Nadia Arellano
Ingeniera en Informática

Evaluación Final – Módulo 4

Pregunta 1

¿Cuál es el principal riesgo de ejecutar un contenedor como usuario root?
Respuesta correcta: b. Permite que un atacante comprometa el sistema host si el contenedor está vulnerado.

Explicación: Ejecutar un contenedor como root implica que cualquier proceso dentro del contenedor tiene acceso completo al sistema operativo host. Si un atacante logra comprometer el contenedor, podría obtener acceso root al host.

Pregunta 2

¿Qué función cumplen las capacidades de Linux en la seguridad de contenedores?
Respuesta correcta: d. Dividir los privilegios del usuario root en subconjuntos más pequeños.

Explicación: Las capacidades de Linux permiten dividir privilegios tradicionales del usuario root en unidades menores, otorgando solo los permisos necesarios para tareas específicas.

Pregunta 3

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

Explicación: Anchore escanea imágenes de contenedores en CI/CD para verificar vulnerabilidades y cumplimiento normativo antes del despliegue.

Pregunta 4

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

Explicación: Trivy revisa bibliotecas y dependencias en las imágenes para detectar vulnerabilidades conocidas.

Pregunta 5

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

Explicación: Anchore se especializa en detectar vulnerabilidades y malas configuraciones en imágenes de contenedores.

Nadia Arellano
Ingeniera en Informática

Pregunta 6

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

Explicación: SAST inspecciona el código fuente o binario sin necesidad de ejecutarlo, identificando patrones de vulnerabilidad.

Pregunta 7

¿Qué es un Namespace en Linux?
Respuesta correcta: d. Una característica del kernel que permite aislar recursos y procesos.

Explicación: Los namespaces proporcionan aislamiento de recursos como procesos, redes o usuarios dentro de un sistema Linux.

Pregunta 8

¿Cuál de los siguientes namespaces aísla los identificadores de procesos (PID)?
Respuesta correcta: d. namespace PID

Explicación: El namespace PID garantiza que cada contenedor tenga su propio espacio de procesos, sin interferir con otros.

Pregunta 9

¿Qué tipo de alerta generaría Prometheus si se detecta un fallo crítico en el pipeline?
Respuesta correcta: b. Una alerta basada en reglas predefinidas, como un umbral de fallos excedido.

Explicación: Prometheus genera alertas automáticas si se superan ciertos umbrales críticos definidos por el usuario.

Pregunta 10

¿Qué es GitOps en el contexto de la gestión de cambios en imágenes de contenedores?
Respuesta correcta: c. Una metodología que utiliza repositorios de control de versiones como fuente única de verdad.

Explicación: GitOps gestiona cambios en infraestructura y aplicaciones desde repositorios Git, asegurando trazabilidad y control.

Pregunta 11

¿Qué política de red en Kubernetes permite segmentar el tráfico entre contenedores?
Respuesta correcta: a. Políticas de red

Explicación: Las políticas de red en Kubernetes controlan el flujo de tráfico entre pods, mejorando la seguridad del clúster.

Nadia Arellano
Ingeniera en Informática

Pregunta 12

¿Qué acción es recomendable para proteger Secrets en Kubernetes?
Respuesta correcta: c. Montar Secrets como volúmenes de solo lectura.

Explicación: Montar Secrets como volúmenes de solo lectura es más seguro que pasarlos como variables de entorno, reduciendo el riesgo de exposición.