Nadia Arellano
Ingeniera en Informática

Actividad Práctica - Sesión 6: Seguridad con WAF y AWS Shield

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 actúa en la capa de aplicación (capa 7) y protege contra ataques como inyección SQL o XSS, mientras que un firewall tradicional opera en capas inferiores (3 y 4), 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 es un tipo de ataque donde el atacante envía comandos SQL maliciosos para alterar el comportamiento de la base de datos.

Pregunta 3:

En AWS WAF, ¿qué componente se utiliza para agrupar reglas y aplicarlas a recursos específicos?

- Respuesta correcta: Web ACLs (Access Control Lists)

Las Web ACLs permiten organizar y aplicar múltiples reglas de seguridad a servicios como CloudFront, ALB o API Gateway, bloqueando o permitiendo tráfico según patrones definidos.

Pregunta 4:

¿Cuál de las siguientes afirmaciones sobre AWS Shield Standard es correcta?

- Respuesta correcta: AWS Shield Standard es un servicio gratuito que proporciona protección básica contra ataques DDoS para recursos como CloudFront y Elastic Load Balancing.

AWS Shield Standard está activado por defecto y protege automáticamente los servicios públicos de AWS contra ataques DDoS comunes, sin costo adicional.

Pregunta 5:

¿Qué herramienta de AWS se utiliza para monitorear eventos y ajustar reglas en AWS WAF según anomalías detectadas?

- Respuesta correcta: AWS CloudWatch

AWS CloudWatch recopila métricas, registros y eventos, y permite generar alarmas para tomar acciones automáticas en servicios como AWS WAF, lo que facilita la respuesta a comportamientos anómalos o ataques.