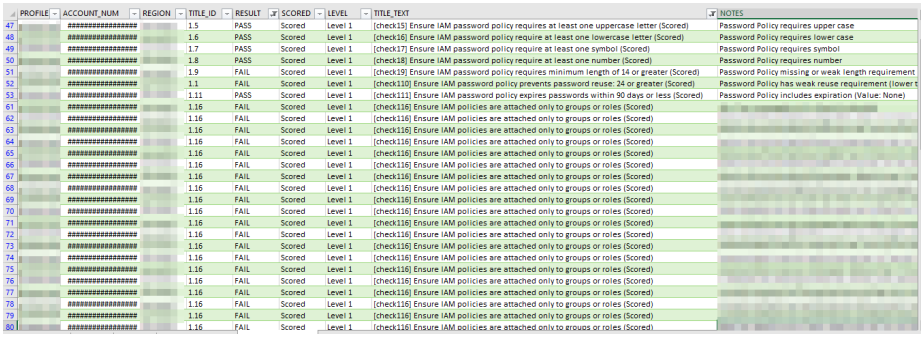
Cumplimiento CIS

AWS CIS

Prowler

Es una herramienta en python que permite realizar un análisis del grado de cumplimiento con el bastionado CIS de el entorno en AWS además de diferentes grupos de checks predefinidos relacionados con el control IAM, monitorización, logging, forense entre otros.

Permite exportar los resultados en múltiples formatos (CSV, JSON, TXT, etc.)



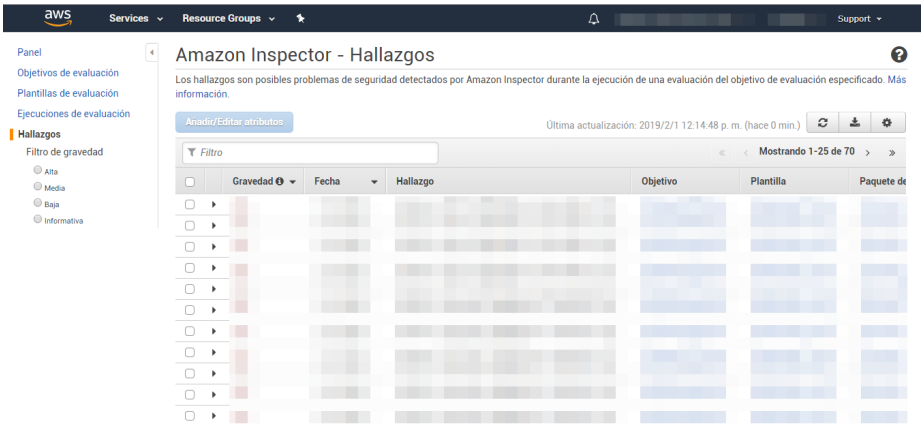
	PROFILE	ACCOUNT_NUM	REGION	TITLE_ID	RESULT	SCORED	LEVEL	TITLE_TEXT	NOTES
47		################		1.5	PASS	Scored	Level 1	[check15] Ensure IAM password policy requires at least one uppercase letter (Scored)	Password Policy requires upper case
48		################		1.6	PASS	Scored	Level 1	[check16] Ensure IAM password policy require at least one lowercase letter (Scored)	Password Policy requires lower case
49		################		1.7	PASS	Scored	Level 1	[check17] Ensure IAM password policy require at least one symbol (Scored)	Password Policy requires symbol
50		################		1.8	PASS	Scored	Level 1	[check18] Ensure IAM password policy require at least one number (Scored)	Password Policy requires number
51		################		1.9	FAIL	Scored	Level 1	[check19] Ensure IAM password policy requires minimum length of 14 or greater (Scored)	Password Policy missing or weak length requirement
52		################		1.1	FAIL	Scored	Level 1	[check110] Ensure IAM password policy prevents password reuse: 24 or greater (Scored)	Password Policy has weak reuse requirement (lower t
53		################		1.11	PASS	Scored	Level 1	[check111] Ensure IAM password policy expires passwords within 90 days or less (Scored)	Password Policy includes expiration (Value: None)
61		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
62		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
63		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
64		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
65		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
66		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
67		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
68		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
69		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
70		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
71		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
72		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
73		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
74		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
75		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
76		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
77		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
78		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
79		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	
80		################		1.16	FAIL	Scored	Level 1	[check116] Ensure IAM policies are attached only to groups or roles (Scored)	

