Nadia Arellano
Ingeniera en Informática

Actividad Práctica – Sesión 1 – Módulo 4

Pregunta 1

¿Cuál de las siguientes afirmaciones describe mejor un contenedor?
Respuesta correcta: b. Una unidad ligera de software que encapsula una aplicación y sus dependencias.

Explicación: Un contenedor empaqueta una aplicación junto con todas sus dependencias, permitiendo su ejecución consistente en distintos entornos. Comparte el kernel del host, siendo más eficiente que una máquina virtual.

Pregunta 2

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

Explicación: Ejecutar como root en el contenedor puede permitir a un atacante que comprometa el contenedor escalar privilegios hasta el host.

Pregunta 3

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

Explicación: Las capacidades de Linux dividen los privilegios tradicionales del usuario en capacidades individuales. Esto permite otorgar solo los permisos necesarios para una tarea específica, reduciendo el impacto potencial de un ataque.

Pregunta 4

¿Qué bandera de Docker se utiliza para desactivar todas las capacidades de Linux en un contenedor?
Respuesta correcta: --cap-drop=ALL

Explicación: Este flag desactiva todas las capacidades de Linux, alineándose con el principio de menor privilegio.

Pregunta 5

¿Qué tipo de ataque implica obtener acceso no autorizado a recursos o funciones del sistema mediante la explotación de vulnerabilidades?
Respuesta correcta: d. Escalada de privilegios.

Explicación: Ocurre cuando un atacante explota vulnerabilidades para obtener más privilegios de los otorgados originalmente.

Nadia Arellano
Ingeniera en Informática

Pregunta 6

¿Qué herramienta permite definir políticas que restrinjan las llamadas al sistema que un proceso puede realizar?
Respuesta correcta: b. SECCOMP

Explicación: SECCOMP (Secure Computing Mode) limita las syscalls disponibles para un proceso, lo cual protege contra ataques que abusen del kernel.

Pregunta 7

¿Qué efecto tiene este comando "*docker run --read-only my-container*" en un contenedor?
Respuesta correcta: b. Hace que el sistema de archivos del contenedor sea de solo lectura.

Explicación: Evita modificaciones del sistema de archivos, lo que mitiga ciertos vectores de ataque.

Pregunta 8

¿Qué función cumplen los NAMESPACES en la seguridad de contenedores?
Respuesta correcta: d. Aislar recursos del sistema entre contenedores.

Explicación: Permiten que cada contenedor tenga su propio espacio de procesos, red, usuarios, etc., aislando su ejecución.

Pregunta 9

¿Qué implica aplicar el principio del menor privilegio en contenedores?
Respuesta correcta: c. Otorgar solo los permisos necesarios para que un contenedor cumpla su propósito.

Explicación: Limita los permisos al mínimo requerido para minimizar el impacto en caso de compromiso.

Pregunta 10

¿Qué herramienta permite definir perfiles de seguridad que limitan las acciones de un programa en un contenedor?
Respuesta correcta: a. APPARMOR

Explicación: APPARMOR define reglas para restringir el acceso a archivos, llamadas al sistema y otras operaciones de procesos.