Container Security

Recordamos

- Docker Daemon Security. (s.1-2)
- Docker Image Security. (s. 3)
- Docker Container Security. (s. 4)

Docker Container Security

Buenas prácticas:

1. No exponer puertos innecesarios
2. No iniciar contenedores en modo privilegiado

3. Eliminar capacidades al iniciar contenedores

- Por defecto, permitimos:
  - cambiar UIDs y GIDs de archivos
  - matar procesos
  - eludir comprobaciones de permisos de lectura, escritura y ejecución de archivos.

- Las opciones --cap-drop y --cap-add del comando docker run te permiten eliminarlas y otorgarlas.

Ejemplo, elimina todas las capacidades y añade CHOWN:

```
$ docker run --cap-drop=ALL --cap-add=CHOWN image:tag
```

4. Establecer cuotas de recursos

- Docker no aplica automáticamente ninguna restricción de recursos a tus contenedores.

- Los procesos en contenedores pueden usar CPU y memoria ilimitadas, lo que podría afectar a otras aplicaciones en su host.

- Establecer límites para estos recursos ayuda a defenderse contra ataques de denegación de servicio (DoS).

Ejemplo, límite de memoria y CPU

$ docker run -m=128m --cpus=2 imagen:tag

5. Ejecutar procesos como un usuario no root

- Los contenedores se ejecutan por defecto como root.
- Usa otro usuario para lanzar los procesos y minimizar el riesgo.

Ejemplo,

$ docker run --user=1000 image:tag

6. Evitar que los contenedores escalen privilegios

- Los contenedores normalmente pueden escalar sus privilegios llamando a los binarios setuid y setgid.

  Esto es un riesgo de seguridad porque el proceso en contenedor puede usar setuid para convertirse en root.

- Para prevenir esto, debes establecer la opción de seguridad no-new-privileges cuando inicies tus contenedores:

Ejemplo,

$ docker run -security-opt=no-new-privileges:true imagen:tag

7. Utilizar RO del sistema de archivos

- Si el contenedor no necesita escribir en el sistema de ficheros, activa el modo de sólo lectura para evitar modificaciones en el sistema de archivos.

- Esto impediría remplazar binarios o archivos de configuración.

Ejemplo,
$ docker run --read-only imagen:tag

8. Utilizar un gestor de secretos dedicado

- Los passwords como deben almacenarse en una solución de gestión de secretos dedicada.

  Esto reduce el riesgo de exposición accidental.