Evaluación Final - Módulo 3: Seguridad en la Nube

Pregunta 1

¿Cuál es la principal diferencia entre un Firewall Tradicional y un Firewall de Aplicaciones Web (WAF)?

- Respuesta correcta: Un WAF filtra tráfico HTTP/HTTPS malicioso, mientras que un firewall tradicional bloquea tráfico IP y puertos.

El WAF opera en la capa de aplicación (capa 7) y está diseñado para proteger contra amenazas como XSS o inyección SQL, mientras que los firewalls tradicionales operan en capas inferiores controlando direcciones IP y puertos.

Pregunta 2

¿Qué tipo de ataque busca insertar código SQL malicioso en una consulta legítima para manipular una base de datos?

- Respuesta correcta: Inyección SQL

La inyección SQL permite a los atacantes ejecutar comandos SQL maliciosos, alterando consultas legítimas para acceder, modificar o eliminar datos sensibles.

Pregunta 3

¿Qué métrica de AWS CloudWatch podría usarse para configurar una alarma cuando el número de solicitudes bloqueadas exceda un umbral específico?

- Respuesta correcta: Solicitudes Bloqueadas

La métrica BlockedRequests muestra la cantidad de solicitudes bloqueadas por AWS WAF. Es útil para activar alarmas si se detecta un comportamiento anómalo en el tráfico.

Pregunta 4

¿Cuál de las siguientes es una buena práctica para el monitoreo y ajuste de firewalls en AWS?

- Respuesta correcta: Realizar pruebas de penetración regulares para evaluar la efectividad de las configuraciones.

Las pruebas de penetración ayudan a validar que las reglas de firewall estén correctamente configuradas y sean efectivas ante amenazas actuales.

Pregunta 5

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

- Respuesta correcta: AWS Security Hub

AWS Security Hub centraliza los hallazgos de seguridad de servicios como GuardDuty, Inspector, y AWS Config, entregando una vista completa del estado de seguridad en AWS.

Pregunta 6

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

- Respuesta correcta: Ataques DDoS

AWS Shield proporciona protección especializada contra ataques de denegación de servicio distribuidos (DDoS), asegurando la disponibilidad de las aplicaciones públicas.