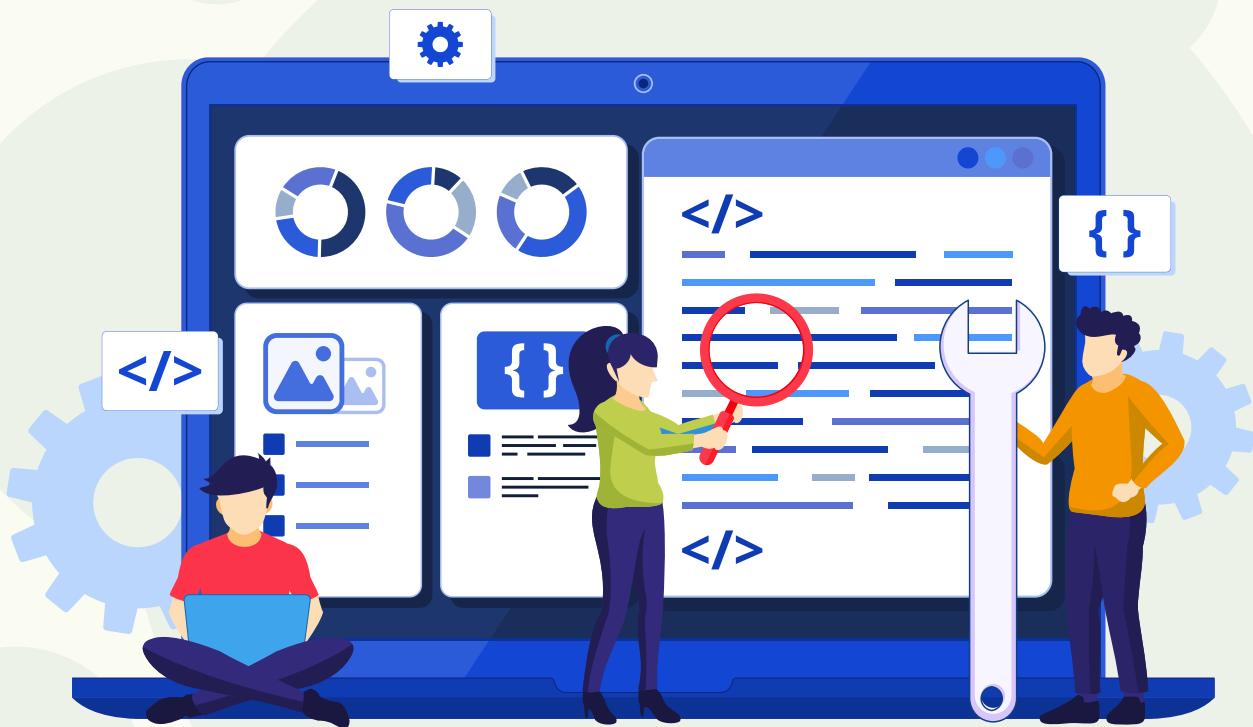


CICLO 4a

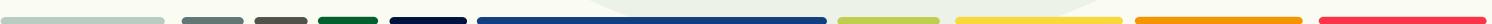
[FORMACIÓN POR CICLOS]

DOCKER SECURITY



UNIVERSIDAD
DE ANTIOQUIA

Facultad de Ingeniería





Como se ha mencionado, Docker es una herramienta que automatiza el despliegue de aplicaciones a partir de lo que conocemos como contenedores, lo cual permite empaquetar proyectos de desarrollo con todas sus dependencias y configuraciones necesarias para su funcionamiento.

Cuando hablamos de seguridad, puntualmente nos referimos al hecho de limitar el acceso del proyecto de *software* de todos los demás recursos que se tienen en el sistema operativo.

Hay cuatro áreas fundamentales a tratar cuando se habla de seguridad en Docker:

1. La seguridad del kernel y el soporte para los grupos de control de namespaces

Esto consiste básicamente en un principio fundamental, pues al momento de correr Docker se crea un conjunto de namespaces y grupos de control para cada contenedor. Estos espacios se encargan de aislar lo que se encuentra dentro del contenedor, de tal manera que se desconocen los procesos que se ejecutan en otros contenedores, y los grupos de control se encargan de limitar los recursos y generar una serie de estadísticas que permiten auditar el uso de cada contenedor

2. Superficie de ataque de Docker Daemon

El demonio de Docker, o Docker Daemon, o Dockerd, tiene permisos tipo root, y se encarga de escuchar peticiones de API y toma los contenedores, imágenes y otros elementos de Docker y los maneja como objetos.

3. Lagunas en el perfil de configuración del contenedor, ya sea de forma predeterminada o cuando los usuarios lo personalicen

El kernel de Linux cuenta con ciertas capacidades de forma predeterminada que permiten arrancar Docker con capacidades restringidas. Por lo general los servidores típicos ejecutan varios procesos como root, y los contenedores son diferentes porque sus tareas son manejadas por la infraestructura del contenedor. Debido a esto, los contenedores pueden ejecutarse con menos privilegios y no requieren ejecutarse desde la raíz, de tal manera que si un intruso ingresa a la raíz, le



es más difícil causar daños graves.

4. Las características de seguridad de “reforzamiento” del kernel y su interacción con los contenedores

Las capacidades son solo una de las características de seguridad que proporciona el kernel, dado que se pueden usar herramientas de terceros para aumentar los contenedores de Docker, lo cual implica que existen muchas formas de fortalecer esta herramienta.

Por ejemplo, ejecutar un kernel con GRSEC y PAX (módulos de seguridad para Linux) agregará varias comprobaciones de seguridad en tiempo de compilación y de ejecución y no requiere una configuración especial de Docker porque este módulo trabaja directo en Linux.

En conclusión, podemos decir que Docker es suficientemente seguro por sí solo desde la concepción de su estructura, y aún así permite otros sistemas que puedan reforzar agregando capas adicionales de seguridad.

Fuentes:

- <https://docs.docker.com/engine/security/>
- <https://www.kernel.org/doc/html/v4.16/admin-guide/LSM/tomoyo.html>
- [https://docs.docker.com/get-started/overview/#:~:text=The%20Docker%20daemon%20\(%20dockerd%20\)%20listens,daemons%20to%20manage%20Docker%20services.](https://docs.docker.com/get-started/overview/#:~:text=The%20Docker%20daemon%20(%20dockerd%20)%20listens,daemons%20to%20manage%20Docker%20services.)