Proyecto Final A
Seguridad y Auditoria de Sistemas
20 puntos / Ingeniería en Sistemas.
Fecha de Entrega 26/10/2024

Gestión Integral de Seguridad en la Nube con AWS Security Hub y Amazon Macie

Objetivo:

Los estudiantes diseñarán e implementarán un entorno de seguridad en la nube, integrando múltiples herramientas avanzadas de seguridad de AWS, como AWS Security Hub, Amazon Macie, GuardDuty, y AWS Inspector. Deberán identificar vulnerabilidades y datos sensibles, gestionar los hallazgos y proponer un plan de mitigación de riesgos.

Fase 1: Configuración de un entorno multi-account en AWS

Objetivo: Crear una infraestructura simulada en AWS que represente diferentes departamentos de una empresa, cada uno con su propia cuenta AWS y roles específicos.

Actividades:

1. **Creación de múltiples cuentas en AWS:**
    - Los estudiantes deben crear un entorno multi-account utilizando AWS Organizations, representando al menos tres departamentos (por ejemplo, Finanzas, Recursos Humanos y TI).
    - Configurar una política de acceso restringido entre cuentas para asegurar que solo roles administrativos puedan gestionar los aspectos de seguridad.
2. **Implementación de AWS Security Hub:**
    - Configurar AWS Security Hub en cada cuenta para centralizar los hallazgos de seguridad desde diferentes servicios de AWS, como Macie, GuardDuty y Inspector.
    - Habilitar reglas de conformidad (compliance) como CIS AWS Foundations Benchmark para evaluar la configuración de seguridad de las cuentas.

- Configurar alertas y visualización de reportes en Security Hub, y consolidar estos hallazgos en una cuenta central (por ejemplo, en una cuenta de auditoría).

3. **Resultado esperado:**
   - Configuración de un entorno multi-account donde AWS Security Hub centraliza los hallazgos de seguridad de diferentes cuentas.

Fase 2: Integración de Amazon Macie y análisis de datos sensibles

Objetivo:

Utilizar Amazon Macie para analizar y clasificar datos sensibles almacenados en Amazon S3, detectando información personal identificable (PII) y posibles violaciones de seguridad.

Actividades:

1. **Escaneo de Buckets de S3 con Amazon Macie:**
   a. Configurar Amazon Macie para identificar automáticamente datos sensibles (PII) en los buckets de Amazon S3 de las diferentes cuentas.
   b. Crear un reporte detallado que indique qué datos se consideran sensibles, su ubicación y qué usuarios tienen acceso.
   c. Configurar políticas de alerta para cualquier acceso no autorizado o actividad anómala en los buckets que contengan datos sensibles.
2. **Análisis de exposición de datos:**
   a. Revisar las políticas de acceso de los buckets de S3 y verificar si cumplen con las mejores prácticas de seguridad.
   b. Identificar posibles configuraciones erróneas que puedan exponer datos sensibles a usuarios no autorizados.
3. **Resultado esperado:**
   a. Identificación de datos sensibles en S3 con Amazon Macie y recomendaciones para reducir la exposición de dichos datos.

Fase 3: Análisis de vulnerabilidades con GuardDuty e Inspector

Objetivo: Detectar posibles amenazas y vulnerabilidades en el entorno AWS utilizando Amazon GuardDuty y AWS Inspector.

Actividades:

1. **Configuración de Amazon GuardDuty:**
   a. Activar Amazon GuardDuty en todas las cuentas para monitorear el tráfico de red, logs de AWS CloudTrail y DNS en busca de

comportamientos anómalos, tales como intentos de acceso no autorizados o malware.

   b. Analizar alertas generadas por GuardDuty y priorizar las más críticas.
   c. Análisis de vulnerabilidades con AWS Inspector:
   d. Utilizar AWS Inspector para realizar escaneos de seguridad en instancias EC2 desplegadas en las cuentas de la empresa, identificando configuraciones débiles, software desactualizado y problemas de seguridad en los paquetes instalados.
   e. Configurar escaneos automáticos en instancias nuevas y existentes.

2. **Correlación de hallazgos entre herramientas:**
   a. Correlacionar los hallazgos de GuardDuty, Inspector y Security Hub para identificar las vulnerabilidades más críticas.
   b. Describir cómo la integración de estas herramientas mejora la visibilidad general de la seguridad.
3. **Resultado esperado:**
   a. Detectar amenazas y vulnerabilidades críticas, con propuestas de corrección para mejorar la postura de seguridad del entorno.

Fase 4: Informe de auditoría de seguridad

Objetivo: Elaborar un informe completo que resuma los hallazgos y proponga medidas de mitigación de riesgos y un plan de respuesta a incidentes.

Actividades:

1. Redacción del Informe:
   a. El informe debe incluir una descripción detallada de los hallazgos de seguridad en las cuentas AWS, destacando las amenazas detectadas por GuardDuty, los datos sensibles identificados por Macie, y las vulnerabilidades encontradas por Inspector.
   b. Para cada hallazgo, se debe proponer una medida de mitigación o corrección, como endurecimiento de configuraciones, eliminación de datos sensibles o actualizaciones de software.
2. Propuesta de controles de seguridad:
   a. Proponer un conjunto de controles de seguridad basados en los hallazgos, incluyendo medidas preventivas y correctivas.
   b. Sugerir mejoras de gobernanza para el entorno multi-account, como el uso de políticas de acceso más estrictas, herramientas de cifrado, y la activación de logs y monitoreo.
3. Plan de respuesta a incidentes:

    a. Crear un plan de respuesta a incidentes detallado para el entorno multi-account, definiendo cómo reaccionar ante diferentes tipos de amenazas, desde accesos no autorizados a datos sensibles hasta ataques activos detectados por GuardDuty.
    b. Incluir una política de notificación y gestión de incidentes.
4. Resultado esperado:
    a. Un informe final bien estructurado, con un análisis completo de la seguridad en el entorno AWS y propuestas concretas para mejorar la postura de seguridad y mitigar los riesgos.

Evaluación y Presentación Final:

Puntuación por fases: Cada fase del proyecto será evaluada individualmente, considerando tanto la implementación técnica como el análisis y la documentación de los resultados.

Defensa del Proyecto: Al final, los estudiantes deberán presentar su informe y demostrar cómo implementaron cada herramienta y cómo respondieron a los riesgos identificados.

Este proyecto integra múltiples herramientas avanzadas de AWS para la gestión de seguridad en la nube, exigiendo a los estudiantes no solo habilidades técnicas para la configuración de estas herramientas, sino también un enfoque profundo en la auditoría de seguridad, análisis de riesgos, y la gestión de incidentes en un entorno cloud.

NOTA: Hacer el despliegue de la infraestructura con Jenkins y Terrraform para IAC.

Éxitos

Ing. Caal