AWS Inspector

Herramienta que permite realizar análisis de vulnerabilidades, cumplimiento CIS, nivel de exposición desde internet, etc. en las instancias virtuales de AWS. Trae implementado por defecto cinco tipos de escaneos: Runtime Behavior Analysis, Security Best Practices, Network Reachability, CIS Operating System Security Configuration Benchmarks (no están soportados todos los S.O.) y Common Vulnerabilities and Exposures aunque también se pueden crear plantillas de análisis personalizadas.

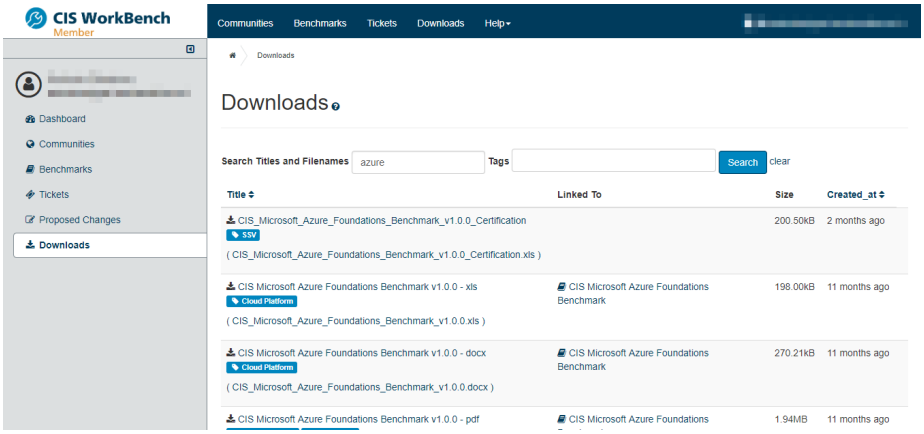
Para ejecutarlo hay que instalar el agente de Inspector en las máquinas virtuales y usando la propia interfaz web de la herramienta definir un "Objetivo de Evaluación" indicando el conjunto de instancias virtuales sobre las que realizar el análisis, definir la "Plantilla de Evaluación" para indicar el/los tipo/s de análisis a correr y una "Ejecución" en donde se puede lanzar manualmente o programar una tarea periódica para que se realice automáticamente.

En la sección "Hallazgos" están los resultados de los análisis ejecutados.

