Nadia Arellano
Ingeniera en Informática

Actividad Práctica – Sesión 3 – Módulo 4

Pregunta 1

¿Cuál es el propósito principal de firmar digitalmente las imágenes de contenedores?
Respuesta correcta: b. Garantizar la integridad y autenticidad de las imágenes

Explicación: Firmar digitalmente las imágenes permite asegurar que no han sido alteradas desde su creación y que provienen de una fuente confiable.

Pregunta 2

¿Qué herramienta se utiliza para habilitar Docker Content Trust (DCT)?
Respuesta correcta: b. Docker CLI

Explicación: Docker Content Trust es una funcionalidad integrada en Docker que se habilita mediante comandos como `export DOCKER_CONTENT_TRUST=1`.

Pregunta 3

¿Cuál de las siguientes prácticas ayuda a reducir la superficie de ataque en una imagen de contenedor?
Respuesta correcta: c. Eliminar paquetes innecesarios y dependencias

Explicación: Reducir la cantidad de componentes disminuye los posibles puntos de explotación en una imagen.

Pregunta 4

¿Qué tipo de análisis realiza una herramienta como Trivy en una imagen de contenedor?
Respuesta correcta: a. Escaneo de vulnerabilidades conocidas

Explicación: Trivy analiza las capas de una imagen para detectar vulnerabilidades en bibliotecas y dependencias.

Pregunta 5

¿Cuál es el propósito de integrar OWASP ZAP en un pipeline de CI/CD?
Respuesta correcta: c. Realizar pruebas dinámicas de seguridad simulando ataques reales

Explicación: OWASP ZAP es una herramienta DAST que simula ataques como inyecciones SQL para detectar vulnerabilidades en tiempo de ejecución.

Nadia Arellano
Ingeniera en Informática

Pregunta 6

¿Qué significa 'superficie de ataque' en el contexto de imágenes de contenedores?
Respuesta correcta: d. El conjunto de puntos vulnerables que pueden ser explotados por atacantes.

Explicación: Incluye bibliotecas, configuraciones y dependencias que representan posibles vectores de ataque.

Pregunta 7

¿Cuál de las siguientes herramientas es ideal para escanear vulnerabilidades en imágenes de contenedores antes del despliegue?
Respuesta correcta: a. Anchore

Explicación: Anchore se especializa en análisis de imágenes de contenedor para detectar vulnerabilidades y problemas de configuración antes del despliegue.

Pregunta 8

¿Qué tipo de prueba de seguridad evalúa el código sin ejecutarlo?
Respuesta correcta: b. Análisis estático de código (SAST)

Explicación: SAST revisa el código fuente en reposo para identificar patrones que puedan representar fallos de seguridad.

Pregunta 9

¿Qué política es recomendable implementar en un pipeline de CI/CD para garantizar la seguridad?
Respuesta correcta: b. Configurar el pipeline para que falle automáticamente si se detectan vulnerabilidades críticas

Explicación: Esto garantiza que no se desplieguen imágenes inseguras a producción.

Pregunta 10

¿Cuál de las siguientes afirmaciones sobre imágenes base minimizadas es verdadera?
Respuesta correcta: d. Las imágenes base minimizadas reducen el riesgo de vulnerabilidades al eliminar componentes innecesarios

Explicación: Imágenes como Alpine Linux o distroless tienen menos software instalado, lo que reduce posibles vulnerabilidades.