Práctica 3. Análisis forense en la nube.

Docker: Introducción y forense de contenedores

Docker es una plataforma de software que permite a los desarrolladores crear, probar y desplegar aplicaciones de forma rápida y sencilla en contenedores. Es una tecnología que ha ganado mucha popularidad en los últimos años, especialmente en el mundo de la tecnología de la información.

Docker se utiliza para encapsular aplicaciones en contenedores, lo que significa que cada aplicación se ejecuta en su propio entorno aislado. Esto significa que los desarrolladores pueden garantizar que sus aplicaciones funcionen de la misma manera en cualquier entorno, independientemente de las diferencias entre el hardware y el software.

La principal ventaja de usar Docker es que se pueden crear entornos de desarrollo y producción idénticos, lo que ayuda a garantizar la calidad y la coherencia de las aplicaciones. Además, Docker permite la integración continua y el despliegue continuo, lo que permite a los desarrolladores desplegar rápidamente nuevas versiones de sus aplicaciones sin interrumpir el servicio existente.

Otra ventaja de Docker es que los contenedores son extremadamente livianos y rápidos de crear. Los contenedores se pueden iniciar y detener en cuestión de segundos, lo que significa que los desarrolladores pueden probar y depurar aplicaciones mucho más rápidamente que en entornos tradicionales.

Sin embargo, también hay algunas desventajas en el uso de Docker. Uno de los principales problemas es la complejidad de la plataforma. Docker puede ser difícil de aprender y configurar, especialmente para aquellos que no tienen experiencia previa en la gestión de contenedores.

Otro problema es que Docker puede ser más lento que los entornos tradicionales en algunos casos. Los contenedores requieren una capa adicional de virtualización, lo que puede afectar el rendimiento en entornos muy exigentes.

Por último, otro desafío al usar Docker es que la tecnología aún está evolucionando. A medida que se agregan nuevas características y se mejoran las capacidades existentes, puede ser difícil mantenerse al día con los cambios.

Objetivos:

- Aprender a realizar operaciones básicas con contenedores.
- Extraer evidencias desde equipo de infraestructura que ofrecen microservicios mediante contenedores.

Materiales

- Cualquier distribución Linux.
- Docker-ce
- Herramientas forenses: Docker-forensics-toolkit, Sysdig, docker-diff y docker-explorer.

PARTE A:Introducción a Docker

Realiza las siguientes tareas:

1. Instala docker en una distribución de Linux como por ejemplo Debian 11.
2. Lanza un comando docker que informe de la versión instalada.
3. Lanza un comando docker muestre información del host dónde se encuentra.
4. Ejecuta el comando docker necesario para descargar la imagen “nginx:latest” desde el hub de docker.
5. Ejecuta el comando docker necesario para listar las imágenes almacenadas en local.
6. Ejecuta un contenedor en segundo plano de la imagen “nginx:latest”
7. Ejecuta un contenedor en modo interactivo de la imagen “nginx:latest”
8. Ejecuta el comando docker necesario para listar los comandos que se están ejecutando.
9. Inspecciona todas las propiedades de uno de los contenedores.
10. Ejecuta el comando docker necesario para listar las redes configuradas para docker.
11. Engancha (attach) la consola a uno de tus contenedores.
12. Ejecuta un comando /bin/bash dentro de uno de tus contenedores en modo interactivo.
13. Para uno de tus contenedores.
14. Inicia de nuevo el contenedor anterior.
15. Borra uno de tus contenedores.
16. Crea un contenedor a partir de un dockerfile.

```
# Imagen base
FROM ubuntu
# Copiar el archivo 'file' a la raíz del contenedor
COPY script /
# Dar permisos de lectura al archivo 'file'
RUN chmod +x /file
```

17. Convierte el contenedor anterior en la imagen llamada “midebian”
18. Exporta la imagen “midebian” como fichero.
19. Exporta el contenedor “nginx” como fichero.
20. Borra alguno de tus contenedores
21. Borra la imagen “midebian”

PARTE B: Forense en Docker

1. Lee el siguiente artículo. Desde un punto de vista forense informático, ¿qué lecciones podemos aprender del artículo anterior acerca de la obtención de evidencias o resolución de incidentes de seguridad donde se vean involucrados contenedores?

2. Lee la ayuda de los modificadores de comando de docker siguientes: DIFF, SAVE, EXPORT, LOAD e IMPORT. Justifica para qué tareas forenses pueden ser de utilidad. Realiza ejemplos con cada uno de los modificadores.

3. Mira la documentación de la utilidad docker-diff se utiliza para comparar imágenes locales de docker con respecto a las que están localizadas en la nube (hub de docker). Descargate la utilidad y haz una prueba de la misma.

4. En el marco de una investigación en curso, se ha obtenido una imagen lógica correspondiente a una instalación de Docker en un sistema informático bajo sospecha. Se sospecha que dicha instalación podría haber sido utilizada para ocultar actividades. Como analista forense, se le ha encargado realizar un análisis exhaustivo de la imagen lógica de Docker, con el objetivo de identificar los servicios que ofrecen:

    a. Descargate una copia forense de la imagen lógica de Docker.
    b. Realizar un análisis de la configuración de Docker y de los contenedores alojados en la imagen lógica, describiendo nombres de las instancias, puertos utilizados, carpetas de datos usadas (mount) y logs de las mismas.
    c. Puedes seguir los pasos de este artículo

5. Docker Scout es una colección de funciones que proporciona información detallada sobre la composición y seguridad de las imágenes de contenedor. Sirve para analizar el contenido de las imágenes y generar un informe detallado de los paquetes y vulnerabilidades que detecta. También puede ayudar a proporcionar sugerencias sobre cómo remediar problemas descubiertos por el análisis de la imagen. Instalarlo y haz una pequeña prueba.
6. Lee el siguiente artículo. Desde un punto de vista forense, ¿para qué pueden ser útiles los checkpoints?