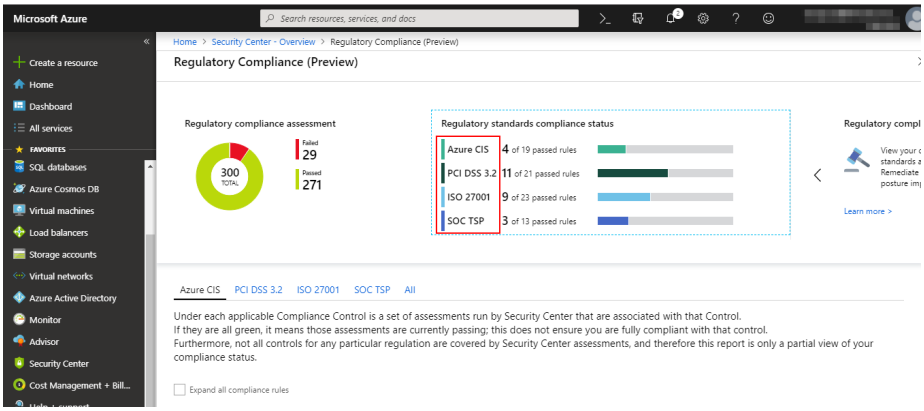


Azure CIS

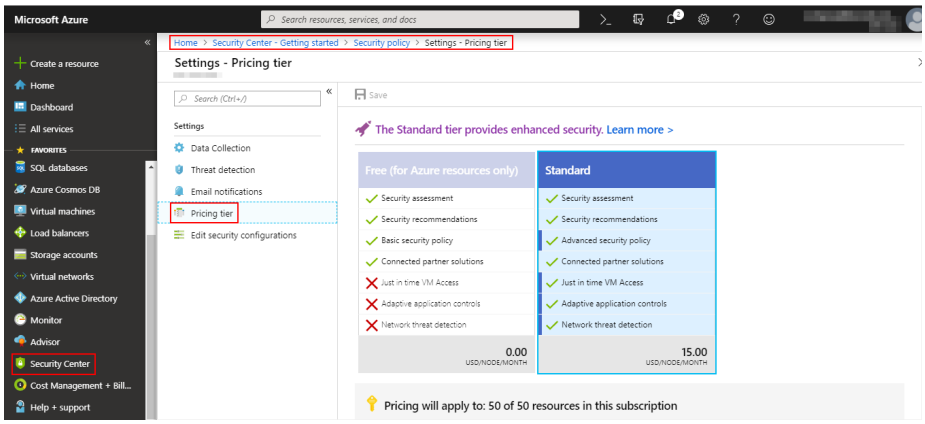
Aunque el benchmark CIS de Azure está definido y es posible encontrar y descargasr los benchmarks en diferentes formatos no he localizado ninguna herramienta que lo tenga incorporado, ni siquiera está en Nessus.



Es posible obtener este grado de cumplimiento a través de la herramienta "Security Center" integrada en la propia suscripción de Azure la cual además muestra el estado referente al cumplimiento PCI DSS, ISO 27001 y SOC TSP.



Para obtenerlo, no basta solo con activar el Security Center e instalar los agentes de monitorización en todos los nodos sino que hay que hacer uso de la versión "Standard" (de pago). Lo bueno que Microsoft deja un mes de prueba gratis para esta versión completa de Security Center y una vez lo tengamos es posible volverlo a desactivar.



Docker CIS

Docker Bench for Security

Este script comprueba automáticamente las buenas prácticas en el despligue de Dockers inspirado en el CIS Docker Community Edition Benchmark v1.1.0.

La manera más sencilla de correr esta herramienta es haciendo uso del contenedor ya definido por ellos el cual se puede correr en el host que queramos comprobar. Antes de ello hay que ajustar los volúmenes a compartir con el Docker para ajustarlos según el S.O. que se vaya a auditar.

```
docker run -it --net host --pid host --userns host --cap-add audit_control \
    -e DOCKER_CONTENT_TRUST=$DOCKER_CONTENT_TRUST \
    -v /var/lib:/var/lib \
    -v /var/run/docker.sock:/var/run/docker.sock \
    -v /usr/lib/systemd:/usr/lib/systemd \
    -v /etc:/etc --label docker_bench_security \
    docker/docker-bench-security
```

```
[                                    ]# docker run -it --net host --pid host --userns host --cap-add audit_control \
>     -e DOCKER_CONTENT_TRUST=$DOCKER_CONTENT_TRUST \
>     -v /var/lib:/var/lib \
>     -v /var/run/docker.sock:/var/run/docker.sock \
>     -v /usr/lib/systemd:/usr/lib/systemd \
>     -v /etc:/etc --label docker_bench_security \
>     docker/docker-bench-security
Unable to find image 'docker/docker-bench-security:latest' locally
latest: Pulling from docker/docker-bench-security
4fe2ade4980c: Already exists
fd43e174d869: Pull complete
7fb014ef1929: Pull complete
3faf9fde7d31: Pull complete
Digest: sha256:071b858f4b40e34fa58b21ed1d746a917ce7adc0530571bc408b61512bfe2dda
Status: Downloaded newer image for docker/docker-bench-security:latest
# ------------------------------------------------------------------------------
# Docker Bench for Security v1.3.4
#
# Docker, Inc. (c) 2015-
#
# Checks for dozens of common best-practices around deploying Docker containers in production.
# Inspired by the CIS Docker Community Edition Benchmark v1.1.0.
# ------------------------------------------------------------------------------

Initializing Mon Jan 14 12:08:27 UTC 2019

[INFO] 1 - Host Configuration
[WARN] 1.1  - Ensure a separate partition for containers has been created
[NOTE] 1.2  - Ensure the container host has been Hardened
[INFO] 1.3  - Ensure Docker is up to date
[INFO]      * Using 18.03.1, verify is it up to date as deemed necessary
[INFO]      * Your operating system vendor may provide support and security maintenance for Docker
[INFO] 1.4  - Ensure only trusted users are allowed to control Docker daemon
[INFO]      * docker:x:991
[WARN] 1.5  - Ensure auditing is configured for the Docker daemon
[WARN] 1.6  - Ensure auditing is configured for Docker files and directories - /var/lib/docker
[WARN] 1.7  - Ensure auditing is configured for Docker files and directories - /etc/docker
```

