Nadia Arellano
Ingeniera en Informática

Actividad Práctica – Sesión 2 – Módulo 4

Pregunta 1

¿Cuál de las siguientes fases del ciclo de vida de un contenedor es crítica para garantizar que no queden datos residuales ni configuraciones comprometidas?
Respuesta correcta: d. Eliminación

Explicación: Durante la fase de eliminación, es crucial asegurarse de que no queden datos residuales (como volúmenes persistentes o credenciales temporales) que puedan ser explotados por atacantes.

Pregunta 2

¿Por qué es importante utilizar imágenes base oficiales o verificadas (como Alpine Linux o Ubuntu oficial) al construir contenedores?
Respuesta correcta: b. Para minimizar el riesgo de vulnerabilidades heredadas

Explicación: Las imágenes base oficiales son mantenidas por proveedores confiables y se actualizan regularmente para corregir vulnerabilidades conocidas.

Pregunta 3

¿Qué función tiene la capacidad “CAP_NET_ADMIN” en un contenedor?
Respuesta correcta: b. Permite realizar operaciones administrativas en redes

Explicación: Esta capacidad permite configurar interfaces de red, modificar reglas de firewall y realizar otras operaciones administrativas relacionadas con la red.

Pregunta 4

¿Cuál de las siguientes herramientas es ideal para escanear imágenes de contenedores en busca de vulnerabilidades conocidas?
Respuesta correcta: a. Trivy

Explicación: Trivy es una herramienta ligera y fácil de usar que escanea imágenes de contenedores en busca de vulnerabilidades en dependencias, bibliotecas y sistemas operativos.

Pregunta 5

¿Qué práctica ayuda a reducir la superficie de ataque en una imagen de contenedor?
Respuesta correcta: d. Utilizar una imagen base minimalista como Alpine Linux

Explicación: Las imágenes base minimalistas tienen menos componentes instalados, lo que reduce significativamente la superficie de ataque.

Nadia Arellano
Ingeniera en Informática

Pregunta 6

¿Por qué es importante eliminar paquetes innecesarios (como compiladores) después de su uso en una imagen Docker?
Respuesta correcta: c. Para mejorar la seguridad y reducir la superficie de ataque

Explicación: Estos paquetes pueden ser usados por atacantes; eliminarlos mejora la seguridad del contenedor.

Pregunta 7

¿Qué ventaja ofrece el uso de compilaciones multietapa en Docker?
Respuesta correcta: a. Separa el entorno de construcción del entorno de ejecución final

Explicación: Esto reduce el tamaño de la imagen final y elimina herramientas innecesarias en producción.

Pregunta 8

¿Cuál es el propósito de firmar digitalmente una imagen de contenedor?
Respuesta correcta: c. Verificar la autenticidad e integridad de la imagen

Explicación: Firmar digitalmente garantiza que la imagen no ha sido alterada y proviene de una fuente confiable.

Pregunta 9

¿Qué herramienta se puede integrar en un pipeline de CI/CD para validar continuamente las imágenes de contenedores antes de su despliegue?
Respuesta correcta: a. Anchore

Explicación: Anchore se integra en pipelines y escanea imágenes en busca de vulnerabilidades, cumplimiento y configuraciones inseguras.

Pregunta 10

¿Qué tipo de análisis realiza una herramienta como Trivy al escanear una imagen de contenedor?
Respuesta correcta: c. Análisis de vulnerabilidades en dependencias y bibliotecas

Explicación: Trivy identifica vulnerabilidades conocidas en las dependencias y bibliotecas de una imagen de contenedor.