Nadia Arellano
Ingeniera en Informática

Actividad Práctica - Sesión 7: WAF y Shield

Pregunta 1

¿Cuál es el propósito principal de AWS WAF?

- Respuesta correcta: Proteger aplicaciones web contra ataques como inyecciones SQL y XSS.

AWS WAF está diseñado para proteger aplicaciones web de amenazas comunes como inyección SQL y XSS, analizando el tráfico HTTP/HTTPS entrante y aplicando reglas personalizadas.

Pregunta 2

¿Cuál de las siguientes métricas es monitoreada por AWS CloudWatch para AWS WAF?

- Respuesta correcta: Número de solicitudes bloqueadas o permitidas.

CloudWatch ofrece métricas como BlockedRequests y AllowedRequests que ayudan a medir la efectividad de las reglas en WAF.

Pregunta 3

¿Qué nivel de AWS Shield ofrece mitigación automatizada sin costo adicional?

- Respuesta correcta: AWS Shield Standard.

AWS Shield Standard protege automáticamente contra ataques DDoS de capa 3 y 4 sin costo adicional.

Pregunta 4

¿Qué tipo de ataque es más comúnmente mitigado por AWS Shield Standard?

- Respuesta correcta: Ataques de capa 3 y capa 4 (DDoS).

Shield Standard mitiga ataques como SYN Flood y UDP Flood que afectan las capas 3 y 4 del modelo OSI.

Pregunta 5

¿Qué herramienta de AWS permite ajustar dinámicamente reglas de seguridad basadas en patrones de tráfico observados?

- Respuesta correcta: AWS WAF.

AWS WAF permite definir reglas que se ajustan dinámicamente ante cambios en el patrón de tráfico, como aumentos repentinos de solicitudes.

Pregunta 6

¿Cuál de las afirmaciones sobre AWS Shield Advanced es verdadera?

- Respuesta correcta: Ofrece soporte técnico prioritario y análisis en tiempo real.

Shield Advanced incluye monitoreo personalizado, mitigación avanzada y soporte técnico especializado.

Nadia Arellano
Ingeniera en Informática

Pregunta 7

¿Qué componente de AWS WAF se utiliza para inspeccionar cadenas de consulta en las solicitudes HTTP?

- Respuesta correcta: FieldToMatch.

FieldToMatch especifica qué parte de la solicitud debe inspeccionarse, como URI, encabezados o query string.

Pregunta 8

¿Qué acción debe realizarse primero al detectar un aumento significativo en solicitudes desde una región geográfica específica?

- Respuesta correcta: Crear una regla para bloquear el tráfico desde esa región.

Se recomienda bloquear temporalmente el tráfico sospechoso con una regla en WAF como primera medida de mitigación.

Pregunta 9

¿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.

BlockedRequests es la métrica que indica cuántas solicitudes fueron bloqueadas por WAF y puede utilizarse para alarmas.

Pregunta 10

¿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 del firewall funcionen correctamente y revelan posibles mejoras.