Kubernetes CIS

Kube Bench

Para determinar el grado de cumplimiento CIS para Kubernetes se puede utilizar la herramienta kube-bench desarrollada en Go la cual realiza una comprobación de los checks definidos en CIS Kubernetes Benchmark aunque también permite añadir test personalizados a través de ficheros de configuración YAML.

Esta herramienta soporta test para múltiples versiones de Kubernetes (1.6, 1.7, 1.8, and 1.11) definidas en las guías CIS 1.0.0, 1.1.0, 1.2.0, y 1.3.0 respectivamente.

La forma más sencilla de ejecutar esta herramienta es ejecutarlo desde un contenedor y lanzar las pruebas sobre el clúster de K8.

```
docker run --pid=host -v /etc:/etc:ro -v /var:/var:ro -t aquasec/kube-bench:latest <master|n
```

Es posible también lanzarlo sobre un clúster de Kubernetes o sobre un POD en concreto indicándolo a través de los archivos YAML job-master y job-node proporcionados.

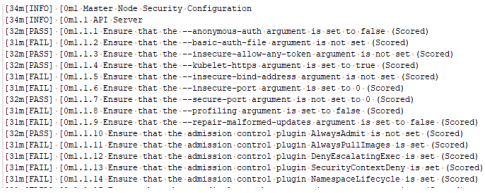
```
$ kubectl apply -f job-master.yaml
job.batch/kube-bench-master created

$ kubectl get pods
NAME                      READY   STATUS              RESTARTS   AGE
```

```
kube-bench-master-j76s9   0/1     ContainerCreating   0          3s

# Wait for a few seconds for the job to complete
$ kubectl get pods
NAME                      READY   STATUS      RESTARTS   AGE
kube-bench-master-j76s9   0/1     Completed   0          11s

# The results are held in the pod's logs
k logs kube-bench-master-j76s9
[INFO] 1 Master Node Security Configuration
[INFO] 1.1 API Server
...
```



