PROYECTO No. 2: Controles de seguridad para una aplicación en la nube

OBJETIVOS

- Integrar el uso de Web Security Scanner en el proceso de desarrollo de software en la nube para identificar vulnerabilidades comunes como inyección SQL, XSS (Cross-Site Scripting) y configuraciones inseguras.
- Configurar y optimizar el uso de Cloud Armor para proteger aplicaciones y servicios contra diferentes ataques.
- Desarrollar políticas de acceso y reglas de firewall y red para mitigar el impacto de tráfico malicioso dirigido a los recursos en la nube.
- Implementar cifrado en reposo y tránsito para diferentes servicios en la nube.
- Diseñar e implementar políticas de control de acceso basadas en principios de mínimo privilegio utilizando IAM (Identity and Access Management) de GCP.

EQUIPO DE TRABAJO

Para este proyecto, deben continuar en los equipos de tres personas. El proyecto está planeado para tres semanas, en las que cada estudiante deberá invertir las horas definidas en su planeación semanal conforme a la cantidad de créditos del curso.

RECOMENDACIONES

En este proyecto, continuará utilizando la aplicación desplegada en GCP. En esta etapa implementará diferentes servicios que evaluarán la seguridad de la solución en la nube y brindarán una capa adicional para mejorar la postura global seguridad en sus ambientes. Finalmente se aplicarán los conceptos teóricos estudiados en esa fase del curso.

DESCRIPCIÓN DE LAS TAREAS A IMPLEMENTAR

Este proyecto es la continuación del diseño, desarrollo y despliegue de una plataforma simplificada de blogging. En esta sección se utilizarán controles para mejorar la postura de seguridad de la aplicación desplegada, utilizando los servicios de la infraestructura de Google Cloud Platform (GCP).

Semana 1: Controles de seguridad en la Capa de Computo

Actividades:

1. **Análisis de Seguridad con Web Security Scanner y Artifact Analysis:**

- Ejecutar análisis detallado sobre el contenedor [Artifact Analysis]
- Ejecutar análisis detallado sobre la aplicación web en ejecución.
- Detectar vulnerabilidades comunes como inyección de SQL, XSS, errores de configuración en cabeceras HTTP, etc.
- Establecer una priorización de las vulnerabilidades para una posterior remediación.

2. **Revisión de Configuraciones IAM existentes:**

- Auditar las políticas de IAM en busca de configuraciones permisivas.
- Generar diferentes roles entre los miembros del equipo de trabajo para brindar accesos específicos a recursos de GCP. También aplicar el principio de mínimo privilegio para los roles y cuentas de servicio que interactúan en la aplicación.
- Documentar pruebas y resultados.

3. **Load Balancing y Controles de red:**

- Implementar un balanceador de carga tipo HTTP, para la aplicación desplegada.
- Establecer mínimo los siguientes controles de red: 3.1. Reglas de firewall a nivel de red para permitir únicamente el tráfico necesario entre los recursos en el proyecto. 3.2. Bastion host para acceder a los recursos. 3.3. Cifrado de tráfico interno activando Encriptación en Tránsito. 3.4. Private Google Access para que los contenedores puedan acceder a los servicios de Google sin usar direcciones IP públicas.

Semana 2: Gestión de secretos y cifrado DB

Actividades:

1. **Google Secret Manager:**

- Configurar Secret Manager para almacenar claves API, credenciales de bases de datos y otros secretos críticos.
- Habilitar el versionado de secretos para facilitar la gestión de cambios.

2. **Roles y Permisos:**

- Establecer roles específicos en IAM para limitar el acceso a secretos según las responsabilidades del equipo:
    - **roles/secretmanager.admin** para administradores.
    - **roles/secretmanager.secretAccessor** para servicios y usuarios que necesitan acceso a secretos.

3. **Rotación de Claves:**

- Implementar políticas de rotación automática de claves cada 90 días utilizando funciones de rotación en Secret Manager.
- Configurar alertas para notificar cuando un secreto esté por expirar.

4. **Cifrado de Base de Datos:**

- Configurar cifrado para la base de datos utilizada en la solución desplegada.
- Implementar buenas prácticas de seguridad para el tipo de base de datos utilizada en el proyecto.

5. **Estrategia de Backup:**

- Definir una estrategia de backup que priorice la seguridad y la disponibilidad de los datos. Esta sección no es necesario implementarla en GCP.

6. **Preparación WAF:**

- Configurar Google Cloud Armor en modo "permisivo" (solo registro) para observar patrones de tráfico sin bloquear ni aplicar reglas.

Semana 3: Implementación de Web Application Firewall (WAF) y otros controles

Actividades:

1. **Configuración de Google Cloud Armor:**

- Crear reglas personalizadas para bloquear:
  - Tráfico basado en IPs sospechosas.
  - Intentos de inyección (SQL/XSS), DDoS y otros 2 ataques OWASP Top 10.
- Aplicar reglas de geolocalización para restringir acceso a regiones no autorizadas.
- Concatenar reglas para ahorro de costos en Google Cloud Armor.

2. **Integración con el Balanceador de Carga:**

- Configurar el WAF para filtrar todo el tráfico a través de Google Cloud Armor antes de llegar a la aplicación.

3. **Pruebas de Simulación:**

- Efectuar un ataque simple sobre la infraestructura de la aplicación en GCP, con herramientas similares a OWASP ZAP y Burp Suite.
- Ajustar las reglas del WAF basándose en los resultados de las pruebas.

ENTREGABLES

- Diagrama de arquitectura actualizada de la solución desplegada en GCP.
- Documentación del proyecto teniendo en cuenta las actividades de las 3 semanas (incluyendo la configuración de los controles de seguridad, detalles de los nuevos servicios y las mejores prácticas aplicadas).
- Demostración de los controles de seguridad sobre la aplicación desplegada en GCP. Realice un video con una duración máxima de 8 minutos en el que presente los controles de seguridad de su aplicación. Enlace el video al repositorio correspondiente.

Nota: Los monitores pueden solicitarles una sustentación síncrona, independiente a la video sustentación. Se recomienda dejar el ambiente configurado para dicho propósito, aunque pueden estar apagados los recursos para no gastar la totalidad de créditos.

ESQUEMA DE EVALUACIÓN

Criterios	Puntos
Semana 1 (25 puntos)	
- Análisis de Seguridad con Web Security Scanner y Artifact Analysis	10
- Revisión de Configuraciones IAM existentes	5
- Load Balancing y Controles de red	10
Semana 2 (25 puntos)	
- Google Secret Manager, IAM	10
- Rotación de claves, Cifrado DB	10
- Estrategia Backup cloud	5
Semana 3 (25 puntos)	
- Google Cloud Armor (Reglas de IP y Geolocalización)	10
- Google Cloud Armor (Reglas del OWASP Top 10)	10
- Pruebas y validación de funcionamiento	5
Sustentación y Documentación (25 puntos)	
- Documento con recortes de pantalla de la configuración realizada	10
- Video de explicación de los controles de seguridad implementados	15
Total (100 puntos)	