Nadia Arellano
Ingeniera en Informática

Actividad Práctica - Sesión 8: Análisis y Buenas Prácticas en Seguridad Cloud

Pregunta 1

¿Qué servicio de AWS se utiliza principalmente para registrar eventos relacionados con la API?

- Respuesta correcta: AWS CloudTrail

AWS CloudTrail registra eventos relacionados con las llamadas a la API, permitiendo rastrear actividades de usuarios, roles y servicios.

Pregunta 2

¿Cuál de las siguientes herramientas se utiliza para realizar escaneos de puertos en una red?

- Respuesta correcta: Nmap

Nmap es una herramienta ampliamente utilizada para escanear puertos y servicios en una red, ayudando a identificar vulnerabilidades.

Pregunta 3

¿Qué tipo de prueba de seguridad implica simular ataques controlados para identificar vulnerabilidades?

- Respuesta correcta: Pruebas de penetración

Las pruebas de penetración simulan ataques reales para evaluar la seguridad de sistemas y detectar fallas antes de que sean explotadas.

Pregunta 4

¿Qué política de seguridad es recomendable implementar para proteger el acceso a cuentas de usuario en AWS?

- Respuesta correcta: Autenticación multifactor (MFA)

La MFA añade una capa adicional de verificación, lo que mejora la seguridad frente a accesos no autorizados.

Pregunta 5

¿Qué servicio de AWS proporciona una vista consolidada de la postura de seguridad?

- Respuesta correcta: AWS Security Hub

Security Hub centraliza hallazgos de varios servicios y entrega una visión unificada del estado de seguridad de tu entorno AWS.

Nadia Arellano
Ingeniera en Informática

Pregunta 6

¿Qué tipo de registro se utiliza para monitorear el tráfico de red dentro de una VPC en AWS?

- Respuesta correcta: Registros de flujo de VPC

Los VPC Flow Logs capturan detalles del tráfico IP que entra y sale de las interfaces de red dentro de una VPC.

Pregunta 7

¿Qué herramienta se utiliza combinada para analizar grandes volúmenes de logs mediante consultas SQL en AWS?

- Respuesta correcta: AWS Athena

Athena permite ejecutar consultas SQL directamente sobre datos almacenados en S3, ideal para el análisis de registros como CloudTrail o Flow Logs.

Pregunta 8

¿Cuál de las siguientes es una práctica recomendada para mejorar la seguridad continua en redes cloud?

- Respuesta correcta: Mantener sistemas y servicios actualizados

Actualizar regularmente ayuda a mitigar vulnerabilidades conocidas y evitar ataques basados en exploits.

Pregunta 9

¿Qué tipo de ataque se puede mitigar utilizando AWS Shield?

- Respuesta correcta: Ataques DDoS

AWS Shield protege contra ataques de denegación de servicio distribuido, asegurando la disponibilidad de servicios públicos en AWS.

Pregunta 10

¿Qué tipo de análisis se realiza al revisar registros para identificar actividades sospechosas?

- Respuesta correcta: Análisis forense

El análisis forense permite identificar eventos inusuales o maliciosos revisando logs detalladamente para investigar incidentes de seguridad.