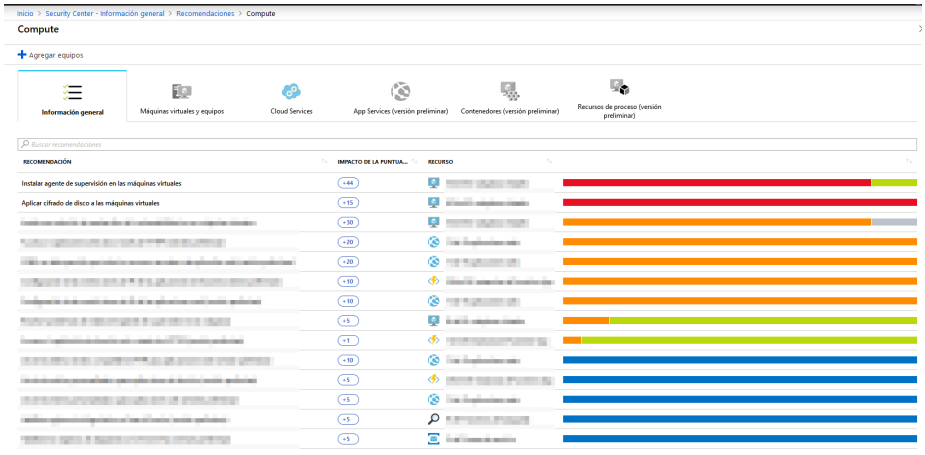
Vulnerabilidades

AWS Vulnerabilidades

En este caso, se puede utilizar directamente uno de los tipos de escáneres definidios en AWS Inspector específico para ello.

Azure Vulnerabilidades

Para el análisis de las vulnerabilidades de los diferentes componentes desplegados en Azure es posible obtenerlas a través del Security Center Azure CIS.



Docker Vulnerabilidades

Aquasec Microscanner Wrapper

Esta herramienta permite analizar las imágenes creadas o utilizadas en Docker para obtener un listado de vulnerabilidades conocidas que hay en los componentes que integran.

Tras registrar un token hay que pasárselo a la herramienta en una variable de entorno y directamente lanzarla contra la imagen que queremos analizar. Permite obtener la salida en formato JSON o HTML.

```
$ MICROSCANNER_TOKEN=xxxxxxxxxxxxxxxx ./scan.sh aquasec/microscanner
```


```
··"scan_started":·{
····"seconds":·1547462687,
····"nanos":·313446686
··},
··"scan_duration":·18,
··"digest":·"0eaa01823ba992b1bea1cd908db5140887ddc7e9384ba361ac9d29e98e2a8f9d",
··"os":·"alpine",
··"version":·"3.7.1",
··"resources":·[
····{
·····"resource":·{
·······"format":·"apk",
·······"name":·"nodejs",
·······"version":·"8.9.3-r1",
·······"arch":·"x86_64",
·······"cpe":·"pkg:/alpine:3.7.1:nodejs:8.9.3-r1",
·······"license":·"MIT",
·······"name_hash":·"671a0da0ba061c98de801409dbc57d7e"
·····},
·····"scanned":·true,
·····"vulnerabilities":·[
·······{
·········"name":·"CVE-2018-12115",
·········"description":·"In·all·versions·of·Node.js·prior·to·6.14.4,·8.11.4·and·10.9.0·when·used·with·UCS-2·encoding·(recognized·by·Node.js·under·the·names·''ucs2'',·''ucs-2'',·''utf16le''·and·''
·········"nvd_score":·5,
·········"nvd_score_version":·"CVSS·v2",
·········"nvd_vectors":·"AV:N/AC:L/Au:N/C:N/I:N/A:P",
·········"nvd_severity":·"medium",
·········"nvd_url":·"https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12115",
·········"vendor_score":·5,
·········"vendor_score_version":·"CVSS·v2",
·········"vendor_vectors":·"AV:N/AC:L/Au:N/C:N/I:N/A:P",
·········"vendor_severity":·"medium",
·········"publish_date":·"2018-08-21",
·········"modification_date":·"2018-11-02",
·········"nvd_score_v3":·7.5,
·········"nvd_vectors_v3":·"CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
·········"nvd_severity_v3":·"high"
·······},
·······{
·········"name":·"CVE-2018-7159",
·········"description":·"The·HTTP·parser·in·all·current·versions·of·Node.js·ignores·spaces·in·the·`Content-Length`·header,·allowing·input·such·as·`Content-Length:·1·2`·to·be·interpreted·as·havin(
·········"nvd_score":·5,
·········"nvd_score_version":·"CVSS·v2",
·········"nvd_vectors":·"AV:N/AC:L/Au:N/C:N/I:P/A:N",
```


DockScan

Esta herramienta está desarrollada en Ruby.

```
gem install dockscan
```

A continuación se muestran algunos ejemplos típicos de uso de la herramienta.

Para realizar un escaneo local de la instalación de Docker

```
dockscan unix:///var/run/docker.sock
```

Para realizar un escaneo remoto y guardar la salida en formato HTML

```
dockscan -r html -o myreport -v tcp://example.com:5422
```

Para realizar un escaneo remoto y guardar la salida en formato TXT

```
dockscan -r txt -o myreport -v tcp://example.com:5422
```

```
################################################################################

[ ]# dockscan -r txt -o dockscan unix:///var/run/docker.sock
[ ]# more dockscan.txt
Dockscan Report

-[ High ]-
=Container have passwordless users in shadow=
Description:
Container have vulnerable entries in /etc/shadow.
It allows attacker to login or switch to user without password.
Output:
0b3d575910662394003cd08ca9b7c5798cd1ef7ffla448fa44e809c7266d06aa ( ) with IP: does not have password
set for user: root
5ac6ae19b86abea3f68a9975e4596b2d7ad2d62d5df38760d04d6felac3d819a ( ) with IP: does not have password set for user:
root

Solution:
It is recommended to set password for user or to lock user account.
```

Docker Scan

Esta herramienta en python permite escanear una red para tratar de localizar Docker Registries para tratar de obtener información, borrar imágenes o subir las nuestras propias y además permite analizar imágenes para buscar información sensible o tratar de modificarlas para inyectar por ejemplo una shell reversa en ellas.

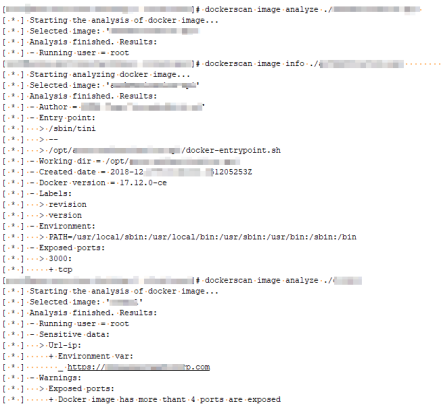
```
[ ]# dockerscan image analyze ./
[*] Starting the analysis of docker image...
[*] Selected image: *
[*] Analysis finished. Results:
[*] -- Running user = root
[ ]# dockerscan image info ./
[*] Starting analyzing docker image...
[*] Selected image: *
[*] Analysis finished. Results:
[*] -- Author =
[*] -- Entry point:
[*] ---> /sbin/tini
[*] ---> --
[*] ---> /opt/ /docker-entrypoint.sh
[*] -- Working dir = /opt/
[*] -- Created date = 2018-12 1205253Z
[*] -- Docker version = 17.12.0-ce
[*] -- Labels:
[*] ---> revision
[*] ---> version
[*] -- Environment:
[*] ---> PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
[*] -- Exposed ports:
[*] ---> 3000:
[*] ----> tcp
[ ]# dockerscan image analyze ./
[*] Starting the analysis of docker image...
[*] Selected image: *
[*] Analysis finished. Results:
[*] -- Running user = root
[*] -- Sensitive data:
[*] ---> Url-ip:
[*] ----> Environment var:
[*] ------> https://
[*] -- Warnings:
[*] ---> Exposed ports:
[*] ----> Docker image has more thant 4 ports are exposed
```

Kubernetes Vulnerabilidades

Kube Hunter

Esta herramienta permite realizar un análisis de vulnerabilidades y debilidades en una instalación de Kubernetes. Permite escaneo remoto, interno o por CIDR sobre un clúster de K8. Además incorpora una opción “Activa” a través de la cual trata de explotar los hallazgos.

Se puede correr en local o a través del despliegue de un contener que ya viene preparado con todo.



Un ejemplo de lo que es posible obtener y hasta donde comprometer una infraestructura se puede ver en el siguiente artículo del blog UN INFORMÁTICO EN EL LADO DEL MAL.

Hacking Kubernetes: Auditoría de seguridad y Explotación de vulnerabilidades